Impact of the internet of things

The Internet of Things has the ability to interconnect the world in unprecedented way and is considered by many to be the next step in the evolution of the internet. The creation of the internet had a significant impact on the way in which society accesses and uses information. For the first time in history there was virtually unlimited access to information from all over the world at any time of the day. Information that used to take weeks or months to gather and analyze was now just a click away enabling people from all over the world to interact and collaborate at unprecedented speeds and significantly reduced costs. People were more connected to each other than ever before sharing knowledge and experiences faster than any time in history. Soon, businesses started leveraging the power of the internet to connect to devices or, things, as well as other people improving productivity and efficiency through improved data processing abilities offered by the internet. The Internet of Things, or IoT for short, is a term coined by Kevin Ashton of the Massachusetts Institute of Technology in 2009 which describes the emergence of things rather than people using the internet to exchange information (Hassan, Khan, & Madani, 2018).

The Internet of Things (IoT) goes beyond the standard home or office computer to include virtually anything capable of accessing the internet through various network technologies. The Internet of Things also encompasses and incorporates many different types of communications and networking technologies such as Bluetooth, Radio Frequency Identification, Bar Code, 4G and 5G cellular networks, and Quick Response Code scanning. The IoT has grown significantly over the years and has become almost seamlessly integrated into society to a point where its no longer noticed by

the average person. Cellular phones, automobiles, critical infrastructure controls, health care, manufacturing, and logistics are just a few of the areas which not only benefit from the IoT but also help to drive its innovation. Companies are pouring millions of dollars into developing products and services for use on the IoT which are intended to improve everything from manufacturing efficiency to quality of life for everyone.

While the IoT is poised to improve just about everything imaginable, it also has some inherent cyber-security risks. While all of these devices on the Internet of Things are collecting and aggregating colossal amounts of data, who is using it and for what purpose are they using it? Are the devices sharing data securely? What standard, if any, is the IoT required to meet for data security? What is being done to secure data ensuring that it is only used for its intended purpose? Who should develop policies that determine appropriate use of data? What level of involvement should the Government have?

Think about all of the smart devices in use today such as smart phones, fitness trackers, home automation devices, smart home appliances, home security systems, infrastructure monitoring devices, weather monitoring devices, and the list goes on and on. All of these things are considered smart because of the way in which they sense, communicate, and acquire data. The average smart phone has a myriad of sensors including an accelerometer for sensing speed, a gravity sensor to help it determine which way is up, a gyroscope that helps applications such as Global Positioning System (GPS), a light sensor, a proximity sensor, a temperature sensor, and motion sensor just to name a few. All of these sensors allow the smart phone

to collect all kinds of data about its environment and how its being used. That data is then transmitted on the internet via either the cellular network or a wireless access point where the data is collected and analyzed by other things. Many people immediately think of advertising, which is certainly one use of the data, there are many other ways in which the data collected can be used to assist with everyday life. Fitness bands for example have been used extensively over the last few years in conjunction with fitness applications to help people track and manage their health more effectively by tracking heart rate, sleep quality, stress levels, and activity level. Now consider the impact of the fitness band being able to share that information with an individual's health care provider. An individual's doctor could have a better understanding of a patients normal so that abnormal things could be identified quicker. The heart rate monitors which are imbedded in most fitness devices could also potentially diagnose symptoms of a heart attack much earlier than before and report that information to the person wearing the band as well as notify a medical provider or emergency services automatically. Automotive technologies which enable vehicles to use hundreds of sensors to learn driving habits, avoid collisions, and automatically report problems are making automobiles safer.

Technology in the internet of things includes many different types of computing and networking technologies. Bluetooth, for example, enables devices to connect with each other in close proximity in order to share information. Wired and wireless connections to the internet allow connected devices to communicate worldwide. Many logistics company's utilize Radio Frequency Identification (RFID) to track and update shipments and inventory

automatically. This technology enables large companies such as Amazon or Wal-Mart to instantly see the status of a shipment or a product as it moves through the logistics chain. When a product is scanned at the check out line it sets off a chain of events where several things communicate with each other on the internet in order to get a replacement item delivered to the store. That data can also be used to determine the demand for specific products in a region which helps stores ensure that they have the right products in the right stores at the right times which equates to better sales and happier customers. RFID is used in a wide range of applications today from managing inventory at a department store to tracking whales in the ocean to Identify Friend or Foe (IFF) on military aircraft.

