NOTES

DEMYSTIFYING THE INTERNET OF THINGS: INDUSTRY IMPACT, STANDARDIZATION PROBLEMS, AND LEGAL CONSIDERATIONS

Robin Kester*

"[N]ecessity . . . is the mother of our invention."[1]

—Plato

I. Introduction

Cisco, the company, has said, "The Internet of Things (IoT), sometimes referred to as the Internet of Objects, will change everything—including ourselves."[2] But what is the Internet of Things (hereinafter "IoT")?[3]

* Solo law practitioner in Greensboro, NC. She received a B.S. degree in Computer Science from High Point University, an M.S. degree in Computer Science from Wake Forest University, and a J.D. from Elon University School of Law. She would like to thank her parents, Walter and Rita, for their support and encouragement.

[1] Plato, The Republic, bk. II (Benjamin Jowett trans., The Internet Classics Archive, MIT 1994) (360 B.C.E.), http://classics.mit.edu/Plato/republic.3.ii.html.

[2] Dave Evans, Cisco Internet Business Solutions Group, The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, 2 (2011), http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[3] *E.g.*, Daniel Kellmereit & Daniel Obodovski, The Silent Intelligence: The Internet of Things 17 (2013). The term the "Internet of Things" was originally coined by Kevin Ashton, the former general manager of Belkin and one of the founders of the Auto-ID Center at Massachusetts Institute of Technology (MIT), around 1995. Kevin Maney, *Meet Kevin Ashton, The Father of the Internet of Things*, Newsweek (Feb. 23, 2015, 12:10 PM), http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html.

Different terminology has been used in association with IoT, such as "Machine to Machine (M2M)" and "smart products."[4] Other terms, such as "ubiquitous computing"[5] and "Big Data," have also been used in conjunction with discussing IoT.[6] However, at the end of the day, IoT is a "network of items—each embedded with sensors—which are connected to the Internet."[7] We interact with sensors on a daily basis without even realizing it. For example, sensors can be found in your car, cellphone, credit cards, gaming consoles, and inside clothing.[8]

The idea behind IoT is to take everyday, physical objects, connect them to the Internet, and monitor and analyze data while providing real-time feedback.[9] While the original intent behind IoT was aimed at improving manufacturing efficiency,[10] today the possibilities and applications of IoT are endless and can be applied in other industries and everyday life. "More things are connecting to the Internet than people—over 12.5 billion devices in 2010 alone. Cisco's Internet Business Solutions Group (IBSG) predicts some twenty-five billion devices will be connected by 2015, and fifty billion by 2020."[11]

One of the driving forces behind the increase in the number of objects connecting to the Internet is the decrease in the cost of computation or computer processing.[12]

> [T]he cost of processing has become 128 times cheaper in the last decade, so cheap that it is almost an insignificant consideration in the development of new connected products and services. We can embed silicon

[4] *Internet of Things, Machine-to-Machine or Smart Products?*, VINNTER, http://www.vinnter.se/internet-of-things/ (last visited Feb. 14, 2015).

[5] M. Scott Boone, *Ubiquitous Computing, Virtual Worlds, and the Displacement Of Property Rights*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 91, 92 (2008) ("[U]biquitous computing has been described as 'the colonization of everyday life' by computers and information technology.").

[6] Howard Baldwin, *A Match Made Somewhere: Big Data and the Internet of Things*, FORBES (Nov. 24, 2014), http://www.forbes.com/sites/howardbaldwin/2014/11/24/a-match-made-somewhere-big-data-and-the-internet-of-things/.

[7] Kathy Pretz, *Smarter Sensors: Making the Internet of Things Soar*, THE INSTITUTE (Mar. 14, 2014), http://theinstitute.ieee.org/technology-focus/technology-topic/smarter-sensors.

[8] *Id.*

[9] *See* Michael Chui et. al., *The Internet of Things*, MCKINSEY & COMPANY (Mar. 2010), http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things.

[10] *See* KELLMEREIT & OBODOVSKI, *supra* note 3, at 17.

[11] Dinesh Sharma, *The Internet of Things Connected by 2015*, EBRAHMA (Dec. 16, 2013), http://www.ebrahma.com/2013/12/the-internet-of-things-connected-by-2015/.

[12] DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 52 (2014).

> and sensors in any object-shoes, pill bottles, light bulbs, wallets, and furniture-virtually without noticing the incremental costs.[13]

This Note brings to light the positive impact of IoT on various industries. This Note also discusses the problems associated with IoT technology and the need for standardization. Finally, this Note explains the present and future legal considerations resulting from the implementation of IoT.

II. Industry Impact

According to Gartner, "IoT product and service suppliers will generate incremental revenue exceeding $300 billion in 2020."[14] Additionally, "[t]he worldwide IoT market is forecast to grow from $1.3 trillion in 2013 to $3.04 trillion in 2020 with a compound annual growth rate (CAGR) of 13%."[15] As a result, many industries will be encompassing IoT into their operations, effectively "changing the way we do business and experience life."[16]

A. *Manufacturing Industry*

IoT will have a great impact on manufacturing because IoT advances productivity.[17] Not only will IoT impact manufacturers by providing increased productivity on the assembly line,[18] but IoT will also change how the product itself is manufactured.[19]

> According to a December 2013 survey by the American Society for Quality (ASQ), only 13 percent of the manufacturers surveyed said they use smart manufacturing within their organization. Of those organizations that claim to have implemented smart manufacturing, 82 percent say they have experienced increased efficiency, 49 percent experienced fewer

[13] *Id.* at 52.

[14] *Gartner Says the Internet of Things Will Transform the Data Center*, Gartner (Mar. 19, 2014), http://www.gartner.com/newsroom/id/2684616.

[15] *Finding Success in the New IoT Ecosystem: Market to Reach $3.04 Trillion and 30 Billion Connected "Things" in 2020, IDC Says*, Business Wire (Nov. 7, 2014, 8:30 AM), http://www.businesswire.com/news/home/20141107005028/en/Finding-Success-IoT-Ecosystem-Market-Reach-3.04.

