Security and Privacy Concerns in the Malaysian National IoT Strategic Roadmap: Legal Response and the Way Forward

Sidi Mohamed Sidi Ahmed
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia
Kuala Lumpur, Malaysia
ORCID: 0000-0002-7607-1978

Sonny Zulhuda
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia
Kuala Lumpur, Malaysia
ORCID: 0000-0003-0192-1971

***Abstract*—Malaysia is geared to maximizing the digital technology and Internet of Things to reap the full benefit of the digital economy. In 2014, the Government came up with an important policy document entitled the National Internet of Things (IoT) Strategic Roadmap ('The Roadmap). Hopes are mounting that the IoT will be smoothly and speedily adopted in Malaysia amid various concerns relating to data security and data privacy. This paper investigates how the Roadmap frames the concerns of data security and privacy *vis a vis* the IoT in Malaysia. Employing a doctrinal and library research, this paper finds that while the Roadmap complements or supports the existing legal framework, its objectives will only be achieved if those legal requirements are complied with.**

Keywords—security, privacy, Internet of Things, Malaysia

I. INTRODUCTION

Technology has penetrated all aspects of modern life and left its positive and negative prints therein. Keeping data and information in the technological environment secure and private is important for earning technology benefits and avoiding its drawbacks. However, security and privacy are challenging issues in the virtual world (cyberspace) as well as in the real one. Like other cyber emerging issues, concern about security and privacy rises with every new waves of technology. The Internet of Things (IoT) is one of those technological waves that raise the concern about security and privacy of data flowing and residing in the cyberspace. This is because IoT technology is being used in almost all segments of life such as smart grids, environmental monitoring, logistics, intelligent transportation systems, e-health. [1] Regarding personal data particularly, IoT devices that could collect personal data like smartwatch, fitness tracker, smart eyewear, smart clothing, wearable medical device and wearable camera [2] can be found everywhere. The nature of IoT as an ever-connected network and device and its wide penetration into human life make security and privacy of this technology among emerging issues that regulative bodies around the world pay much attention to.

Malaysia joined the IoT caravan and became one of those many countries that put IoT in their national agenda and consider it as a rapid growing technology that could bring tangible benefits to citizens, businesses and governments. To this in practice, the Malaysian Minister of Science, Technology and Innovation (MOSTI) published the country's first National Internet of Things (IoT) Strategic Roadmap in 2014. [3] This Roadmap specifies the mission and vision of the country towards IoT and highlights advantages and disadvantages of implementation of the IoT system in the country. This paper aims to discuss security and privacy as obstacles that could affect implementation of the IoT in the country. To be precise, the focus of this paper is on the intention paid in the Roadmap to the issue of privacy and security and the magnitude of such intention. To achieve this objective, the second section of the paper makes an overview of the Roadmap through analysing the context of its main headings. The third section focuses on privacy and security as emerging issues mentioned in the Roadmap. The discussion here will focus on security and privacy as the legal means to protect interests of persons and property. The fourth section examines and analyses protection of privacy and security of data in the current legal system of Malaysia. The discussion will be restricted to the Principles set by the Personal Data Protection Act 2010 (PDPA). Finally, conclusion and recommendations are provided in the fifth section.

II. AN OVERVIEW OF THE ROADMAP

IoT has been in the developmental agenda of the international community and it is considered as a means that can be used to boost economy and other social sectors. For example, the United Nations (UN) through its specialized agencies such as the International Telecommunication Union (ITU) involved in continuing discussions about IoT and issued recommendations which aim to provide a unique definition to the phenomenon. [4] In most continents of the planet there are growing roots of IoT structures but the development of such structures differ from a place to place. Like its counterparts in the world, Malaysia has embarked on IoT and introduced its National Internet of Things (IoT) Strategic Roadmap in 2014. The country has a proper environment for development of IoT and the number of Internet users in the country are continuously growing. According to the Malaysian Communications and Multimedia Commission (MCMC), Internet users increased from 76.9% in 2016 to 87.4% in 2018. [5] Moreover, the MCMC found that smartphones are the most common means used to connect to the internet as they are used by 93.1% of users.