Another popular technology that bridges the gap between connected devices and things that cannot connect to the internet directly is the Quick Response Code or QR Code. Originally developed by Toyota to assist in the manufacturing process, QR Code uses an optical image to identify an object. QR codes contain small amounts of data such as product information or a link to a web site containing information about the item it is attached to (Downing 2013). QR Codes allow things that are not able to communicate with a network by themselves to still provide information to things through the use of a QR code scanner.

Bluetooth Low-Energy (BLE) is another technology currently utilized in some applications such as cell phones but is also being investigated by the healthcare industry for its use in biomonitoring devices in the human body. Body Sensor Networks (BSN) use Bluetooth Low Energy in implantable biomonitoring devices means that the device can sense and transmit data

about the specific function it is monitoring. Paired with a device, like a cellphone, running a mobile gateway it can connect to the IoT cloud allowing a healthcare provider to monitor and track a patient's vital statistics wirelessly. Patients with persistent or recurring medical problems like, heart disease or diabetes could link their implanted devices to an application which would compare vitals to specified parameters. If those parameters are not met or exceeded then the device could alert the individual long before the physical symptoms are felt. Sort of an early warning system for the body (Wu, Wu, Redoute, & Yuce, 2017, p. 11413-11414).

All of this data which is collected and analyzed by the internet of things must be important to someone, but who? And Why? The date collected by the internet of things is also worth a lot of money to companies developing products for the IoT. In an article by Riaan Rudman and Natasha Sexton they write, " by 2020 there will be over 26 billion connected devices, while Cisco Consulting Services says that by 2022 the Internet of Things could generate $4. 6 trillion in value". Many companies like Google, Apple, IBM, Samsung, and General Electric use the data to create or improve products or experiences to enhance a particular area of life such as creating the Smart Home. Innovations in technology and products for the IoT are allowing many homes to become automated or " Smart Homes" which, Forbes has forecasted to generate $7. 8 billion by 2019 (Wolf 2014). Some of these products include intelligent thermostats that can make temperature adjustments based on environmental conditions, lighting systems that can detect whether or not people are in the room and turn lights on or off, and home security systems that can alert emergency services and the

homeowners of break-ins. Many of these devices are also capable of monitoring the environment, learning user's preferences, and anticipating user needs making Smart Home systems nearly fully automated and seamlessly integrated into the home. Ultimately, the use of Smart Home technology could result in energy usage reductions and cost savings for homeowners.

The same technology that makes Smart Homes more efficient can also be applied to city management systems enabling city managers to move towards Smarter Cities. Remote monitoring and maintenance via the internet is already common in much of the infrastructure. Programmable Logic Controllers (PLC) are devices that can maintain control of a specific function based on pre-designated specifications. In the not so distant past, these PLC's required regular monitoring and human interaction in order to analyze the data and make adjustments based on other environmental variables. Now, in the IoT, a system or application can monitor most if not all of the environmental variables in a single facility and make automatic adjustments based on information received from hundreds of sensors throughout the facility. For example, a hydroelectric dam operator used to monitor a bank of sensors that would tell them how much power generation was occurring and how much power was being used by the serviced area. They would then take that data and adjust the flow of water through the dam to either speed up or slow down the generators. With the IoT enabling those devices to collect and analyze data and make adjustments based on the data, a single operator can monitor multiple dams across a region reducing the amount of labor needed to operate those facilities.

Developments in the IoT have also impacted healthcare services and, as new technologies are proven, will continue to be increasingly integrated into healthcare facilities such as hospitals and private practices. Development of automated patient monitoring systems, Body Sensor Networks (BSN), and Wireless Body Area Networks, could drastically change the way and the speed at which healthcare data is collected and healthcare services are rendered. Theoretically a patient with a Bluetooth Low Energey enabled biomonitoring device could arrive in any hospital emergency room, the device could authenticate to the network which could then retrieve the necessary medical records ensuring the staff has access to critical medical data instantaneously.