[16] Chris Neiger, *3 Industries Being Overhauled by the Internet of Things*, The Motley Fool (Nov. 3, 2014, 9:00 AM), http://www.fool.com/investing/general/2014/11/03/3-industries-being-overhauled-by-the-internet-of-t.aspx.

[17] *See* Jeremy Rifkin, The Zero Marginal Cost Society 70 (2014).

[18] *See id.*

[19] *The Internet of Things: How a World of Smart, Connected Products is Transforming Manufacturers*, PTC 10, http://www.ptc.com/File%20Library/About%20PTC/Manufacturing%20Transformation/PTC_Impact_of_IoT_on_Manufacturers_eBook.pdf (last visited Feb. 21, 2015).

> product defects and 45 percent experienced increased customer satisfaction.[20]

In other words, a majority of manufacturers who have already incorporated IoT into the manufacturing process have experienced an increase in efficiency or productivity, and almost half of these manufacturers have produced fewer defective products, while increasing the satisfaction of their customers.

For example, by receiving IoT data from machines on the factory floor that are connected to the Internet, production line facilities managers will have access to real-time information regarding the status of each machine from any location.[21]

> When you equip people with mobile technology, you can dramatically shrink the delta between when a problem occurs and when it's acted upon. If there's a quality control problem in a production line, they can shut down the line before it continues to create products that will all be waste.[22]

Moreover, IoT and IP Networks can connect multiple manufacturing locations that have typically been isolated from one another, resulting in the sharing of information.[23] Manufacturers can then use this information to optimize production and automate workflows, while not requiring any human intervention.[24] For example, the Harley Davidson motorcycle plant in Pennsylvania uses software to measure and detect deviations in equipment, such as fan speeds, temperature, and humidity.[25] The software will automatically adjust the equipment if levels start to fall out of a permissible range.[26]

With sensors on manufacturing equipment, IoT will also help plants and facilities to become more proactive in the preventative maintenance of their manufacturing equipment by adjusting certain

[20] Lopez Research LLC, "Building Smarter Manufacturing with the Internet of Things (IoT)": Part 2. of "The IoT Series" 2 (2014) (on file with the author).

[21] *Id.* at 5. In the past, this type of information has generally been available on a PC in a control room where the facility manager would have to reside. *Id.*

[22] *Id.* (citing Alan Joch, *United Airlines and GE Make Room for Mobility*, BizTech (Dec. 13, 2013), http://www.biztechmagazine.com/article/2013/12/united-airlines-and-ge-make-room-mobility).

[23] *Id.* at 6.

[24] *Id.*

[25] *Id.* (citing James R. Hagerty, *How Many Turns in a Screw? Big Data Knows*, Wall Street J. (May 17, 2013, 7:57 PM), http://www.wsj.com/articles/SB10001424127887324059704578472671425572966).

[26] *Id.*

levels, such as temperature and vibration, prior to a malfunction.[27] In addition, manufacturers can use IoT to discern what is going on in the supply chain in real-time through location tracking and inventory monitoring.[28]

The products that are manufactured will also be impacted by IoT.[29]

> Products have evolved from purely physical components to complex systems combining processors, sensors, software, and digital user interfaces that are now connected to the Internet and each other . . . . The impact is a fundamental transformation of how manufacturers create and exchange value with customers. This transformation is shifting the sources of value and differentiation to software, the cloud, and service, and spawning entirely new business models.[30]

In other words, manufacturers will need to produce products that are embedded with sensors and software, which are connected to the Internet, in order to stay competitive and provide value for their customers. FitBit's® bracelet is a great example of a product that contains embedded sensors and has the capability of tracking physical activity.[31]

B. *Automobile Industry*

Most modern cars already contain sensors that monitor fuel and coolant levels, oil pressure, temperature,[32] and the author's personal favorite, the O2 or oxygen sensor, which often attempts to conceal itself as the "Check Engine" light on the dashboard of her Nissan Pathfinder.[33] However, with IoT technology, "The ultimate car with sensors and cameras will be self-driving."[34] "[S]elf-driving vehicles not only promise new productivity when driving, they will also help us avoid

[27] *Id.* at 7.

[28] *Id.*

[29] *The Internet of Things: How a World of Smart, Connected Products is Transforming Manufacturers*, *supra* note 19, at 2.

[30] *Id.*

[31] ROSE, *supra* note 12, at 53.

[32] Kevin Clemens, *Understanding Your Vehicle's Sensors*, MOBIL, https://mobiloil.com/en/article/car-maintenance/basic-car-maintenance-tips/understanding-your-vehicles-sensors (last visited Feb. 21, 2015).

[33] Philip Reed, *How to Fix Your Car's Oxygen Sensor*, EDMUND'S (Feb. 11, 2013), http://www.edmunds.com/car-care/how-to-fix-your-cars-oxygen-sensor.html.

[34] Piet De Moor, *Internet of Things: Image Sensors for a Smart Environment*, SENSORS ONLINE (Feb. 20, 2015), http://www.sensorsmag.com/internet-things/image-sensors-smart-environment-17213.

accidents and make roads safer. Adding sensors to automobiles to prevent low-speed crashes could create economic value of as much as $50 billion per year by 2025."[35]

In 2014, Ford Motor Company introduced a "smart car" at the Mobile World Congress.[36] The car's technology "included[ed] 360-degree views of the area around the vehicle, sensors to scan for other vehicles, pedestrians and objects, and smart cruise control to avoid accidents."[37]

Smart cars, coupled with intelligent roadside sensors and traffic management systems, will also enhance the driving experience.[38] For example, new routes could be suggested to the smart car in order to avoid traffic congestion.[39] In addition, parking spaces within the city could be monitored for availability, and this information could be relayed to the smart car.[40]

Gartner research predicts that by the year 2020, one out of every five cars will be connected to the Internet wirelessly, resulting in over 250 million connected cars worldwide.[41] However, as the car becomes more automated, car manufacturers will be exposed to more liability.[42]

C. *Health Care Industry*

Applying IoT to the health care industry will provide more access to health care, enhance the quality of life of patients, and will ultimately decrease the cost of health care.[43] For example, many people who have health problems on a global scale may not have access to

[35] Rose, *supra* note 12, at 235.