The IoT Roadmap provides an overview of Malaysian mission and vision towards IoT. Apart from IoT definition and megatrends, the Roadmap discussed the importance of IoT

and readiness of the country to implement IoT. For example, it mentioned that the IoT economic potential for Malaysia is forecast to reach RM 9.5 billion in 2020 and the growth will continue to RM 42.5 billion thereafter. In terms of employment opportunities, IoT was also estimated to create more than 14000 high-skilled employment opportunities by 2020. It could also serve the research community and help them commercialise R&D outputs.

Regarding readiness of the country for IoT, the Roadmap mentioned that Malaysia has a suitable environment for IoT and a strong ground in terms of technical, political, societal and political aspects. Nevertheless, the Roadmap highlights some obstacles that can hamper implementation of the IoT system in the country including, among others, barriers to free market competition exist, rural adoption, technology phobia, technology complexity, data accessibility and security and privacy concerns. All these factors can impede implementation of IoT in the country, according to the Roadmap. Therefore, the Roadmap outlines that its achievement strategic keys include (1) formulating an interoperability framework that harmonises the heterogeneity and complexity of standards and technologies to enable fast development and deployment of the IoT and (2) instituting a centralised regulatory and certification body to address privacy, security, quality and standardisation concerns [3].

Further on, alleviating concerns over data security and privacy has been made as a part of the long-term strategy to create an open community data framework. This was to be achieved through opening up public data with the intention of expanding the applications of IoT [3]. Obviously with this objective and strategy, settling data security and privacy problems must be one key success factors of the deployment of IoT in Malaysia.

In this paper, the focus will be on the concern about security and privacy of data flow in the IoT environment. The next sub-section will be devoted on security and privacy governance as mechanisms or tools used to protect people and their interests in the digital age.

III. Security and Privacy as Emerging Legal Issues

Like other technologies, using IoT has advantages and disadvantages. Without doubt security and privacy of data in the IoT environment are important and at the same time difficult to fully be achieved. The following paragraphs discusses the issue and highlight the cause of the concern about security and privacy in the IoT environment.

A. IoT Security Concern

Conventionally, information security aims to ensure availability, integrity and confidentiality of data. [6] In the IoT, this is not easy to be done because insecurity of IoT is caused by many factors. On one hand, securing IoT requires communication security (securing data from its source to destination), network security (availability of the service to legitimate users) and securing data in its storage (observing its confidentiality and integrity) and on the other, implementing strong security mechanism in IoT devices is not an easy task because these devices have limited "computational capabilities, memory and battery power." [7] Moreover, the comparative among the manufactures leads to focus on functionality and overlook security of IoT devices. [8] This results in that data flow in the IoT ecosystem can be manipulated and IoT devices can be tampered and used as a means to steal data, interrupt business operations, distribute denial-of service attacks and even disrupt critical infrastructure. [9]

The complex of IoT security could explain the particular stress of the Roadmap on security of IoT. Additionally, the wide usage of IoT and the consequence of data breach could be another factor that makes security among the priority. According to the Roadmap, IoT technology is been used in some specific areas of the Digital Lifestyle Malaysia such as connected healthcare, home and community living, traceability and people-friendly community and pointed out the role that IoT implementations can help transform and enhance these areas. [3, p. 37] In addition to the Roadmap, the Malaysian Communications and Multimedia Commission (MCMC) has published a Technical Report aiming to clarify technical regulatory requirements for IoT and also serve as technical reference for IoT interested stakeholders. [10] Moreover, the MCMC has also published a white paper about regulatory challenges of IoT. [11] Security and privacy are among the issues rose in these documents.

