THE CONCEPT OF INTERNET OF THINGS AND ITS CHALLENGES TO PRIVACY

Sidi Mohamed Sidi Ahmed
Lot 3857-38 Jln Kunci Air Batu
6 3/4 Simpang Tiga -,68100 Gombak Selangor
kaldbkar@yahoo.com

Sonny Zulhuda
sonny@iium.edu.my

ABSTRACT

People today live in a connected environment that can negatively or positively affect almost all aspects of life. The Internet of Things (IoT) is a term used to describe the ubiquitous smart devices that can connect to the Internet. The IoT was described by advocates as "the first real evolution of the Internet" that can improve the way people live-in terms of education, work, health care, entertainment and so forth. However, the IoT has a cost especially when it comes to security and privacy. It also raises serious questions which need to be legally addressed. For example, how these smart devices generated, stored and collected information? Who own that information? And who will be responsible in case of damage? This paper attempts to discuss the concept of the IoT from various aspects -including its pros and cons- in order to clarify the term as it is used by the experts and researchers. In addition to that, the paper also goes further to touch upon the IoT's challenges to privacy from legal perspective. Last but not least, the paper provides recommendations on how to protect privacy and reap IoT's advantages. Furthermore, it is argued that a study such this will positively contribute to the academic discussion as it looks at IoT from one of its most contentious aspects (privacy challenges) that could slow IoT progress.

Key words: Internet of things, privacy, data protection

Introduction

Advances in technology in contemporary time have made people's lives better and easier and have provided them with myriad benefits. This improvement is pervasive in the economic, health, educational and social sectors and so on. The Internet of Things (IoT) is a term used to refer to the ubiquitous smart devices that connect to the Internet. In 2010, around 12.5 billion devices were estimated to be connected to the internet and the number increased dramatically to reach 25 billion in 2015. The same statistics estimates that in 2020 about 50 billion devices will be connected to the Internet. (Cisco IBSG). These connected devices include health and fitness devices, automobile black boxes, home and electricity sensors, smart phones, smart cars, smart glasses and such like. In the fact, the IoT is a reality that is impossible to be ignored because it promises unprecedented benefits and at the same time challenges.

The IoT is described by advocates as "the first real evolution of the Internet" that could enhance man's quality of life[1]. For example, it is believed that when the IoT is fully utilized, the gap between poor and rich people will be closed or at least minimized as resources and services will reach the needy people. In the healthcare sector, the IoT could help health professionals to serve more patients and detect diseases, as an instance. However, the IoT has a cost especially when it comes to security and privacy. In other words, data stored and collected about individuals have great values and the same could be said about data collected from inanimate things (cars, houses, offices). As insecure IoT devices can be utilized and deployed to generate and store sensitive private information about individuals and things, human dignity and privacy are likely to be invaded by intruders. For this reason, data protection becomes an urgent issue in the internet of thing era where everything could reveal everything.

The aim of this paper is to investigate the concept of the IoT while demonstrating its pros and cons as it is used by the experts and researchers. In addition to that, it also examines the IoT's challenges to privacy from the legal perspective. In the view of law, serious questions relating to IoT devices and their functions need to be addressed. For example, how do these smart devices generate, store and collect information? Who own that information? And who will be responsible in case of a damage resulting out of the IoT use? Last but not least, the paper provides recommendations on how to protect privacy and reap IoT's advantages. In the end, it is argued that a study such this will positively contribute to the academic discussion as it looks at IoT from one of its most contentious aspects (privacy challenges) that could slow down IoT progress.

The concept of Internet of Things (IOT)

[1] Dave Evans, (2011). *The Internet of Things – How the Next Evolition of the Internet is Changing Everything.* Cisco Internet Business Solutions Group (IBSG).

The phrase "Internet of Things" consists of three words; Internet, of, and things. In their efforts to clarify the reality of 'IoT', researchers deployed different scenarios. While some approached IoT as a whole phrase, others discussed its words separately. Most researchers agreed that the term "Internet of Things" was coined by Kevin Ashton in 1999. Ashton himself wrote: "I could be wrong, but I'm fairly sure the phrase 'Internet of Things' started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999"[2]. The coming point attempts to cite examples of the IoT's definitions in recent literature.