Unfortunately, the same systems that allow remote users to monitor automated facilities and systems also have inherent risks associated with them, namely security. Since the IoT is still in its infancy there are several issues that can affect the ability to secure the heterogeneous devices and applications that make up the IoT. For starters, the sheer number of different types devices connected to the IoT presents a challenge. Each device and application has unique qualities that in turn present unique vulnerabilities which hackers can exploit causing severe damage. In their article Yang Lu and Li Da Xu (2018) explain how quickly the number of connected devices per person has increased during the last eight years from less than one device per person in 2010 to two devices in 2018 and is expected to continue to grow to almost seven devices per person by the year 2020. There was also 48% increase in global cyber-attacks from 2013-2014 (Wadhwa, 2015). Cyber-attacks are estimated to cost an average of $2. 7

million per event however, cost is not the only danger associated with cyber-attacks on devices connected to the IoT, physical safety of people is also a major concern.

In 2015, Chrysler recalled 1. 4 million vehicles after Wired magazine exposed a vulnerability in the Udrive system used by the vehicles in which the vehicle could be hi-jacked while the driver was at the wheel leaving them without physical control of the vehicle they were driving. Although Chrysler knew about the possible vulnerability there were no regulations requiring Chrysler to act nor was there any motivation to do so until exposed by the media (Wadwha, 2015). Attacks on medical devices that use the IoT could also be detrimental to the individual connected to the device. If an attacker used a Man in The Middle attack to alter or steal sensitive data traversing between the medical device and the server storing the data the results could range from stolen information to life threatening interference. In an article written by Kuo-hui Yeh (2016, p. 10288-10299), he discusses several security concerns including authentication, communications security, and data privacy for which he provides some concepts and solutions for addressing those concerns.

The question about data confidentiality does not stop at cyber attacks or criminal behavior. There are many other legal issues involving privacy and the use of data collected by the Internet of Things. The data aggregated by all of the seemingly innocuous sensors imbedded in everything creates hundreds of gigabytes about an individual daily. Many of the companies that offer the devices and applications for use on the IoT put statements in their privacy policies that state the data collected by the device or the application

is property of the company and may be used for various reasons including improving the user experience, tailoring advertising, and even sold to other companies for similar purposes. Legal experts argue that the data belongs to the user regardless of the method by which it is collected and should not be used unless explicitly authorized by the user. Fitness bands for example collect a substantial amount of health data about its user and sends that data to an application created by the device manufacturer. Is it possible that the data collected by your fitness band about an individual's overall health be sold to a health insurance provider without consent to determine health or life insurance premiums or possibly be denied insurance based on the data collected? Worse yet is the idea that data collected by Body Sensor Networks could also be used in discriminatory practices by insurance providers.

Progressive Insurances' Snapshot tool is a device or application, depending on the vehicle, that collects information from your vehicles sensors and transmits it via the Snapshot Application back to the insurer. Data collected can include vehicle speed, location, brake pressure application, and even cell phone usage. This data is then analyzed by the insurer when calculating insurance premiums. Progressive's privacy policy concerning the snapshot tool states that it will not use the data while resolving insurance claims, it will turn over the data if required by law during accident investigations. Data collection and privacy challenges extend well beyond adults and can impact children as well. Consider the amount of electronic devices kids have access to in today's society. Computers, game consoles, mobile gaming applications, tablet PC's, baby monitors, and so on. Most gaming consoles

and tablet computers have cameras and listening devices integrated into them which could potentially record everything within its field of view or range of hearing. Smart toys are becoming cheaper and easier to obtain and have little to no security features to safeguard the information collected. In his article, Scott Peppet sums up the legal challenges by stating, “ These are the real challenges of the Internet of Things: what information do these devices collect, how might that information be used, and what-if any-real choice does consumers have about such data?” (Peppet, 2014). Like most emerging technologies, the lack of understanding makes it difficult at best to develop new legal policies and legislation or apply existing policies to the new technology.

Experts on the Internet of Things like Bruce Schneier of Harvard University and Kevin Fu of Virta labs believe that the federal government should be more involved with regulating the Internet of Things through legislation. They feel that the IoT’s ability to cause substantial damage in the physical world like the problem revealed in Chrysler’s UDrive system, is unlike any previous cyber-security threats and warrants government regulation to protect consumers (James, 2016). Although the vulnerabilities and threats to consumers of IoT devices and applications has been thoroughly documented since near the beginning of the IoT, the government is slow to respond to the threat. Only recently has Congress introduced legislation concerning cyber-security and the Internet of Things devices. Unfortunately, the proposed legislation only pertains to IoT in the government.

