Volume: 4 Issues: 17 [December, 2019] pp.01-12]
International Journal of Law, Government and Communication
eISSN: 0128-1763
Journal website: www.ijlgc.com

DATA PROTECTION CHALLENGES IN THE INTERNET OF THINGS ERA: AN ASSESSMENT OF PROTECTION OFFERED BY PDPA 2010

Sidi Mohamed Sidi Ahmed[1]
Ahmad Ibrahim Kulliyyah of Laws (AIKOL), International Islamic University Malaysia (IIUM).
(Email: kaldbkar@yahoo.com)
Sonny Zulhuda[2]
Ahmad Ibrahim Kulliyyah of Laws (AIKOL), International Islamic University Malaysia (IIUM).
(Email: sonny@iium.edu.my)

Received date: *04-08-2019*
Revised date: *01-10-2019*
Accepted date*: 04-10-2019*
Published date*: 15-12-2019*

To cite this document: Ahmed, S. M. S., & Zulhuda, S. (2019). Data Protection Challenges in The Internet of Things Era: An Assessment of Protection Offered by PDPA 2010. *International Journal of Law, Government and Communication*, 4(17), 01-12.
DOI: 10.35631/ijlgc.417001

Abstract: *The Internet of Things (IoT) is an emerging technology of the 21st century. It is described as the first real evolution of the Internet that could positively or negatively affect all aspects of life. The basic idea of the IoT revolves around connecting things and objects (persons, animals, cars, trees, etc.) to the Internet and enabling them to communicate and then process (generate, receive, send, etc.) data about themselves and the environment surrounding them. Without a doubt, the IoT will bring countless benefits and provide timely-data and information about places and objects. However, the IoT, like other technologies, has disadvantages especially in terms of privacy and security of data. Particularly, the IoT might challenge personal data protection law and misgive its ability to effectively stand in the rapid successive technology waves. As the most important law relating to the protection of personal data in Malaysia, the Personal Data Protection Act (PDPA) 2010 could be used as a benchmark for assessing the adequacy of data protection law in the country. Thus, this paper attempts to shed light on data protection challenges in the IoT era and then assess the adequacy of this Act in dealing with those challenges. The paper employs a legal doctrinal method to analyze the legal frameworks relevant to personal data protection. It may also use a comparative method to compare the PDPA with its counterparts in other countries. A study such as this is arguably useful and timely as Malaysia is already embarked in the IoT caravan with the vision of being "the Premier Regional IoT Development Hub."*

Keywords: *IoT Era, Data Protection, Assessment of PDPA*

Introduction

The Internet of Things (IoT) is an emerging technology that plays an essential role in the modern age. At present time, the IoT technology can be found almost in all things surrounding people such as cars, houses, wearable devices and such like. The basic function of IoT revolves around connecting things (persons, animals, cars, trees, etc.) to the Internet and enabling them to communicate and then process (send, receive, generate, etc.) information about themselves and the things they are attached to. Without any doubt, IoT brings countless benefits to humans because data and information generated by IoT technology can be used to enhance existing services and create new ones. However, IoT, like other technologies, has disadvantages especially in terms of privacy and security of data streaming through it. For example, in its Report 2015 about IoT, the Federal Trade Commission (2015) mentioned that IoT could enable unauthorized access and misuse of personal information, facilitate attacks on other systems and most dangerously create safety risks. Particularly, IoT could challenge personal data protection law and misgive its ability to effectively stand in the rapid successive technology waves. As the most important law relating to protection of personal data in Malaysia, Personal Data Protection Act (PDPA) 2010 could be used as a benchmark for assessing the adequacy of data protection law in the country. This is the objective that this paper attempts to achieve by shedding light on data protection challenges in the IoT era and then assessing the efficiency of the PDPA in terms of dealing with those challenges. In order to achieve this, the second section of this paper provides an overview of the IoT including its definition and main features. Moreover, the discussion will be extended to challenges that IoT could pose on data flow through it. The third section will concentrate on PDPA and its relevance to data flow in IoT devices and systems. This includes discussing the applicability of the Act to IoT data and examining some important terms used in the Act. The fourth section deals with principles of data protection established by the Act and how they can be complied with in the IoT environment. Lastly, the fifth final and final section provides concluding points that summarize the outcome of the discussion as well as suggestions or recommendations to strengthen and improve data protection law in Malaysia.