The Internet in the term of "Internet of Things", can either be seen as a metaphor- as the web used today, things will connect to each other, use services, produce data, etc. or in a stricter sense, IoT suggest that an IP protocol stack are going to be used by smart things- or by proxies, i.e. their preventatives on the network[3]. Rolf and Romana described the IoT as "an emerging global Internet-based information architecture facilitating the exchange of goods and services."[4] Having recognized that the term IoT is interpreted differently by experts and interested stakeholders, Adam Thierer states that IoT "is a term for when everyday ordinary objects are connected to the Internet" via microchips and sensors and "the point in time when more 'things or objects' are connected to the Internet than people."[5]

Delving into the literature let one to say that internet of things is a term used to describe the technologies (RFID, sensors, wireless, wires, etc.) that create connection between things/objects, people and environment. Other terms used interchangeably with IoT include, *inter alia*, Internet of Anything (IoA), Internet of people (IoP), Internet of data (IoD) and Internet of everything (IoE)[6] The authors went on to suggest the term IoE as a projected vision of what is possible as the IoT grows to accommodate a growing number of things. The above terms indicates that IoT constitutes of technological and non-technological (people, things, etc.) aspects.

Given the above definitions, the present authors argue that the Internet of Things represents a living concept of how today's technology increasingly connects to each other as well as to the human. They would entirely define the new relationship of human and technology and will further bring about new opportunities and challenges to human life.

IOT apparatus

Understanding the concept of IoT necessitates understanding of the technical apparatus that form its infrastructure. According to the International Telecommunications Union's ITU-T Y.2060 Recommendation[7] IoT devices can be categorized into data-carrying devices, data-capturing devices, sensing and actuating devices and general devices. 'Data-carrying device' is a device attached to physical things to connect them with communication networks. 'Data-capturing device' refers to reader/writer devices that have the capability to interact with physical things. 'Sensing and actuating devices' communicate with each other via wireless or wired communication technologies and use gateway to connect to the networks. These devices may have the ability to detect or measure information related to their surrounding environment and also convert such information into digital electronic signals. Lastly, 'general devices' have embedded processing and communication capabilities and may also connect with the communication networks. Examples of these devices are industrial machines, home electrical appliances and smart phones.

The Internet of Things applications can be found almost in all aspects of life –from industries to human body. Scott R. Pepper[8] mentioned examples of IoT devices that could challenge privacy and security among other aspects of today life. According to the author, they include, *inter alia*: (1) Health and fitness devices sensors –such as countertop devices, wearable, intimate and implantable sensors. There are many types of personal health devices -ranging from least physically invasive to the most invasive- that can generate and store valuable and intimate personal information about users (this information may include how much and how fast you eat, steps taken each day, heart rate, skin temperature, breathing patterns, blood pressure, weight scale, etc.). (2) Automobile sensors (black boxes) -such as Event Data Recorders (EDR), and consumer's automobile sensors. These sensors can collect enormous amounts of information about vehicles and drivers' behaviour. (3) Home and electricity sensors- such as the smart home and the smart grid. These are types of IoT devices that provide information to the homeowners and let them control home-appliances remotely, but in the same time they can generate, transmit, and store huge information about homes and their dwellers. (4) Employee sensors. The purpose of these sensors is to enable the employers to monitor their employees in the workplace and know what they are doing and whether they act in accordance with employment rules or not. But these sensors could create problems if employers try to access and collect intimate information about the employees. (5) Smartphone sensors. Sensors embedded in smart-phones can be considered one of the most ubiquitous new sensors technologies. These sensors can detect physical orientation, track the phone movement in space, and so forth.

[2] Kevin Ashton, (2009). That 'Internet of Things' Thing. available at <http://www.rfidjournal.com/articles/view?4986> accessed on 17-11-2015.

[3] Friedemann Mattern and Christian Floerkemeier (n.d.). *From the Internet of Computers to the Internet of Things* . Zurich : Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich .

[4] Rolf H. Weber, Romana Weber, (2010). *Internet of Things – Legal Perspectives.* Berlin: Springer.

[5] Adam Thierer (2013). *Privacy and Security Implications of The Internet of Things.* Mercatus Center at George Mason University.

[6] Edewede Oriwoh and Marc Conrad (2015). Things in the Internet of Things: Towards a Definition. *International Journal of Internet of Things.* 4(1): 1-5 DOI: 10.5923/j.ijit.20150401.01

[7] Recommendation ITU-T Y.2060. (2013). *Overview of the Internet of things, (ITU.* Geneva: ITU.

[8] Scott R. Peppet, (2014). Regulation of the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Concent. Texas Law Review, Volume, 93, Issue 1. pp 85.

Based on the above description, it becomes obvious that the Internet of Thing devices generate, transmit and store valuable information about users' habits, activities, characteristics and personalities as well as about their surrounding environment. As much of the data in the Internet of Thing environment might be personal information, worrying about misusing it is warrantable. In a smart environment such this, data protection and privacy aspects should be at the forefront of legal concerns.

IOT pros and cons

As with all technologies, IoT is estimated to play positive functions in modern life and at the same time it may create challenges. In its bright side, IoT proponents proclaim that it can be considered the first real evolution of the internet and it has the potential to enhance people life in terms of education, work, entertainment and so forth. The IoT's benefits are expected to cover most aspects of life such as healthcare, security and safety, entertainment, transport, businesses, etc. (David Niewolny[9], Dave Evans[10] and Bhaskara Reddy Sannapureddy[11]). In the healthcare sector, IoT devices can play an essential role from managing chronic diseases to preventing diseases at other scenarios, in addition to safeguards of the elderly. For example, patients can be monitored using IoT devices. In return, this will improve the quality of care and lower its cost. For improving life of the elderly, IoT devices that can detect a fall or other interruption can be employed to monitor elderly people's activities and well-being and report them to emergency responders or family members. Moreover, security and safety are other examples of IoT's advantages. Houses and other buildings can also be monitored and controlled to detect and prevent theft and other dangerous activities. Additionally, IoT can also employ to manage traffic and reduce accidents.

Regarding drawbacks, privacy and security threats are in the front of IoT's problematic concerns. In the IoT environment, information collected by sensors, chips, smart phones, etc., create vast amount of data and therefore, data volumes expand between 50 and 60 percent every year[12]. These volumes include a very valuable and sensitive data such as personal and financial data. The problem here is that IoT devices are prone to security breach and privacy law is unprepared to curb the threats created by the Internet of Things[13]. The IoT might also cause employment problems especially among primary workers and less educated staff[14]. When IoT fully takes its place, most of daily activities will be handled by machines. For example, checkout in supermarkets and withdrawal of money from ATM are automatically done. Accordingly, some people will lose their jobs. Besides, it is argued that dependence on technology is also another problem associated with IoT[15]. If people use technology on a daily basis, there is a real fear that they become dependent on it. Consequently, if the technology infrastructure broke down for whatever reason –hacking, design faults, material defects, sabotage, overloading, natural disasters or crises–, the economy sector and society as a whole could badly be affected. Technical problems are also another barrier that can slow the adoption of IoT and minimize its benefits. Power for sensors, agreed on management standards, and development of IPv6 are essential for the progress of IoT[16].

These are positive and negative implications of IoT on society in general. But what are impacts of IoT on privacy? The subsequent sections are devoted to answer this question.

IOT and privacy

In its linguistic sense, privacy is "the state of being alone or away from other people who may disturb you"[17]. The main objective of the right to privacy is to protect individuals from unwarranted surveillance. Theoretically, privacy has been widely recognized by national and international laws as a fundamental right. For example, Article 12 of the UDHR 1948 states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". However, the specific meaning and scope of privacy rights are far from commonly agreed.