[36] Danielle Goodman, *This Week In the Internet of Things: Connected Cars, Smart Home Controls, Gesture Based Sensors and Big Data Processing*, Skyhook (Mar. 14, 2014), http://blog.skyhookwireless.com/devices/this-week-in-the-internet-of-things.

[37] *Id.*

[38] *What Things Are Included in Internet of Things (IoT)?*, AppStudioz (Dec. 18, 2014), https://medium.com/@Appstudioz/what-things-are-included-in-internet-of-things-iot-4adac3077578.

[39] *Id.*

[40] *See Id.*

[41] Anu Passary, *250 Million: Number of Connected Vehicles on the Road in 2020, According to Gartner*, Tech Times (Jan. 28, 2015, 1:33 AM), http://www.techtimes.com/articles/29002/20150128/250-million-number-of-connected-vehicles-on-the-road-in-2020-according-to-gartner.htm.

[42] Rose, *supra* note 12, at 236.

[43] David Niewolny, How the Internet of Things is Revolutionizing Healthcare, Freescale 1 (2013), http://cache.freescale.com/files/corporate/doc/white_paper/IOTREVHEALCARWP.pdf.

sufficient health monitoring.[44] However, IoT devices that are wirelessly connected to the Internet can monitor patient health with the use of sensors and remotely send the information to the appropriate medical professionals who can make a proper health recommendation.[45]

The quality of life of people will also be improved because the mobility of IoT will allow elderly patients to remain living in their homes while still being monitored remotely.[46] With continuous monitoring through IoT devices, the cost of care will also be reduced because the caregiver will not have to constantly collect and analyze biometric data.[47]

The cost of health care will further decrease with IoT devices because IoT will assist in earlier diagnosis and preventative care.[48] By collecting patient data such as "blood sugar levels, temperature, exercise levels, food ingested, and even external information like ambient temperature or pollen counts" over a long period of time, emerging patterns can be detected and can subsequently be used to prevent disease.[49]

Another area in health care that IoT will impact is patient medication, which will also drive the cost of health care down.[50]

> Almost half of the population of the United States is prescribed some medication by a doctor, but on any given day 50 percent do not take their pills as prescribed, often with serious health consequences and at an onerous cost to society—the New England Healthcare Institute estimates that this nonadherence results in as much as $300 billion annually in unnecessary costs in the United States alone.[51]

GlowCap® is a "smart pill-bottle cap" that has a wireless chip connected to the Internet and will text or phone the patient to take his medication if he has forgotten.[52] Reminders to take medications are especially critical with patients who have received an organ transplant,

[44] *Id.* at 4.

[45] *Id.*

[46] Don DeLoach, *Internet of Things Part 9: Mobile Health and the Internet of Things*, INFOBRIGHT (Apr. 8, 2014), https://www.infobright.com/index.php/internet-things-part-9-mobile-health-internet-things/#.VPHmbvnF_QQ.

[47] NIEWOLNY, *supra* note 43, at 4.

[48] DeLoach, *supra* note 46.

[49] *Id.*

[50] ROSE, *supra* note 12, at 127, 130.

[51] *Id.* at 127–28.

[52] *Id.* at 128–29.

as well as patients who suffer from diabetes or HIV, because such conditions require a strict regimen.[53] "The use of GlowCap also cuts the cost of care for insurance companies in a number of ways, by reducing the number of doctor and hospital visits and admissions, and avoiding the costly complications that can come with uncontrolled diabetes, such as limb amputation."[54]

With respect to the health care industry, the privacy of patient health information and data ownership are important concerns.[55] For example, the "Health Insurance Portability and Accountability Act (HIPAA), [ ] defines 'health information' as 'any information, including genetic information, . . . that (1) [i]s created or received by a health care provider, health plan, . . . and . . . (2) [r]elates to the . . . physical or mental health or condition of an individual.' "[56] In other words, "HIPAA's definition would most likely *not* encompass fitness- or health-related—let alone other—potentially sensitive sensor data."[57] On the other hand, states may provide some protections for biometric-related data by passing statutory data-breach laws.[58]

D. *Energy*

"IoT deployments will generate large quantities of data that need to be processed and analyzed in real time . . . Processing large quantities of IoT data in real time will increase as a proportion of workloads of data centers, leaving providers facing new security, capacity and analytics challenges."[59] In other words, IoT will require more electricity to sustain an IoT environment of data centers and data storage.

[53] *Id.* at 130.

[54] *Id.*

[55] Stephanie Baum, *Healthcare's Application of the Internet of Things is Directly in the FTC's Crosshairs*, MedCity News (Jan 7. 2015, 3:33 PM), http://medcitynews.com/2015/01/ftc-heads-data-privacy-warning-connected-devices-offers-critical-reminder-consumer-health-space/. *See generally* Scott R. Peppet, *Regulating The Internet Of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85 (2014) (discussing the regulation of sensor-based technology); Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. Rev. 385 (2012) (discussing the privacy of health information).

[56] 45 C.F.R. § 160.103 (2014); Peppet, *supra* note 55, at 139.

[57] Peppet, *supra* note 55, at 139.

[58] *Id.*

[59] Press Release, Gartner, Gartner Says the Internet of Things Will Transform the Data Center (Mar. 19, 2014), http://www.gartner.com/newsroom/id/2684616.