Methodology

This research is a doctrinal research depending on both primary and secondary related sources.

It uses the doctrinal legal method to analyse and assess data protection principles provided in the PDPA 2010. The aim is to assess the efficiency of the PDPA in the IoT environment. It also employs a comparative method to compare the protection offered by the PDPA to personal data in the IoT era with its counterparts in other countries especially in the European Union (EU) region where such comparison is relevant.

It is argued and believed that a study such this will positively contribute to the field of legal studies as it concerns one of the most penetrated technologies that could affect everyone in the digital era. In Malaysian particularly, protecting personal data in the IoT environment is an essential matter because the country is already joined the IoT caravan with the aim of being “as the Regional Development Hub for IoT” (Ministry of Science, Technology and Innovation (MOATI), 2014).

IoT and Data Challenges

IoT is one of the terms used to describe the evolving technology that enables connection of

things to the Internet. Other names include, inter alia, Internet of Anything (IoA), Internet of Data (IoD), Internet of People (IoP) and Internet of Everything (IoE) (Edewede Oriwoh, 2015). The term IoT was firstly coined in 1999 with the vision that computers would be able to collect data and render it into useful information without human intervention (Jorge E. Ibarra-Esquer, 2017). At the present time, IoT is a hyped term that is preoccupying time and agenda of many stakeholders including some governments around the globe (Johanna Virkki, 2013). Before highlighting challenges pose by IoT on data protection law, it is important, especially in the view of those who are not familiar with the subject, to mention what IoT is. IoT encompasses three words: internet, of and things. The Internet can be defined as, "a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location" (Barry M. Leiner, 2009, p. 22). On the other hand, the term "thing" in the context of IoT is defined by the Concise Oxford English Dictionary as "an object that one need not, cannot, or does not wish to give a specific name to" (Catherine Soanes, 2003). It includes both inanimate and animate creations. In the context of IoT, 'things' can virtually include anything such as computers, electronic devices, clothing, trees, houses, fridges, people, animals, trees, house (Somayya Madakam, 2015) (Stephan Haller), cars, and so forth. As for the IoT definition, it can be approached from two aspects, namely time and description. In the time phase, IoT is a term used to refer to "the point in time when more "things or objects" were connected to the Internet than people" and that point of time was "sometimes between 2008 and 2009" (Evans, 2011, p. 2). The other approach defines IoT by describing its components and functions. In this regard, IoT is defined in the Malaysian National IoT Strategic Roadmap as "Intelligent interactivity between human and things to exchange information and knowledge for new value creation" (Ministry of Science, Technology and Innovation (MOATI), 2014, p. 4). It seems that the Roadmap's definition restricts interaction in the IoT environment to humans and things. However, interaction in IoT is not restricted to human and things only, but there are also interactions between people and people and between things and things (Spyros G. Tzafestas, 2018). Moreover, IoT also is described as "the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable through information sensing device and/ or controllable via the Internet, irrespective of the communication means" (Patel, 2016, p. 6122). Probably, the best description of IoT (Leloglu, 2017) is the one provided by the International Telecommunication Union (ITU) which considers IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (The International Telecommunication Union (ITU), 2013, p. 1). The above definitions clearly indicate that the idea of IoT revolves around connecting things to the Internet in a way that enables such things to generate and process data about themselves and their environment.

Simply put IoT aims to connect all things in all places during all times in order to create smart environments where cities, transport, energy, etc., become more intelligent (Patel, 2016) and (River Publishers , 2014). IoT devices and applications include, inter alia, health and fitness devices, smartphone sensors, smart grids, home, banking (Spyros G. Tzafestas, 2018) and (Pepper, 2014) and other applicable things. The wide usage of IoT is expected to bring a positive impact on aspects of economy and society (education, health care, energy, consumers, cities infrastructure and cities), but at the same time there are some challenges including privacy, security and technical issues that could act as a hindrance to the IoT growth (Fischer, 2015) and implications. As an illustration, the Malaysian Roadmap counted some potential advantages that IoT could bring to the country in terms of economy, creating

employment opportunities, serving the research community, etc., but at the same time the Roadmap acknowledged the existence of some potential challenges most especially in security and privacy (Ministry of Science, Technology and Innovation (MOATI), 2014).