The right to privacy has two general characteristics that distinguish it from other rights and at the same time make it difficult to be defined. These characteristics -as explained by Yael Onn et. al.[18]- are as follows: (i) Interests protected by privacy laws may also be protected by other laws (criminal laws; i.e. bodily harm, property law, physical domain) and (ii) the right to privacy is subjective in nature, culturally dependant, and derived from expectations of the society in a specific time. The fact that some aspects of privacy law are protected by other laws, encourage some to argue that there is no need for specific privacy law. The second characteristic indicates that privacy changes overtime and what are considering privacy here and today may not be so tomorrow and there. This is made more obvious when we face myriad of challenges to privacy due to the use of modern technologies.

[9] David Niewolny, (2013). *How the Internet of Things Is Revolutionizing Healthcare.* Freescale Semiconductor, Inc.
[10] Dave Evans,
[11] Bhaskara Reddy Sannapureddy. (2015) Pros & Cons of Internet Of Things (IOT) <://www.linkedin.com/pulse/pros-cons-internet-things-iot-bhaskara-reddy-sannapureddy> (Accessed on Feb 25, 2015)
[12] Samuel Greengard, (2015). *The Internet of Things.* Massachusetts Institute of Technology.
[13] Scott.
[14] Bhaskara,
[15] Friedemann and Christian,
[16] Dave Evans
[17] *Oxford Wordpowe*r (1999). Oxford University Press (maker).
[18] Yael Onn et. al. (2005). *Privacy in the Digital Environment.* Haifa: Haifa Center of Law & Technology.

Having acknowledged that privacy has no universal definition, Robert Gellman[19] stated that privacy can be described as a "broad, all-encompassing concept that envelops a whole host of human concerns about various forms of intrusive behavior, including wiretapping, surreptitious physical surveillance, and mail interceptions." Generally speaking, privacy information consists of two branches, autonomy (the right to be left alone) and information privacy (the right to decide what to reveal about oneself) (Will Thomas DeVries[20] and PISA Consortium[21]). So far, the notion of privacy and its fuzziness has been highlighted, now the authors wish to examine how the IoT challenges the notion of privacy in the section to come.

In today digital era, all interactions can be recorded, distributed, and saved for long time. The digital revolution's effects on privacy can observe in three dimensions: (1) the ease of collecting data leads to accumulation of massive personal information via recording almost every modern communications, (2) the digital revolution flourishes the data market globally and gives every interested stakeholder an opportunity to examine and collect such data, and (3) there is no means or mechanisms that can sufficiently protect data in the digital age[22].

Recent literature counts some ways in which IoT can challenge privacy right as follows: (i) IoT devices such cameras, sensors, and smart glasses can identify the location of persons and what he are doing at anytime, (ii) in the IoT era, behavior and consumption patterns- from food to entertainment- could become public knowledge[23], (iii) technically, it is possible to identify anonymous dataset because each person has a unique gait or style of walking that could eventually distinguish him from a million of anonymous data. As an illustration, researchers –who analysed data on 1.5 million cell-phone users over fifteen months- found that it is easy to extract location of a single person from an anonymous dataset containing more than a million people[24], (iv) sensitive data such as precise place, financial account and health is collected directly by IoT devices as in traditional Internet, (v) collection of habits, locations and physical conditions over time may allow entity that does not collect sensitive information to infer it, (vi) IoT data might be used by companies to make insurance, credit and employment decisions.[25]

IOT and the legal framework

As much of the data streaming in the Internet of Things era might be personal-related information, worrying about misusing it is warrantable. In a smart environment such as IoT, data protection and privacy aspects should be at the forefront of legal concerns. Unfortunately, protecting privacy in a smart milieu is one of the biggest and important tasks which have not wholly achieved. In the legal view, dealing with private information has to be done in accordance with principles of Data Protection and other Laws.

When talking about IoT legal framework, the most important thing is to determine the model of laws that should regulate IoT. Regarding this, Weber and Romana[26] are on the view that self-regulation and international agreements are suitable for IoT as a global system, while the state law is not appropriate due to its territorial limitations. The authors mention that IoT legislations could have deferent purposes and goals: right-to-know-legislation, prohibition-legislation, IT-security-legislation, utilization-legislation, and task-force- legislation- as the objectives of privacy and data protection vary depending on the nature of protected data. For example, a Radio Frequency Identification technology (RFID) can be used to monitor products, animals, persons and to collect data for profiling purposes.