In 2011, the cost of electricity used to run data centers and servers was about $7.5 billion in the United States.[60] With more and more interconnectivity and the addition of computation devices, the amount of electricity used will continue to rise.[61] "Google . . . uses enough energy to power 200,000 homes."[62]

"Cutting energy costs at data centers will ultimately come from powering facilities with renewable energy."[63] Some companies have already begun using renewable energy, such as solar power, to run their data centers.[64] For example, Apple's® data center in North Carolina is powered by solar power and a biogas fuel-storage system that stores solar power, so the facility can receive a steady supply of energy at all times.[65]

Energy consumption in an IoT world is also responsible for the development of "smart grids" comprised of "smart meters."[66] As more and more objects in buildings and homes become connected to IoT, consumers will require more energy to power all of these objects and appliances in their homes.[67]

> [B]uilding a smart grid means securing the future of energy supply for everyone in a rapidly growing population with a limited power production capacity. A smart grid reduces the losses, increases efficiency, optimizes the energy demand distribution[,] and also makes large-scale renewable energy such as solar and wind deployments a reality. With an aging infrastructure, the [current power] grid is facing severe challenges including recurring black-outs in major industrialized cities around the globe.[68]

Although many smart electrical meters (hereinafter "e-meters") can be found throughout homes today, the e-meters of IoT will be capable of sending and receiving information back and forth between

[60] JEREMY RIFKIN, THE ZERO MARGINAL COST SOCIETY 85 (2014).

[61] *Id.* at 84–85.

[62] *Id.* at 85.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] James F. Tracy, *Digital Electronic "Internet of Things"(IoT) and "Smart Grid Technologies" to Fully Eviscerate Privacy*, GLOBALRESEARCH (Feb. 2, 2015), http://www.globalresearch.ca/digital-electronic-internet-of-things-and-smart-grid-technologies-to-fully-eviscerate-privacy/5428595.

[67] *See id.*

[68] OLIVIER MONNIER, TEXAS INSTRUMENTS, A SMARTER GRID WITH THE INTERNET OF THINGS 1 (2013), http://www.ti.com/lit/ml/slyb214/slyb214.pdf.

the meter and the utility provider.[69] As a result, consumers will be able to monitor and adjust their energy behavior, thereby lowering their utility bills.[70] Eventually, smart flow meters will also be deployed in order to measure gas, water, and heat flow usage.[71]

"[T]he first step for the smart grid is to transition from mechanical meters to smart electronic meters to establish two-way communication between the meter and utility providers."[72] The substations at the city, state, and national levels will also eventually require connectivity in addition to the equipment therein, such as breakers and generators.[73] Thus, the equipment within a substation will also need the capability of two-way communication.[74]

Energy consumers will also be able to adjust their behavior by looking at real-time IoT devices that are installed within their home.[75] For example, the Ambient™ Energy Joule?, a small energy-monitoring device, can be positioned in areas of the home where people congregate often, such as the kitchen.[76] As such, a passerby can glance at the Energy Joule to see a current snapshot of energy consumption used in the home.[77] The Energy Joule? displays the energy price by glowing.[78] As a result of the Energy Joule?, which has already been deployed by several energy companies, people have been able to reduce their home's energy usage by twenty percent.[79]

E. *Local Government and Law Enforcement*

IoT will prove beneficial to cities and local law enforcement. For example, with smart parking technology, parking spaces throughout the city can be monitored for availability.[80] The structural health of buildings, bridges, and monuments could be monitored for vibrations and material conditions.[81] Noise levels and sound could be monitored

[69] *Id.* at 2–3.

[70] *Id.* at 3.

[71] *Id.* at 4.

[72] *Id.* at 6.

[73] *Id.* at 7.

[74] *Id.*

[75] *See* Rose, *supra* note 12, at 180.

[76] *Id.* at 180.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *50 Sensor Applications for a Smarter World*, Libelium, http://www.libelium.com/top_50_iot_sensor_applications_ranking (last visited Oct. 21, 2015).

[81] *Id.*

in real-time at bars and centralized social activities to build noise urban maps.[82] Vehicles and pedestrian traffic levels could be monitored for traffic congestion in order to optimize walking and driving routes.[83] With smart lighting, street lights can communicate with each other and adapt to different weather conditions.[84] As a final example, trash containers can be monitored in order to improve trash collection routes for waste management departments.[85]

IoT will also be beneficial for local law enforcement. For example, Yardarm Technologies has developed smart firearms, accessories, and sensor technology that can monitor and record data each time the weapon is discharged.[86] Some police departments, including Santa Cruz, California, and Carrollton, Texas, have started to test these devices, and the smart guns also contain either biometric fingerprint sensor technology on the triggers, or smart bracelets that use RFID microchips, such that only the assigned officer is able to discharge the weapon.[87]

Another IoT technology called ShotSpotter™ is able to determine when and where gunshots are fired in public using connected microphones that are installed throughout a city, town, or college campus.[88] As a result, police may be able to quickly determine an active shooter's location.[89] Although this technology is currently limited to outdoor gunfire, the ShotSpotter™ Company is working on technology that would be able to discern even a muffled gunfire sound that was discharged within a building or home.[90]

In terms of wearable IoT technology, there are body-worn cameras that could send video to the cloud in real-time and smart clothing that

[82] *Id.*

[83] *Id.*

[84] *Id.*; Shane Mitchell, et al., Cisco, The Internet of Everything for Cities 4 (2013), http://www.cisco.com/web/strategy/docs/gov/everything-for-cities.pdf. In 2013, Amsterdam implemented smart lighting technology that uses LED lighting. *Smart Light*, Amsterdam Smart City, http://amsterdamsmartcity.com/projects/detail/id/93/slug/smart-light (last visited Oct. 23, 2015). The street lights can be dimmed or adjusted for weather resulting in improved security and safety. *Id.*

[85] *50 Sensor Applications for a Smarter World*, *supra* note 80.

[86] Colin Neagle, *How the Internet of Things is Transforming Law Enforcement,* Network World (Nov. 3, 2014, 6:33 AM), http://www.networkworld.com/article/2842552/internet-of-things/how-the-internet-of-things-is-transforming-law-enforcement.html.