Regarding challenges pose by IoT on data protection, there is no doubt that billions of unsecured objects connecting to the Internet and generating data including personal data will have an impact on the safety of data flowing in IoT devices and systems. This can be supported by the fact that most of IoT applications (63% of IoT applications-5.2 billion units) are found to be consumer applications (Meulen, 2017). The European Commission counted some features of IoT that could have an effect on data-these features include the followings. Firstly, communication between objects to objects and person. Secondly, huge amount of personal data coming from various sources and automated communications (European Commission, n.d.). These features could generate some challenges ranging from unease compliance with data protection principles to deciding the applicable law (European Commission, n.d.). Moreover, others asserted that IoT could affect data protection through facilitating identification of persons (by linking objects to specific persons), profiling (by combining data collected by various objects linked to specific persons) and geolocation (by locating places of persons through smartphone etc.) (Fabiano, 2017). These manifestations or examples of IoT challenges to the existing data protection laws illustrate or support the view that IoT "will be a legal tsunami, the intensity and magnitude of which are unknown to date" (BARBRY, 2012). The next paragraph will discuss these challenges in light of protection provided by the Malaysian PDPA 2010.

An Overview of PDPA 2010

Data or information is the essence of the digital age because the function and operation of every modern activities depends on it. It becomes a valuable object that many people are yearning to possess and use for legitimate and illegitimate purposes. The importance of data in the information age resulted in the enactment of data protection laws which aim to protect interests of data subjects and at the same time encourage and facilitate the free movement of data. The efforts of protecting data in the electronic environment have started in the fourth quarter of the 20th century and placed on the agenda of national and regional organisations such as the United Nations (UN) (United Nations-Economic and Social Council, 1990) the Council of European (Council of Europe, 1981) and the Organisation for Economic Co-Operation and Development (OECD) (Organisation for Economic Co-Operation and Development (OECD), 2013). At this time, there are more than 100 countries that have data protection laws (United Nations Conference on Trade and Development (UNCTAD), 2016). In Malaysia, personal data is protected by Personal Data Protection Act (PDPA) 2010 (Act no 709) which came after a long wait "to regulate the processing of personal data in commercial transactions." This Act consists of 146 sections and 11 parts and remains the most relevant law in the country that deals with protection of personal data. However, relevance of this law to IoT does not guarantee applicability of the Act to all types of data flow in the IoT environment. Thus, discussing the scope of PDPA in light of data flow in IoT devices and systems is necessary.

According to section two of the Act, PDPA applies to any person who processes or controls personal data for the purpose of commercial transactions established in Malaysia or used equipment for purposes other than transition of the data through the country. Moreover, PDPA has a specific set of material and territorial scopes. The territorial scope includes two scenarios: processing personal data by someone who is inside or outside the country. In the first scenario, the Act applies to data users who are established in Malaysia in all

circumstances (processing done by themselves their agents, etc.). In the case of data processed by someone who is not established in Malaysia, the Act will apply to all processing accept "for the purposes of transit through" the country (S 2 (2-b). This could arguably have the power to extend the territorial scope of the Act to some data processed in the IoT environment by data users who are established outside the country. For example, personal data collected by some IoT devices (wearable devices, etc.) and share with outside-data users such as manufacturers could come into the scope of this section because they are engaging in processing data for purposes other than transiting through the country. As a comparison, IoT device manufacturers "qualify as data controllers" under the EU law because they do more than selling the devices and most of them engage in collecting and processing data generated by these devices (Article 29 Data Protection Working Party (WP29), 2014). Moreover, the EU GDPR applies to the processing of personal data by data controllers or data processors who establish outside the Union region in case of they are offering goods or services to data subjects in the Union or monitoring their behaviour thereto (Art. 3 (2, a & b) of the EU General Data Protection Regulation (GDPR) 2016/679). Nevertheless, it is necessary to extend the scope of local legislation to include those who operate from other jurisdictions in the modern borderless world. In this regard, it would be advised to interpret the term "uses equipment in Malaysia for processing the personal data" in a way that covers those who offer goods or services or control behaviour of data subjects in Malaysia, as GDPR does (Art. 3 (2, a & b). This, if done, could arguably enable PDPA to cover a variety of data processed in the IoT environment by data users who establish outside the country.