Around the globe, recent data protection laws provide guidelines on how to collect, process, and store information in the digitals environment. As an example, the Malaysian Personal Data Protection Act (PDPA) 2010 sets seven principles relating to the processing of personal data in a commercial activities (See, section 5 of PDPA 2010). These principles include all rights, duties and liabilities of all relevant stakeholders[27]. The principles encompass the whole data processing life-cycle, including the collection of personal data (that cannot be done without consent of data subjects), the use of personal data (that has to comply with pre-determined purposes, scope of use and need for disclosure), the maintenance of personal data (which must ensure the accuracy and adequate security measures), the retention as well as the disposal of data (which must strictly adhere to the limitation of period and secure methods of disposal).

These principles can arguably be employed to protect personal data in IoT environment as long as the data comes under the scope of the Act. However, as noted earlier, the Act applies to personal data in respect of commercial transactions which means any transaction of a commercial nature whether contractual or not. Some inter-connected personal devices may not come strictly under commercial transactions. The Act in section 3 also excludes the Federal and State Government from its scope. Another challenge to the privacy which trigger the legal concern is the lack of control over the information used or processed during the

[19] Robert Gellman, ((2013). *Robert Gellman (2013) Privacy and B An Approach Using Fair Information Practices for Developing Countries.* Washington DC.: Center for Global Development .

[20] Will Thomas DeVries, (2003). Protecting Privacy in the Digital Age. *Berkeley Technology Law Journal , Volume 18* (1 Article 19), 284-311.

[21] PISA Consortium. (2003). *Handbook of Privacy and Privacy-Enhancing The case of Intelligent Software Agents.* the Hague: College bescherming persoonsgegevens, copyright.

[22] William Thomas,

[23] Samuel,

[24] Scott,

[25] FTC Staff Report. (2015). *Internet of Things Privacy & Security in a Connected World.*

[26] Weber and Romana,

[27] Sonny Zulhuda, et.al. (2015). Big Data, Cloud and BUOD: How the Data Protection Law Addresses the Impact of "Datafication". *Advanced Science Letters* (October 2015) (in print).

process. As an illustration, inter-connected objects can automatically communicate without the awareness of the data subjects. Moreover, interactions between individuals, objects, individuals' objects and system are likely to cause massive and ubiquitous data flows and have bad effect on the data management. Lack of control may affect the data subject's interest and rights. Security Principle as prescribed under section 9 of PDPA 2010 does require the data user to take practical steps to protect personal data from all types of security threats or breaches. To what extent this can be fulfilled is yet to be seen because the IoT has not fully been adopted in Malaysian context. Nevertheless, in IoT environment, security undoubtedly is a tough task that needs a lot of efforts and protection. Regarding processing personal data, General principle (sec.6) obliges the data user to take the consent of data subjects. However, the legal validity of IoT user's is problematic as in some cases users may not know that their devices collect data about them[28]. The same technology that threats privacy in digital environment can also be employed to safeguard it. For example, the mechanisms established by Privacy-Enhancing Technology (defined as "a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system") could help protect data in IoT Environment. The use of this technology may as well be a proof of taking practical steps as required under the security principle of the PDPA 2010.

Another critical issue is the fact that devices and objects that are inter-connected in IoT environment are not necessarily originating from or located in one single jurisdiction. In fact, servers and providers are from multiple countries across legal and political boundaries. This will pose another compliance challenge to the legal framework on personal data protection. In Malaysian context, for example, section 129 of the PDPA 2010 puts a restriction on the trans-boundary transfer of personal information to countries outside Malaysia that do not provide equal protection to the personal data. Similar provisions are found in major data protection regime globally. Therefore, managing data across borders will be another challenge to manage by data users and service providers by, among others, ensuring that all parties involved will have in place guarantees on the data protection requirements either by law or by contractual force. It is argued that this area is another point of concern in allowing the smooth adoption of IoT in Malaysia and many other countries alike.