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *Id.*

can monitor the vital signs of officers and alert dispatchers.[91] Police departments have considered Google Glass™, but Google™ won't allow the use of Google Glass™ for facial recognition technology.[92] However, Google™ has recently invented a smart contact lens with an integrated camera on it.[93] The possibilities are endless and can include determining oncoming traffic, facial recognition, and infrared vision.[94]

Police K9 units could also benefit from IoT technology.[95] For example, wearable protective vests could monitor the dog's body temperature, and if the dog's temperature gets too high, the officer would be alerted on his smartphone.[96] Other technology would be able to automatically turn fans on in the officer's car and roll down windows upon detecting that a dog got too hot from sitting in the police car.[97]

F. *Environment*

IoT connected devices will also impact other areas, including water conservation, land management, agriculture, and rural wildfire fighting.[98] For example, with respect to water, municipalities can place IoT devices inside water pipes to detect problems, monitor the quality of tap water in cities, and conserve valuable water resources.[99] Streams could also be monitored for chemical leakage detection, such as waste from factories.[100]

National parks will particularly benefit from IoT connected devices because wildfire detection is currently performed manually, which is a labor-intensive and expensive task.[101] As a result, there is a

[91] *Id.*

[92] *Id.*

[93] Sebastian Anthony, *Google Invents Smart Contact Lens with Built-In Camera: Superhuman Terminator-Like Vision Here We Come*, EXTREME TECH (Apr. 15, 2014, 8:53 AM), http://www.extremetech.com/extreme/180571-google-invents-smart-contact-lens-with-built-in-camera-superhuman-terminator-like-vision-here-we-come.

[94] *Id.*

[95] Neagle, *supra* note 86.

[96] *Id.*

[97] *Id.*

[98] Martin LaMonica, *GreenBiz 101: What you need to know about the Internet of Things*, GREENBIZ (May 14, 2014, 7:30 AM), http://www.greenbiz.com/blog/2014/05/12/greenbiz-101-what-do-you-need-know-about-internet-things; Paul Pounds & Surya Singh, *Samara: Biologically Inspired Self-Deploying Sensor Networks*, IEEE POTENTIALS, Mar./Apr. 2015, Vol. 34 No. 2, at 10.

[99] LaMonica, *supra* note 98; *50 Sensors for a Smarter World*, *supra* note 80.

[100] *50 Sensors for a Smarter World*, *supra* note 80.

[101] Pounds & Singh, *supra* note 98, at 10.

need to deploy scalable IoT devices within forests for automatic wildfire detection, monitoring, and identifying high-risk areas at a low cost.[102]

Other environmental uses for IoT connected devices include the monitoring of combustion gases and carbon dioxide emissions produced by factories and cars, as well as toxic gases emitted from farms.[103] Moreover, snow levels could be measured by IoT devices in real-time to determine the quality of ski trails and assist in the prevention of avalanches.[104] Finally, IoT connected devices could contribute to early earthquake detection.[105]

III. The Need for Standards

"Wherever there are rival standards—as purchasers of junked consumer electronics standards like Betamax and HD-DVD know—there are winners, and there are losers."[106] In other words, when there is competition in the consumer market between competing standards, generally one product or standard ends up going by the wayside. As such, IoT standards will likely impact consumers, specifically if competing standards are unable to be negotiated and agreed upon.[107] A standards war could also slow down the progress of IoT.[108] Thus, IoT standards are critical to the success and expansion of IoT devices and networks.

The standards that are involved with wearable devices include Wi-Fi, 2G/3G/4G, Near Field Communication ("NFC"), and Bluetooth™.[109] With respect to smart home appliances, the standards include X10, Insteon, ZibBee, and Z-Wave.[110] Vehicles are connected

[102] *Id.* at 10–11.

[103] *50 Sensors for a Smarter World*, *supra* note 80.

[104] *Id.*

[105] *Id.*

[106] Mark Anderson, *Is There Any way to Avoid Standards Wars in the Emerging Internet of Things?*, IEEE Spectrum (Aug. 4, 2014, 9:00 PM GMT), http://spectrum.ieee.org/tech-talk/consumer-electronics/standards/is-there-any-way-to-avoid-standards-wars-in-the-emerging-internet-of-things.

[107] *Id.*

[108] Patrick Dehahn, *Could The Internet Of Things Be Overhyped?*, Associations Now (Nov. 19, 2014), http://associationsnow.com/2014/11/internet-things-overhyped/.

[109] Karen Bartleson, *The Internet of Things Is A Standards Thing*, Electronic Design (May 7, 2014), http://electronicdesign.com/communications/internet-things-standards-thing.

[110] *Id.*

using standards such as IEEE 1901, IEEE 2030, V2V, and STMF.[111] Some of these standards were created by private companies, the U.S. Government, and various federal agencies.[112]

Half a dozen or more private organizations have been created to come up with and reconcile standards with respect to IoT.[113] For example, the "AllSeen Alliance" was created in December 2013 and chartered by Qualcomm®, Cisco Systems®, Panasonic®, and other consumer electronics vendors.[114] "AllSeen's aim is to give home and business devices that use different operating systems and network protocols a way to find and coordinate with each other."[115]

The "Open Interconnect Consortium" ("OIC") was charted in July 2014 by Intel®, Samsung Electronics®, and Dell®.[116] Hewlett Packard® ("HP") and Lenovo® have also recently joined, and the organization is working on "a series of specifications to help devices find each other and work together."[117]

Various companies chartered the "Thread Group," including ARM Holdings, Samsung®, and Google's Nest Labs™ (a thermostat-and-smoke-alarm acquisition).[118] Thread Group has been working on a mesh networking protocol aimed at low-power devices in homes.[119] The organization's protocol currently works on a certain type of microchip that already exists in the market and works on IPv6.[120]

[111] *Id.*

[112] *Id.*

[113] Stephen Lawson, *Intel-Backed OIC Advances in Fast-Moving IoT Standards Race*, TECHWORLD (Jan. 15, 2015), http://www.techworld.com/news/networking/intel-backed-oic-advances-fast-moving-iot-standards-race-3594070/ [hereinafter Lawson, *Intel-Backed OIC Advances*].