However, the Act on the material scope applies to personal data processed in "commercial transactions." According to this, the terms processing of personal data and commercial transactions play a vital role in defining the material scope of the Act. Processing includes most dealing with personal data such as collecting, recording, storing and so forth (s 4 of PDPA 2010). The broadening definition of processing "is deliberately done to cover all the activities of a data user" (Abu Bakar Munir, 2012) and this could be useful in the IoT environment where data is being processed in new ways. As for personal data, the Act (s 4) defines it as any information "relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that information and other information in the possession of the data user," including sensitive data (data related to physical or mental health, political, religions, etc.). Moreover, the term "commercial transactions" covers "*any transaction of commercial nature, whether contractual or not, which includes any matter relating to supply or exchange of goods or services*…" (s 4 of PDPA). Currently, there are various classes of data users under PDPA including communications, banking and financial institutions, private health and education, insurance, transportation, etc. (S 2 of the Personal Data Protection (class of users) Orders 2013). It is fact that IoT technology penetrates in most sectors including commercial sectors and thus there is no doubt that PDPA could apply to some IoT data processed in its scope. As an example, mobile banking applications installed in smart phones (Maybank2u Mobile, 2018) which are part of IoT like smart home (Spyros G. Tzafestas, 2018) could be taken as an example of IoT personal data protected by PDPA.

More than anything else, the term "commercial transactions" is one of the important terms that leaves its impression on the Act. On one hand, the term could cause confusion because distinction between commercial and non-commercial activities could be uneasy in some circumstances (Abu Bakar Munir, 2012). On the other hand, it has the power to exclude variety of personal data from the scope of the Act. In the context of IoT, "commercial transactions" is arguably the most important term that could affect or lessen the ability of PDPA to comprehensively protect personal data flow in the IoT environment. This is because

some IoT consumer-applications used for personal purposes may not be covered by the phrase "commercial transactions" and such applications constitute a great part of the IoT applications (Meulen, 2017). Experts have opined that PDPA should be amended to cover personal data in both non-commercial and commercial transactions to effectively protect personal data in Malaysia.

Also, non-applicability of the Act to data processed by governmental bodies (s 3 of PDPA) is another important issue that could lessen the efficiency and capability of PDPA to adequately coexist with waves of new technology such as IoT. Hence, the wide range exemption and extent of application of the data protection law on government agencies is an important issue to be addressed here. Regarding applicability of data protection law to the government, the approach taken by the EU law could be better to be followed by the Malaysian government. For example, GDPR clearly mentions that it "applies to the processing of personal data" including data processed by governmental and non-governmental bodies. However, the GDPR exempts personal data processed by competent authorities, data processed for personal or household purposes among others. As for the PDPA, section 45 exempts some types of personal data from provisions of the Act or some of them. Moreover, Section 46 authorizes the Minister to make new exemption. As an illustration, the exemption includes data processed for personal or family use purposes, taxation and criminal purposes, statistics or research purposes, order or judgments, regulatory functions, journalism, literary or artistic purposes and data related to physical or mental health (s 45 of PDPA). Unlike the various exemptions made by PDPA, the non-applicability of the Act to the Federal and States Governments could have far-reaching on data protection because it will exclude the biggest data user (the Governments) from the scope of the Act. The Act does not define the term government but it usually refers to *"the whole class or body of office-holders or functionaries considered in the aggregate, upon whom devolves the executive, judicial, legislative, and administrative business of the state"* (Henry Campbell Black, 1968, p. 824) This means that the term government in the Act could include ministries, public hospital, schools or universities, and such like. In fact, the Personal Data Protection (Class of Data Users) Orders 2013 subject private healthcare, schools and higher educational institutions to registration (s 2 (4 &7), but the Orders are silent about their public counterparts. This means that Act considers them as governmental bodies. For the sake of personal data protection, PDPA could be extended to include personal data processed by the government, but at the same time necessary exemption, shall be made as the EU Regulation does (Art. 2 (1 &2) of GDPR).

