Matthew Liu

PHIL3127

2 February 2019

Research Paper on IoT devices – A Reflection and Risk Benefit Analysis

IoT, Internet of Things, represents a network of interconnected devices. In each device, sensors are embedded to collect data which is dumped onto IoT platforms such as the cloud or internet. Then, the cloud sourced data is extracted to improve user experience, efficiency, automation, etc. Newly developed IoT devices impacts our personal devices, lifestyle, economy, companies, privacy concerns, legal issues, cyber security, safety, manufacturing, job market, health and more.

As a computer engineering and computer science student, IoT represents itself as an important and pervasive field of study and research. IoT continue to find applications from detecting dental hygiene from our toothbrush to designing a smart city with more efficient traffic controls. In our society, films, and cultural perspective, we often see the future as incredibly advanced technologies represented as highly sophisticated AI, virtual reality, self-driving cars, automation, and robots. IoT may present itself as an important well-integrated part to all these innovative technologies. Although it might be awe-inspiring to imagine a world where all your appliances and devices are connected, it is also important to consider human values and ethical, philosophical, and even religious issues posed by such technologies.

According to New York Times, USA Today, and other news sources, there have been many estimations that IoT will generate trillions in economic benefit; however, will these massive gains come at a great cost? There are many questions to be asked, and some may not have a clear answer in the present. For example, who is responsible for nefarious use or exploitation of IoT devices? Business information and home appliances could be targeted by hackers in hopes of theft or even terrorism. Could the dangers that hackers pose rise to the level of a national security threat? Perhaps the real threat of IoT lies in corporations’ greater jurisdiction over our lives as companies begin to gather greater insight into your daily comings and goings. This begs the question of how should IoT device data be stored, used, treated, or controlled? Should the data be stored at all? Suppose the threat of hackers and companies appears too great, what can we do to stop IoT’s growth? Or on the contrary, can Adam Smith’s “invisible hand” market theory resolves issues with privacy and security as they receive more attention? In the present, IoT devices already pose many concerns and benefits, and in the future, the impact of IoT can only grow and may be more daunting as it reshapes our society either in forefront or in the shadows of our devices. In this paper, I will develop a perspective on how IoT’s benefits toward the economy and the consumer shine in the darker issues of privacy and security concerns.

IOT’s impact on the economy appears tremendous. According to the IDC “worldwide technology spending on the Internet of Things to reach $1.2T in 2022”, and according to IoT Analytics “analytics predicts the global market for Internet of Things is expected to grow 37% from 2017 to $151B in 2018.” Senior market and business analyst Louis Columbus explains “IoT is the cornerstone of many organizations’ digital transformations, enabling them to optimize existing operations and excel at creating and pursuing exciting new business models.” There are complex challenges today in manufacturing and production that may be resolved through IoT devices. IoT sensors can help streamline, speed up, and ensure better quality in manufacturing processes through real-time monitoring. A good example of IoT’s potential economic benefits come from a case study in Barcelona. In 2016, a Harvard study found that “Barcelona estimates IoT systems have helped them save 58$ million on water, increased parking revenues by 50$ million, saved an additional 37$ million using smart lighting systems, and created 47,000 jobs last year.” Other strong examples of smart city development include Milton Keynes, Southampton, Amsterdam, and Stockholm. As businesses and countries are investing more into IoT, the monetary benefits of IoT are empirically proven to be a reality.

The benefits of IoT to the average middle-class consumer also proves monumental especially in terms of healthcare. Beyond simple pleasures of switching lights on/off or changing the thermostat with any device in the home, IoT has the potential to identify signs of heart attack. The Internet of Things has potential to save lives in medical procedures such as quickly notifying doctors in matters of seconds with knowledge of a patient’s symptoms especially during a life-threatening situation. According to Digital Solutions and Health Management technology, “Internet of Things (IoT) devices are proving to be a perfect answer for remote monitoring--they're relatively inexpensive, convenient, reliable, and most importantly, easy to implement […] IoT can play a crucial role in remote monitoring across the spectrum: wellness, prevention, post-discharge follow-ups, and chronic condition management.” In the future, it is possible that the implementation of health management IoT devices in homes will be a major deterrent toward mortality due to lack of medical aid and attention. In the status quo, many other technologies such as portable EKGs already greatly influence the health and wellness landscape.

Of course, it would be rather complacent to assume that IoT does not have its drawbacks. Transmission of medical information could be a vulnerable area where hackers could aim to attack in order to obtain sensitive data. With many devices such as cars being connected to the IoT, large-scale cyber-attacks could deal great damage to society. For example, a DDoS attack could render cars undrivable, homes unlocked, household appliances malfunctioning, and more. According to Beale and Berris from Duke Law, “Indeed, in the last few years, hackers have gained control of cars, trains, and dams, and some experts think that even commercial airplanes could be at risk.” In the current state awareness of personal online security, it would probably be dangerous to transition immediately into a world in which every device is connected to the internet. In my opinion, it is important for consumers to understand the dangers of using the same password across multiple platforms, the value of turning on auto-updates for companies to protect your data, the benefits of encrypting your hard drive, and other security measures. Although much of this may seem to be a culmination of paranoia, there will be a growing agenda for security and privacy as our lives become more interlaced with the Internet which opens many vulnerabilities toward hackers and even terrorists. In this way, IoT may be very beneficial for growing the agenda of protecting data. From my perspective, in the future, there will be a need of full transparency of data collected by devices (between the company and consumer) and growing agenda for cyber security. In this way, we may achieve a balance by minimizing the drawbacks of IoT while still reaping the tremendous benefits that it may provide to us physically, personally, socially, and economically.

In conclusion, the value of IoT is tremendous in many facets, but it does come with immense risk. Currently, it may be too dangerous for us to be “completely” connected to the internet; however, a growing agenda for cyber-security may minimize risks in the future.

Sources:

<https://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789>

<https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#20f6fe5c7d83>

<https://www.idc.com/getdoc.jsp?containerId=prUS43994118>

<https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>

<https://www.i-scoop.eu/internet-of-things-guide/smart-internet-things-facts-benefits/>

<https://hitconsultant.net/2017/11/03/internet-things-digital-future-value-based-care/#.XG9_cOhKjIU>

Sara Sun Beale & Peter Berris, Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses, 16 D*uke* L*aw* & T*echnology* R*eview* 161-204 (2018)

<https://scholarship.law.duke.edu/dltr/vol16/iss1/6/>