The Internet of Things Cyber-security Improvement Act of 2017 focuses on IoT devices and applications utilized by the government and not on general

consumer electronics (Text – S. 1691 – 115th Congress (2017-2018): Internet of Things (IoT) Cybersecurity Improvement Act of 2017," 2017). California's Governor signed SB-327, the first Internet of Things law on September 28 th , 2018. This law which will take effect in 2020 will require manufacturer's of IoT devices to equip the devices with security features appropriate to the level and type of information collected by the device (" Bill Text – SB-327 Information privacy: connected devices," 2018). Neither of these laws does anything to address the privacy, data ownership, and use of data challenges presented by the Internet of Things. Current laws regarding information handling and data security require companies to notify consumers that their data may have been compromised in the event of a data breach. As of March 2018, all fifty states have enacted some type of data breach notification laws. Additional challenges presented by the Internet of Things include regulatory concerns. Unfortunately, due to the rapid growth of the IoT and the institutional and capacity gap between the government and the private sector there are still underdeveloped policies and regulatory frameworks for the Internet of Things. Creating technical and legal standards for the IoT will be challenging at best due to the heterogenous nature of the devices and applications that make up the IoT. The current lack of technical standards will affect how all of the different things are operated and secured, further increasing the cybersecurity and integration challenges associate with the IoT. In their article, " Internet of Things In Industries: A Survey (2014)", Xu, He, and Li state, " The success of IoT depends on standardization, which provides interoperability, compatibility, reliability, and effective operations on a global scale".

The Internet of Things has the potential to have significant implications, both positive and negative, around the globe. For starters, the infrastructure is going to have to grow in order to meet the demands of the billions of added devices all transmitting packets across the internet. Growing infrastructure can bring new jobs which will have positive impacts on local economies. Building automation can make residential and commercial buildings more efficient thereby reducing energy consumption. The Internet of Things will also have significant impacts on businesses and their use of human resources. Automation has already consumed a large number of jobs that used to be done by people. Jobs that were previously handled by people that require no collaboration or specialized skill are prime candidates for future automation. The Internet of Things will require employees to take on new roles or specialized skill (Kranz, 2017 p. 125-127). Businesses will have to retrain or replace its workforce as needed in order to operate successfully with the IoT. Finally, the IoT has created a whole market for businesses through developing technology, devices, security measures, and applications for the Internet of Things. By 2020 the Internet of Things is projected to be a $4. 6 trillion industry (Rudman & Sexton, 2016).

In conclusion, the internet has connected people to each other in an unprecedented way enabling better collaboration, improved efficiency, and greater access to information. The Internet of Things is considered to be the next step in the evolution of the internet in which more things will use the internet than people. The Internet of Things is basically defined as a network of things or devices connecting to each other using the internet to share data. The Internet of Things goes beyond traditional computing devices to

include any devices that are enabled to communicate over the internet such as smart appliances, cell phones, medical devices, and infrastructure management devices to name a few. Devices on the IoT use various technologies like Radio Frequency Identification (RFID), Bluetooth Low Energy (BLE), and Quick Response Codes (QR Codes) to interact, collect, and share data about their environment. New technologies based on the Internet of Things are being developed every day in areas like smart homes and cities, infrastructure management, transportation, logistics operations, and healthcare which are designed to improve services and quality of life for everyone.

The IoT is also transforming the job market by enabling automation of tasks and requiring employees to acquire new skills and take on new roles. Since its introduction the IoT has grown substantially and is expected to continue growing at a rapid pace for the next several years to the tune of 26 billion devices and a market valued at $4. 6 trillion by 2020. This also presents many challenges that will have to be addressed as the IoT continues to grow. Cybersecurity, data privacy, and regulations concerning the appropriate use of collected data are at the forefront of challenges posed by the Internet of Things. The heterogeneous nature of the IoT and the proprietary protocols and designs are a challenge to create secure methods of transmitting and storing data considered to be private or sensitive in nature. Also, since the IoT is still considered to be in its early stages, regulatory frameworks will need to be developed in order to protect consumers data and trust in the IoT. The impact of the Internet of Things is ever increasing yet becoming less noticeable as society becomes more dependent and less aware of the every

day devices in use by the IoT. Seamlessly integrating all of the things used by people into their everyday lives could improve quality of life as long as people are aware of the data collection and usage challenges using the Internet of Things. Microsoft founder Bill Gates said, “ The advance of technology is based on making it fit in so that you don’t really even notice it, so it’s part of everyday life.”