[114] Stephen Lawson, *IoT Groups are Like an Orchestra Tuning Up: The Music Starts in 2016*, COMPUTERWORLD UK (Dec. 24, 2014), http://www.computerworlduk.com/news/networking/3592131/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016/ [hereinafter Lawson, *IoT Groups are Like an Orchestra Tuning Up*].

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.* It is important to note that IPv6 extends the current IPv4 from 32 bits to 128 bits per IP address, which will allow for billions of IoT devices to have individual IP addresses and connect to the Internet. Chris Poulin, *The Importance of IPv6 and the Internet of Things*, IBM: SECURITY INTELLIGENCE (Dec. 23, 2014), http://securityintelligence.com/the-importance-of-ipv6-and-the-internet-of-things/#.VQ2jGI7F_QQ.

The "Industrial Internet Consortium" (hereinafter "the Consortium") is comprised of General Electric®, Cisco Systems®, IBM®, Intel®, AT&T®, Microsoft®, Samsung®, and Huawei Technologies.[121] The group's intention is to focus on IoT at an enterprise level and not set standards.[122] The Consortium will work with other organizations to help define requirements for standards, develop test beds, and ensure that IoT technologies work together across multiple business sectors.[123]

The Institute of Electrical and Electronics Engineers (hereinafter "IEEE") comprises a majority of engineers who work with vendors.[124] IEEE has been working on a standard for an architectural framework for IoT.[125]

These organizations will also have to consider security, privacy, and efficiency, in addition to other concerns with respect to coming up with IoT standards.[126] Whether the U.S. government will need to intervene and impose an IoT standard is yet to be seen. "When technology takes a big leap forward, policy-makers are usually left behind."[127] However, "[t]he market is typically remarkably adept at deciding between competing standards without government intervention—like what happened in the video standard wars between HD[-]DVD and Blu-ray or Betamax and VHS."[128]

IV. Legal Considerations

IoT will likely impact various areas of the law. Some of these areas include: mergers and acquisitions, which will also implicate anti-trust laws; consumer protection, data privacy, and security; intellectual property; and federal regulations that govern the bandwidth spectrum.

[121] Lawson, *IoT Groups are Like an Orchestra Tuning Up*, *supra* note 114.

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] Oleg Logvinnov, *Standard for an Architectural Framework for the Internet of Things (IoT)*, IEEE Standards Ass'n 5, http://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf (last visited Mar. 21, 2015).

[126] Anderson, *supra* note 106.

[127] *Id.*

[128] Aaron Sankin, *The One Problem the Internet of Things Hasn't Solved*, The Kernel (Jan. 4, 2015), http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11298/internet-of-things-regulation-policy/.

A. *Mergers and Acquisitions*

With about one trillion devices expected to be connected by 2022, the opportunities for innovation are endless.[129] As a result of the IoT growth, there will be an increase in mergers and acquisition activity as companies try to capitalize on the IoT market.[130] "The biggest profit potential of the IoT may not be in the things themselves, but in the data they can provide and additional services that they can enable."[131]

For example, there will be merger and acquisition opportunities in advertising services because "our devices know a lot about us, including where we go, whom we interact with, what we e-mail and text message about, and what products and services we search for."[132] In addition, usage information services will provide another opportunity because "[d]evices can report metrics to manufacturers about which features are being used, and which are not. The data can then be analyzed to improve the products and ultimately sell more of them."[133] Some of the other services for profit include cost control, such as collecting data about energy usage, in addition to mobile security and public safety.[134]

Suppliers will also have opportunities to expand their offerings in order to compete.[135] "Examples abound in the semiconductor and embedded software space where consolidation may occur."[136] Hackers are capable of adapting quickly, and as a result, suppliers will need the expertise of those who can assist in the development of security technology suppliers as opposed to suppliers building from scratch.[137]

Many of the top software and semiconductor companies are currently sitting on large amounts of cash, which will be used in their acquisitions.[138] Microsoft®, Google™, Samsung®, Oracle®, and In-

[129] Brent Lorenz, *The Explosion of the IoT for Business: How the Internet of Things Will Spur Buyouts*, The Institute (Mar. 17, 2014), http://theinstitute.ieee.org/ieee-roundup/opinions/ieee-roundup/the-explosion-of-the-iot-for-business.

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] *Id.*

tel®, have billions of dollars to acquire other companies.[139] Google™ acquired Nest Labs™, a manufacturer of smart thermostats and smoke alarms back in January 2014 for $3.2 billion.[140] Cisco® also bought Tail-F Systems® for $175 million to assist with Cisco's® network management tools for IoT.[141] Facebook® also bought Oculus®, a virtual reality company in 2014, while Samsung® purchased SmartThings® in 2014, which allows people to "sync their devices and IoT gadgets with a standalone smartphone application."[142]

Antitrust concerns will likely arise from the increase in merger and acquisition activity, especially where the buying and selling companies are in the same market.[143] Moreover,

> Antitrust risks may arise with IOT products sold using restrictive sales and distribution methods, bundled sales policies, price discrimination, and other nonprice restraints that are normally analyzed under the rule of reason (or Section 2 standards where the supplier has a significant market position). [Thus] [a] range of factual issues may arise with the early-stage IOT in defining relevant product and geographic markets for rule of reason analysis or in showing direct evidence of anticompetitive effects that may obviate the need for relevant market analysis.[144]

B. *Consumer Protection, Data Privacy, and Security*

In January 2015, the Federal Trade Commission (hereinafter "FTC") released a report addressing the concerns of protecting consumers' privacy and security.[145] The report was partially based on pub-

[139] *Id.* ("Another good predictor of future acquisitions is past history. In the last two years, the semiconductor and software companies making the most acquisitions include Google with 42, Intel with 21, Samsung with 20, Oracle with 19, and IBM with 15.")

[140] *Top 10 Mergers and Acquisitions in The Internet of Things Space 2014*, COMPUTER TECHNICAL SUPPORT IN USA (Sept. 3, 2014), https://computertechsupportinus.wordpress.com/2014/09/03/top-10-mergers-and-acquisitions-in-the-internet-of-things-space-2014-2/.