As the discussion revealed, it can be argued that the Act may not apply to a variety of personal data processed in the IoT environment because such data might be processed out of the commercial atmosphere. For example, individuals who buy IoT wearable devices which are used to track some aspects of health or fitness data, etc., (Pepper, 2014) from the market and voluntary use them to generate and store data about themselves. When those individuals use these IoT devices and upload their data to the Internet or mobile applications, there is apparently no commercial transactions between those individuals and the manufacturers of these devices who can be in other jurisdictions. In this regard, protection offered by PDPA can be considered as insufficient because it could not provide protection to personal data in scenarios like the above one.

IoT and Data Protection Principles

Data protection laws around the world establish some principles to be followed in the course of processing personal data. These principles mention rights and duties of parties involved in the processing. For example, section 5 of PDPA sets out 7 principles including the general,

notice and choice, disclosure, security, retention, data integrity and access principles (s 6-12). These principles are backed by a system of punishments including fine (up to three hundred thousand ringgit) or imprisonment (up to 2 years) or both (s 5 (2) of PDPA). In the following subsections, these principles will briefly be discussed in order to highlight the difficulty of implementing them in an automated environment such as the IoT one.

General Principle

As mentioned in section 6, this principle obliges the data user to take the consent of the data subject before processing personal data related to the latter. This section also restricts the processing of personal data to lawful, necessary and non-excessive activities. Additionally, this Principle makes a distinction between processing personal data and sensitive personal data which is subjected to more restrictions mentioned in section 40 of the Act. Taking consent of the data subject is a central issue in data protection law. Apart from mentioning that consent can be withdrawn (s 38), PDPA refers to data subject consent in various matters including disclosure of personal data, processing of sensitive personal data and transferring data outside the country (Ss 8, 40 (1, a) and 129 (3, a). The Act does not define the term of consent, but the subordinate regulations mention that consent can be obtained "in any form that such consent can be recorded and maintained properly by the data user" (S 3 (1) of the Personal Data Protection Regulations (PDPR) 2013). This means that consent can "be oral and implied" (Abu Bakar Munir, 2012) In the IoT context, using IoT wearable devices such as health and fitness devices (Pepper, 2014) by individuals could be considered as consent in the meaning of PDPA.

The Notice and Choice

The second principle in the Act is the principle of Notice and Choice (s 7). This Principle obliges the data user to inform the data subject, as soon as possible, through written notice about the description of the data, the purposes of collection and processing of the data and the third party whom the data being or might be shared with, in addition to matters related to correction, restriction etc., and the means used therein. It is important to note that the principle of notice and choice is an important principle especially in the online world. Linguistically, the term notice and choice mean "a written statement giving information or news" and "an act of choosing between two or more…things" (Oxford Wordpower, 1999, p. 507 & 123) respectively. In data protection atmosphere, while the term notice consists of "a presentation of terms," choice is "an action signifying acceptance of" the terms presented in the notice (Robert H. Sloan, 2013, p. 3). Complying with this principle in the IoT environment could be a challenging ed task. As an illustration, this principle makes it compulsory for the data user to provide written notice to the data subject including information about the data and the direction that it will take in addition to contact of the data user(S 7 of PDPA and s 4 of the Data Protection Regulations 2013). In the IoT environment, however, identifying the data user could be a challenging task as in some cases (wearable devices, etc.) the data subject is dealing with devices that connected to the virtual world and has no connection with the manufacturers or suppliers of these devices. In such scenarios, who shall provide the written notice and who is be contacted: the devices, manufacturers or suppliers? These and other challenges imposed by the IoT on data protection laws need a suitable solution.