References

- Bill Text – SB-327 Information privacy: connected devices. (2018, September 28). Retrieved November 13, 2018, from https://leginfo. legislature. ca. gov/faces/billTextClient. xhtml? bill_id= 201720180SB327
- CBBC Newsround | YOUR REPORTS | Exclusive Bill Gates interview. (2001, December 7). Retrieved November 20, 2018, from http://news. bbc. co. uk/cbbcnews/hi/club/your_reports/newsid_1697000/1697132. stm
- In Hassan, Q. F., In Khan, A. R., & In Madani, S. A. (2018). *Internet of things: Challenges, advances, and applications* .
- James, S. B. (2016). Legislating and regulating the internet of things. *SNL Kagan Media & Communications Report,* Retrieved from https://search-proquest-com. ezproxy2. apus. edu/docview/1841292075? accountid= 8289
- Kranz, M. (2017). *Building the internet of things : implement new business models, disrupt competitors, and transform your industry* . Hoboken, New Jersey: Wiley.

- Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet of Things Journal* , 1-1. doi: 10. 1109/jiot. 2018. 2869847
- Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review, 93* (1), 85-176. Retrieved from https://search-proquest-com. ezproxy2. apus. edu/docview/1636877419? accountid= 8289
- QR Code. (2013). In D. Downing, *Barron's business guides: Dictionary of computer and internet terms* (11th ed.). Hauppauge, NY: Barron's Educational Series. Retrieved from http://ezproxy. apus. edu/login? url= https://search. credoreference. com/content/entry/barronscai/qr_code/0? institutionId= 8703
- Rudman, R., & Sexton, N. (2016). The internet of things. *Accountancy SA,* , 22-23. Retrieved from https://search-proquest-com. ezproxy1. apus. edu/docview/1794510817? accountid= 8289
- Snapshot® Privacy Statement. (n. d.). Retrieved November 20, 2018, from https://www. progressive. com/support/legal/snapshot-privacy-statement/
- Text – S. 1691 – 115th Congress (2017-2018): Internet of Things (IoT) Cybersecurity Improvement Act of 2017. (2017, August 1). Retrieved November 13, 2018, from https://www. congress. gov/bill/115th-congress/senate-bill/1691/text? q=%7B%22search%22%3A%5B%22Internet+of+Things%22%5D%7D&r= 1
- Wadhwa, V. (2015). *When kids start getting hacked, it's time to wake up about cybersecurity* . Washington: WP Company LLC d/b/a The

Washington Post. Retrieved from https://search-proquest-com. ezproxy2. apus. edu/docview/1748080803? accountid= 8289

- Wolf, M. (2014, August 14). http://webcache. googleusercontent. com/search’q= cache://www. forbes. com/sites/michaelwolf/2014/08/14/samsung-acquires-smartthings/. Retrieved November 4, 2018, from ttps://www. forbes. com/sites/michaelwolf/2014/08/14/samsung-acquires-smartthings/#428274a2ba2b
- Wu, T., Wu, F., Redoute, J., & Yuce, M. R. (2017). An Autonomous Wireless Body Area Network Implementation Towards IoT Connected Healthcare Applications. *IEEE Access* , *5* , 11413-11422. doi: 10. 1109/access. 2017. 2716344
- Xu, L., He, W., & Li, S. (2014). Internet of Things In Industries: A Survey. *IEEE Transactions on Industrial Informatics* , *10* (4), 2233 – 2243. doi: 10. 1109/TII. 2014. 2300753
- Yeh, K. (2016). A Secure IoT-Based Healthcare System With Body Sensor Networks. *IEEE Access* , *4* , 10288-10299. doi: 10. 1109/access. 2016. 2638038