[141] *Id.*

[142] *Id.*; Junko Yoshida, *Top 2014 Acquisitions that Advanced the Internet of Things*, EE TIMES (Dec. 11, 2014, 9:30 AM), http://www.eetimes.com/document.asp?doc_id=1324935.

[143] *Cf.* Gregory G. Wrobel, *Connecting Antitrust Standards to the Internet of Things*, ANTITRUST MAG., Fall 2014, at 64–66 (stating "[m]ost mergers related to the IOT have been vertical rather than horizontal, and antitrust risks have been minimal for early movers in such transactions" and that sharing data outputs containing sensitive personal or business information with rival suppliers may created unwarranted antitrust risks of horizontal collusion).

[144] *Id.*

[145] *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, FED. TRADE COMM'N (Jan. 27, 2015), https://www.ftc.gov

lic comments submitted to the FTC, in addition to industry representatives, consumer advocates, leading technologists, and academics joining together to participate in FTC's IoT workshop on November 19, 2013.[146] Due to the nature of networked devices, security was one of the main topics, and the FTC report made the following recommendations to companies that are manufacturing IoT devices:

- "[B]uild security into devices at the beginning, rather than as an afterthought;"[147]
- Train employees about the importance of security, and ensure that security is managed at an appropriate level in the organization;[148]
- Ensure that when outside service providers are hired, that those providers are capable of maintaining reasonable security and provide reasonable oversight of the providers;[149]
- When a security risk is identified, consider a "defense-in-depth" strategy, whereby multiple layers of security may be used to defend against a particular risk;[150]
- Consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on the network;[151]
- Monitor connected devices throughout their expected life cycle and where feasible, provide security patches to cover known risks.[152]

The report also makes recommendations about data minimization in terms of the amount of consumer data collected, as well as the length of retention.[153] "[C]ompanies can choose to collect no data, data limited to the categories required to provide the service offered by the device, less sensitive data[,] or choose to de-identify the data collected."[154] The report also recommends that "companies notify consumers and give them choices about how their information will be

/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices; *see generally* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[146] *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD at i (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[147] *Id.* at iii.

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *FTC Report on the Internet of Things*, supra note 145.

used, particularly when the data collection is beyond consumers' reasonable expectations."[155]

At the 2015 Consumer Electronic Show ("CES"), Ruby Zefo, the chief privacy and security counsel for Intel® said, "Consumer interest in privacy issues may be a bigger factor for companies than fear of government backlash."[156] Zefo continued, "If the first generation of a product has security and privacy flaws, the customer will be less likely to trust the second version."[157] "'The law is low-hanging fruit' compared with the customer's expectation . . . , 'which may be much higher than the law requires.'"[158]

C. *Intellectual Property*

Issues related to intellectual property could hinder the progress of IoT because industry leaders want to protect their patents and trade secrets.[159] As was mentioned in Part III of this article, there is a need for standards.[160] However, if this standardizing technology becomes patented, "third-party users could be forced to either infringe on these patents, or to pay exorbitant license fees."[161] Such consequences would result in a substantial obstacle to IoT.[162]

"In many other technology industries, the owners of standard essential patents (SEPs) are obligated to offer non-exclusive licenses to prospective licensees on fair, reasonable, and nondiscriminatory (FRAND) terms in order to avoid this problem."[163] On the other hand, one drawback to FRAND is that the "[p]arties cannot always agree

[155] *Id.*

[156] Tom Risen, *The Internet of Things: FTC Chairwoman Calls for Tech Privacy at CES*, U.S. NEWS & WORLD REPORT (Jan. 6, 2015, 6:45 PM), http://www.usnews.com/news/articles/2015/01/06/the-internet-of-things-ftc-chairwoman-calls-for-tech-privacy-at-ces.

[157] *Id.*

[158] *Id.*

[159] John F. O'Rourke & Patrick Soon, *The Internet of Things and the Issue of IP Rights (Part 1)*, INSIDE COUNSEL (Mar. 28, 2014), http://www.insidecounsel.com/2014/03/28/the-internet-of-things-and-the-issue-of-ip-rights.

[160] *See* discussion *supra* Part III.

[161] John F. O'Rourke & Patrick Soon, *The Internet of Things and the Issue of IP Rights (Part 2)*, INSIDE COUNSEL http://www.insidecounsel.com/2014/04/15/the-internet-of-things-and-the-issue-of-ip-rights?page=2.

[162] *Id.*

[163] *Id.*

what terms are fair and reasonable, particularly as regards royalty rates."[164]

The eligibility of software patents has also gained more attention since the *Alice v. CLS Bank* decision.[165] The Supreme Court decision impacted software patents because the market appeared to slow down in the months following the decision.[166] However, by the end of the fourth quarter of 2014, the market appeared to rebound as a result of a significant number of software patents being bought and sold during that period.[167]

It is unclear what the future impact of the *Alice* decision will be on software patents with respect to IoT.[168] However, "[g]iven the continual march toward more computerization in nearly every industry and the public policy favoring the promotion of innovation, it is hard to imagine a day when software processes are held by the Supreme Court to be, *per se*, patent ineligible."[169]

The mergers and acquisitions activity will also have an impact on intellectual property issues, such as licensing agreements.[170] Even if the software technology used is "open source,"[171] such licensing agreements may cause problems when companies attempt to incorporate this open source software into their business.[172]

[164] Paul England & Kathleen Fox Murphy, *Patent Issues and the Internet of Things*, TAYLORWESSING (Feb. 2014), http://www.taylorwessing.com/download/article_patent_iot.html.

[165] Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347 (2014); Gene Quinn, *The Race to Dominate the Internet of Things*, IP WATCHDOG (Feb. 15, 2015), http://www.ipwatchdog.com/2015/02/15/the-race-to-dominate-the-internet-of-things/id=54698/.

[166] Quinn, *supra* note 165.