Disclosure Principle

Section 8 of the Act spells out the context of disclosure Principle which prohibits revealing personal data in cases other than the agreed cases without the consent of the data subject especially in cases mentioned in section 39 of the Act.

Security Principle

The Principle of Security is another crucial principle in the Act. It obliges the data user to "take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure" (s 9 (1, a) of PDPA). Additionally, this Principle mentions that the security measures should consider the nature of the personal data, its places or locations, storage, persons accessed to it, and the consequences of any security breach and such like. Both the PDPR 2013 (s 6) and the Personal Data Protection Standard (PDPS) 2015 (s 4) establish practical steps to be implemented in securing personal data. Without delving deeply into details of these rules, it is argued that the security measures required by the security principle are not easy to be achieved in the IoT environment because of countless flow of data from objects. Technically, IoT devices have a limited physical, low powers and computational capacity which in turn make adding security measures to them are not easy (Pepper, 2014). Another element of security that must be observed by the data user is "the place or location where the personal data is stored" (s 9 of PDPA). Practically speaking, complying with these could be a challenging matter because some IoT devices will be put in outdoor environments that are subject to physical attacks (Mohamed Abomhara, 2015) such as theft, vandalism and so forth. Accordingly, the IoT challenges to security of personal data is a major concern because the data users who are obliged to take those measures are not easy to be identified. Needless to say, that both physical and technical security are important in the IoT context because the consequences of any security breach may not only result in revealing personal data, but more dangerously IoT could be used to shut down transportation systems, alter medical devices, destroy industrial components, etc., (Oltsik, 2014) which in turn could have an effect on people lives.

Retention Principle

This principle deals with the necessity of deleting personal data after the collection and usage. The retention principle is an obligation on the data user to destroyed or permanently delated the data. The execution of data retention is done in accordance with guidelines spelt out in the PDPS 2015 (s 6) constituting 7 steps to be taken by the data user in that regard. In the case where PDPA applies to personal data processed in commercial transactions executed in the IoT environment, the data user shall comply with all rules of Retention Principle either in the PDPA or its subsidiary regulations.

Data Integrity & Access Principles

Data Integrity & Access Principles deal with the accuracy of data and the right of the data subject to access his personal data. For example, the Data Integrity obliges the data user "to take reasonable steps to ensure" the accuracy of the personal data in fulfilment of its purpose, etc. (s 11 of PDPA). The reasonable steps required by this Principle are explained in the PDPS 2013 (s 7). In general, the Access Principle establishes the right of the data subject to access his personal data held by the data user in accordance with principles and guidelines set by PDPA and its subsidiary regulation (Ss 12, 30-37 of PDPA and 9-11 of PDPR 2013).

Like the other data protection principles, the Access and Integrity principles oblige the data user to take specific steps to ensure the integrity and accessibility of the personal data. However, the implementation of these principles requires identifying data users and processors and communicating with them. In the IoT environment, however, data users and processors in some scenarios (wearable devices, etc.) may neither be identified nor communicated with. That is, because, unlike the EU perspective where the IoT device

manufacturers is considered as data controllers on the ground that they are engaging in processing data generated by the devices (Article 29 Data Protection Working Party (WP29), 2014), the Malaysian regulatory body does not deal with novel issues such as these.

From the above discussion, it seems that current protection provided by PDPA is insufficient in the IoT environment. The inadequacy of the Act to provide enough protection to data flow in IoT could arguably be attributed to two reasons. The first one is the narrow scope of the Act which only applies to personal data processed in commercial transactions. The second reason is inability of the Act in its current version to cope with the rapid technology used in processing personal data. For example, PDPA applies primarily to data users who collect personal data in commercial transactions environment. However, the concept of data users is extended by the IoT to new stakeholders who collect personal data in various ways. In the EU region, device manufacturers, social platforms, application developers, etc., are considering data users (Article 29 Data Protection Working Party (WP29), 2014). By contrast, PDPA is not explicitly extended to cover those newcomers.