Conclusion and recommendations

It can be seen from above discussions, that the 'Internet of Things' has become a household concern -at least among the academicians- that may cause a major challenge in the information age as it is expected to affect either positively or negatively all aspects of people's life, including personal life. Privacy challenges among other things could interrupt the IoT or at least slow its progress. Fortunately, privacy issue is not insurmountable problem and thus, various measures have being employed to minimize the risks and fully reap the benefits including technical and regulatory requirements. As have been discussed above, the IoT poses challenges to the compliance of data protection laws because *firstly* most of the IoT devices and functions are not clearly known. *Secondly*, applicability of the existing laws to IoT is open to debate, at least in the years to come.

While talking about IoT laws may be premature because the IoT is still in its infancy, the lawmakers should be ready to act in reasonable time before it becomes too late. This paper recommends knowing all facts about IoT devices and processes, especially the way they generate, collect, store or share information, etc. This is believed to be the first step which enables lawmakers to examine the risk associated with the IoT and then to take necessary actions. Raising awareness among the public about this technology is also essential because there is a real need to sensitize the public to the problem of privacy and data breach and their grave consequences. In the digital environment, people are willing to share everything including personal information and the criminals, as always, wait in ambush.

References

Article 29 Data Protection Working Party (2014). *Opinion 8/2014 on the on Recent Developments on the Internet of Things.*

Ashton, K. (2009). That 'Internet of Things' Thing. available at <http://www.rfidjournal.com/articles/view?4986> accessed on 17-11-2015

Bhaskara Reddy Sannapureddy. (2015) Pros & Cons of Internet Of Things (IOT) <://www.linkedin.com/pulse/pros-cons-internet-things-iot-bhaskara-reddy-sannapureddy> (Accessed on Feb 25, 2015)

Edewede Oriwoh and Marc Conrad (2015). Things in the Internet of Things: Towards a Definition. *International Journal of Internet of Things.* 4(1): 1-5 DOI: 10.5923/j.ijit.20150401.01

DeVries, W. T. (2003). Protecting Privacy in the Digital Age. *Berkeley Technology Law Journal , Volume 18* (1 Article 19), 284-311.

Evans, D. (2011). *The Internet of Things – How the Next Evolition of the Internet is Changing Everything.* Cisco Internet Business Solutions Group (IBSG).

Floerkemeier, F. M. (n.d.). *From the Internet of Computers to the Internet of Things* . Zurich : Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich .

FTC Staff Report. (2015). *Internet of Things Privacy & Security in a Connected World.*

Gellman, R. ((2013). *Robert Gellman (2013) Privacy and B An Approach Using Fair Information Practices for Developing Countries.* Washington DC.: Center for Global Development .

Greengard, S. (2015). *The Internet of Things.* Massachusetts Institute of Technology.

[28] Article 29 Data Protection Working Party (2014). *Opinion 8/2014 on the on Recent Developments on the Internet of Things.*

Niewolny, D. (2013). *How the Internet of Things Is Revolutionizing Healthcare.* Freescale Semiconductor, Inc.

*Oxford Wordpowe*r (1999). Oxford University Press (maker).

Peppet, S. R. (2014). Regulation of the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Concent. Texas Law Review, Volume, 93, Issue 1. pp 85.

PISA Consortium. (2003). *Handbook of Privacy and Privacy-Enhancing The case of Intelligent Software Agents.* the Hague: College bescherming persoonsgegevens, copyright.

Recommendation ITU-T Y.2060. (2013). *Overview of the Internet of things, (ITU.* Geneva: ITU.

Sonny Zulhuda, et.al. (2015). Big Data, Cloud and BUOD: How the Data Protection Law Addresses the Impact of "Datafication". *Advanced Science Letters* (October 2015) (in print).

Thierer, A. (2013). *Privacy and Security Implications of The Internet of Things.* Mercatus Center at George Mason University.

Weber, R. H. (2010). *Internet of Things – Legal Perspectives.* Berlin: Springer.

Yael Onn et. al. (2005). *Privacy in the Digital Environment.* Haifa: Haifa Center of Law & Technology.