[167] *Id.*

[168] James M. Lennon, *A Peek at the Past to Predict the Uncertain Future of Software Patent Eligibility*, IC INSIDE COUNSEL (Mar. 3, 2015), http://www.insidecounsel.com/2015/03/03/a-peek-at-the-past-to-predict-the-uncertain-future.

[169] *Id.*

[170] *See* Jeffrey C. Johnson & Michelle Pham, *Tips for Dealing with Open Source Issues in M&A*, LAW 360 (Mar. 3, 2015, 10:40 AM), http://www.law360.com/articles/622748/tips-for-dealing-with-open-source-issues-in-m-a.

[171] OPEN SOURCE INITIATIVE, http://opensource.org/ ("Open source software is software that can be freely used, changed, and shared (in modified or unmodified form) by anyone. Open source software is made by many people, and distributed under licenses that comply with the Open Source Definition.")

[172] Johnson & Pham, *supra* note 170.

> For example, one common type of open source license, known as a "viral" license, requires any company incorporating, modifying or otherwise using the open source software to make its source code generally available to the public (which could potentially allow competitors access to what would otherwise be proprietary information) and to license their software to all third parties under the same terms as the open source license.[173]

As a result, the bidding company will often put a provision in the transaction agreement that requires the target company to represent that it is not using open source software distributed under a viral licensing model in any of its products.[174] The due diligence phase may lead to substantial delays upon the discovery of noncompliant open source code "due to [the] renewed negotiation of a target company's valuation or the demand for the target company to take measures to be compliant (e.g., removing infringing code and substituting it with new, non-infringing code)."[175]

D. *Bandwidth Spectrum*

The Federal Communications Commission (hereinafter "FCC") may be busy dealing with problems in the near future as a result of the increased use of mobile devices.[176] Because IoT devices will need to be connected to the Internet (most likely wirelessly), the FCC will need to free up more space on the broadband spectrum.[177]

Currently, most IoT devices operate in unlicensed radio frequencies, including the industrial, scientific, and medical ("ISM") bands.[178]

> The sub-125 kilohertz (kHz) for video surveillance and access control systems; 13.56 megahertz (MHz) for near-field communications (NFC) to support mobile payments; and 900 MHz for Electronic Product Code (EPC), one of the industrial standards for global Radio Frequency Identification (RFID) usage, just to name a few. And they make their critical connections using a range of different (and sometimes competing) wireless connectivity standards, such as Bluetooth, ZigBee, Z-Wave, and Wi-Fi, all of which were designed to work in unlicensed spectrum.[179]

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] Paul Barbagallo, *As 'Internet of Things' Evolves, FCC's Spectrum Strategy Will Be Put to the Test*, BLOOMBERG BNA (Nov. 19, 2014), http://www.bna.com/internet-things-evolves-n17179912070/.

[177] *Id.*

[178] *Id.*

[179] *Id.*

According to Kevin Ashton,[180] "There are no spectrum bottlenecks for dedicated IoT systems yet, but we are seeing Wi-Fi services get maxed out, as there are only so many channels you can cram into the available spectrum."[181] Ashton thinks that the FCC "should make almost all global spectrum unlicensed and subject to ISM-band-type rules about sharing, with exceptions for emergency and security systems," resulting in a huge paradigm shift.[182]

Regardless of the FCC's ultimate resolution to the problem, the FCC has begun discussing IoT issues.[183] However, with the recent net neutrality decision, the FCC can regulate Internet Service Providers ("ISPs") under Title II of the Telecommunications Act,[184] but it is yet to be seen how the new ruling will impact IoT.[185]

V. Conclusion

As has been discussed, IoT is going to have a significant impact on manufacturing, automobiles, health care, energy, local government and law enforcement, and environmental controls. Early detection and monitoring will drive costs down and will allow for a quicker (if not an automatic) response time to correct issues that arise.

In addition to the impact on various industries, the need for standardization may hinder the advancement of IoT implementation due to competing markets. At the moment, it is unclear whether these necessary standards will be determined as a result of the consumer market, technology industry leaders and private organizations, or federal regulation. Based on past trends, "[t]he law has consistently failed to keep up with technology. Issues like cyberbullying, data protection, and even Internet regulation had all reached a pandemic level before the governments and courts of the world caught up."[186]

[180] Kellmereit & Obodovski *supra* note 3.

[181] Barbagallo, *supra* note 176.

[182] *Id.*

[183] *Id.*

[184] *See* Jacob Kastrenakes, *FCC Votes to Protect the Internet with Title II Regulation*, The Verge (Feb. 26, 2015), http://www.theverge.com/2015/2/26/8114265/fcc-ruling-net-neutrality-victory-internet-title-ii.

[185] Monica Alleven, *Net neutrality: Long-term implications loom for Internet of Things*, FierceWirelessTech (Feb. 26, 2015), http://www.fiercewireless.com/tech/story/net-neutrality-long-term-implications-loom-internet-things/2015-02-26.

[186] Daniel Price, *The Internet of Things—Beyond the Long Arm of the Law?*, CloudTweaks (Jan. 28, 2015), http://cloudtweaks.com/2015/01/internet-things-beyond-long-arm-law/.

Finally, IoT will influence legal issues relating to merger and acquisition activity, consumer protection, data privacy and security, intellectual property, and the bandwidth spectrum regulated by the FCC. Finally, an example of IoT and its potential interaction with a lawyer's daily activities, which we may see in the not so distant future, is the following:

> A client, needing to reschedule an appointment to an early morning time, late the night before notifies the sleeping lawyer's calendar app via e-mail. The calendar relays the information to the lawyer's computerized alarm clock. The alarm clock checks the weather and traffic conditions, calculates how long it will take the lawyer to get to the office, and resets the wake-up time accordingly. It also resets the coffee makers at home and at the office, as well as the office thermostat, so that everyone will be comfy at the meeting.[187]

[187] Daniel E. Harmon, *The IoT & Law Practice: How Will the Internet of Things Impact You This Year?*, 32 No. 8 Law PC 1, Jan. 15, 2015, at 1.