Conclusion and Policy Recommendations

This paragraph attempts to summarise the above discussion and then provide some recommendations that could improve protection of data or at least open the door for further discussion and suggestions.

Conclusion

The IoT brought challenges to data protection law and such challenges should be recognized in order to take proactive reforms as steps towards solutions. This paper was dedicated to the assessment of protection offered by PDPA to data flow in the IoT environment. It started with a general introduction highlighting the role that the IoT currently plays in today life and its challenges to the legal systems especially those provisions relating to data protection. It then defined the main terms such as the Internet of things. As the objective of this paper is to assess protection provided by this Act to personal data processed in the IoT environment, the applicability of the PDPA to the IoT was discussed. In this regard, it was found that the term "commercial transactions" will affect and lesson the ability of the Act to adequately protect all data processed in the IoT environment as some IoT devices used for personal or family purposes may not be covered by such term. It is also mentioned that, the Act excluded data processed by governmental bodies (Both the Federal Government and the States Governments) from its applications and exempted various types of personal data processed by non-governmental entities. Apart from discussing the applicability of the Act to data flow in the IoT environment, the paper also discussed the difficulty of complying with data protection principles mention in the Act in the IoT age where data continuously flows. It concludes that there is a need for reforming and updating PDPA to enable it to provide suitable protection to personal data in the IoT environment. It is mentioned that the approach taken by EU to protect personal data could be flowed by the Malaysian legislators to improve data protection in the country. The next section will provide some suggestions that is believed to be useful and necessary for the interests of both data subjects and ~~data~~ users or in other words, the whole society.

Recommendations

As evidently seen above on the analysis of the Act, some personal data processed in the IoT environment may not be covered by the Act which is considered the most important Act dealing with personal data protection in the country. This could have an effect on individuals whom personal data are not protected by this supreme Act or probably on the interests of the

country because protection of personal data is important for its free movement or exchange with other countries. The above discussion revealed that the term "commercial transactions" have the power to exclude all personal processed outside the commercial atmosphere. For the sake of data protection, this paper recommends extending protection to personal data processed in both commercial and non-commercial transactions. Another important thing that this paper recommends is the extension of the scope of PDPA to cover personal data processed by the Federal and States Governments of the country. This extension, if done, will grant some rights to data subjects and help prevent misuse of personal data processed by data users (here the Government employers) and also harmonize data protection law in the country in both public and private sectors. The extension of the scope of the Act to data processed by the Governments shall consider the nature of the Governments and their functions and therefore making necessary exemption. Moreover, this paper also recommends extending the concept of the data user and data processor to cover new stakeholders in the IoT environment such as device manufacturers, application developers and such like.

References

Abu Bakar Munir, S. H. (2012). Personal Data Protection Act: Doing Well by Doing Good. *Malayan Law Journal, 1*, lxxxvi.

Article 29 Data Protection Working Party (WP29). (2014). Opinion 8/2014 on the Recent Development on the Internet of Things. ec.europa.eu. Retrieved 9 7, 2018, from Article 29 Data Protection Working Party (WP29), "Opinion 8/2014 on the Recent Development http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

BARBRY, E. (2012, 3rd Q,). The Internet of Things, Legal Aspects What Will Change (Everything)…". *Digiworld Economic Journal, 87*, p. 83.

Barry M. Leiner, R. E. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5), 22.

Catherine Soanes, a. s. (Ed.). (2003). *The Concise Oxford English Dictionary* (11 ed.). Oxford University Press.

Council of Europe. (1981). Convention for the Protection of Individual with regard to Automated Processing of Personal Data. Strasbourg: European Treaties Series-No. 108.

Edewede Oriwoh, M. C. (2015). Things in the Internet of Things: Towards a Definition. *International Journal of Internet of Things, 4*(1), 1-5.

European Commission. (n.d.). *IoT Privacy, Data Protection, Information Security*. Retrieved January 30, 2019, from semanticscholar.org/paper: https://www.semanticscholar.org/paper/IoT-Privacy-%2C-Data-Protection-%2C-Information/e4f35abaff323159dd66997dbea6d72d5c0a73cc

Evans, D. (2011). *The Internet of Things – How the Next Evolution of the Internet is Changing Everything*. (Cisco Internet Business Solutions Group (IBSG)) Retrieved January 29, 2019, from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Fabiano, N. (2017). Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation. *Athens Journal of Law, 3*(3), pp. 203-204.

Fischer, E. A. (2015, October 17). *The Internet of Things: Frequently Asked Questions*. Retrieved 9 7, 2018, from GOVLAB: http://thegovlab.org/the-internet-of-things-frequently-asked-questions/

Henry Campbell Black, M. A. (1968). *Black's Law Dictionary* (4 ed.). (1968, Ed.) (West Publishing Co.

Johanna Virkki, L. C. (2013). Personal Perspectives: Individual Privacy in the IOT. *Advances in Internet of Things, 3*(2), 21. doi:10.4236/ait.2013.32003

Jorge E. Ibarra-Esquer, F. F.-N.-R.-V. (2017). Tracking the Evolution of the Internet of Things Concept Across Different Application Domains. *Sensors, 17*, 1379.

Leloglu, E. (2017). A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications, 5*(1). doi:http://dx.doi.org/10.4236/jcc.2017.51010

Maybank2u Mobile. (2018, November 25). *Maybank2u.com is now on your mobile phone!* Retrieved from maybank2u.com: https://www.maybank2u.com.my/mbb_info/m2u/public/personalDetail04.do?channelId=&cntTypeId=0&cntKey=ACC08.03.06&programId=ACC08.03-MobileBanking&chCatId=/mbb/Personal/ACC-Accounts

Meulen, R. v. (2017, February 7). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Retrieved January 31 , 2019, from gartner.com: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Ministry of Science, Technology and Innovation (MOATI). (2014). *National Internet of Things (IoT) Strategic Roadmap* (1st publication ed.). Kuala Lumpur: MIMOS Berhad.

Mohamed Abomhara, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security, 4*, 65–88.

Oltsik, J. (2014). White Paper. *The Internet of Things: A CISO and Network Security Perspective*. The Enterprise Strategy Group, Inc.

Organisation for Economic Co-Operation and Development (OECD). (2013). *Privacy Framework": OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).* Retrieved 5 3, 2018, from cecd.org: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

Oxford Wordpower. (1999). Oxford University Press.

Patel, K. K. (2016). , "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing (IJESC), 51*(5).

Pepper, S. R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review, 93*, 95-117.

River Publishers . (2014). *River Publishers Series in Communication Internet of Things-From Research and Innovation to Market Deployment.* (O. V. Friess, Ed.) Aalborg, Denmark: River Publishers.

Robert H. Sloan, R. W. (2013). Beyond Notice and Choice: Privacy, Norms, and Consent. *Journal of High Technology Law*.

Somayya Madakam, R. R. (2015). "Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications,, 3*, 164-173.

Spyros G. Tzafestas. (2018). "Ethics and Law in the Internet of Things World. *Smart Citie, 1*(1), 99. doi: https://doi.org/10.3390/smartcities1010006

Stephan Haller. (n.d.). *The Things in the Internet of Things (A paper presented as a poster at the Internet of Things Conference 2010, Tokyo, Japan).* Retrieved January 29, 2019, from Researchgate: https://www.researchgate.net/publication/228488111_The_Things_in_the_Internet_of_Things

The Federal Trade Commission (FTC) Staff Report. (2015). *Internet of Things: Privacy & Security in a Connected World.* Retrieved AFebruary 17, 2019, from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

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

United Nations Conference on Trade and Development (UNCTAD). (2016). *United Nations Conference on Trade Data Protection Regulations and International data flows: Implications for Trade and Development.* United Nations Publication.

United Nations-Economic and Social Council. (1990). Revised Version of the Guidelines for the Regulation of Computerized Personal Data Files" (E/CN.4/1990/72.). UN Digital Library. Retrieved 9 7, 2018, from https://digitallibrary.un.org/record/85149/files/E_CN.4_1990_72-EN.pdf