In the Report, the MCMC identified and discussed five technical regulatory challenges namely, (1) technical standardization, (2) spectrum requirement, (3) mobility requirement, (4) network numbering and addressing and (5) security and data privacy. As can be seen from the above, most of these issues discussed by this Report are technical issues. However, the Report acknowledged the increase of cyber-attack via IoT and noticed that aspects of data privacy and security requirement have been overlooked. In the aspect of security, the MCMC white paper established some measurements and steps to be taken to mitigate IoT risks. Apart from asserting that IoT devices have been used to launch attack, the white paper recommended subjecting IoT devices and systems in Malaysia "to close scrutiny and certified to a minimum level of vulnerability and penetration testing." [11, p. 12] The MCMC seems to take a holistic approach to secure IoT from both cyber and physical threats. For instance, it sees that while cyber security can help minimise service interruption, physical security would minimise theft and vandalism. Additionally, MCMC White Paper recommended some practical steps to be taken including (1) incorporating "security in the device security programme," (2) introducing "certification scheme on vulnerability and penetrability of IoT systems and devices" and (3) cooperation with agencies such as cybersecurity and police to safeguard IoT. [11, pp. 12-13] These steps and measurements suggested by the regulatory agency (MCMC) are important and workable and thus they should be followed by IoT stakeholders in order to reap the benefit of IoT and avoid its drawback. All the above shows the important of security of IoT and the concern about it in the Roadmap and other relevant documents issued by the relevant authority in the country.

B. IoT Privacy Concern

Like security, privacy in the IoT sphere has also been seriously considered by the Roadmap and other relevant documents among the concerning issues that could impede

implementation of IoT [3]. This is so because IoT technology has facilitated the aggregation of enormous types of data about ordinary citizens, consumers, organizations and groups and such data can be used as a means to discover people's interests and visited places. [12] Moreover, apart from facilitating the aggregation of countless data about individuals (e.g., tooth-brushing, refrigerators and fitness tracking devices can reveal tooth-brushing habits, types of food and activities of persons), IoT challenges the social norms and expectations that distinguish between privacy in public and private places. [13] For example, IoT bring monitoring technologies (e.g., surveillance cameras, location tracking) that are usually found in public places to private places such as home and personal cars. [13] These and other privacy challenges justifies the Roadmap concerned about privacy of the IoT users when it stated that "connected devices can communicate with consumers, transmit data back to companies, and compile data for third parties such as researchers, healthcare providers, or even other consumers." [3, p. 23]

Regarding privacy challenges, the MCMC Report asserted that solving issues related to privacy and security is an important for flourishing IoT. It is also emphasized protecting privacy and certainty of legal rules relating to data collection and flow as this could promote the end users' trust and confidence in IoT. To overcome IoT challenges to privacy, the MCMC Report recommended developing some strategies to promote transparency, enhance security and observe privacy, among other things. Additionally, the MCMC white paper acknowledged that data protection could be an issue in IoT and thus it recommended working with the department of personal data protection. [11] More importantly, the MCMC Report viewed that "the existing privacy guidelines imposed on operators can also be applied to IoT applications and services." [10, p. 19] The idea of applying existing privacy guidelines to IoT services and applications is an important innovative idea that could help fill the gap of IoT regulatory aspects. Even though the words of the MCMC statement seems to mean service providers, the idea can arguably be furthered to include applying provisions of PDPA 2010 and its sub-regulations to IoT.

It can be said that the emphasis of the Roadmap and the MCMC documents on the necessity of taking privacy and security into account when dealing with IoT are clear evident that the ignorance of the security and privacy could affect IoT implementation. This leads us to discuss the current legal provisions or legislation applicable to data protection in the country. This will be done in the next section.

IV. Current Legal Response

The most relevant legislation to be looked at for ensuring security and privacy of IoT is arguably be the PDPA 2010 as this Act is most important legislation dealing with data protection in the country. The PDPA establishes seven principles (s. 5-12 of the Act) to be implemented in processing personal data in commercial transactions. The Act makes contravention of these principles as an offence punishable by a fine, or imprisonment or both (s. 5 (2) of the Act). The following is a brief discussion of these principles.

1- The General Principle

The General Principle, while acknowledging personal data as either sensitive or non-sensitive data, mentions that personal data shall not be processed without the consent of the data subject or other legal grounds such as serving interests of the data subject or compliance with legal obligations, etc. [PDPA 2010, S 6 (1 & 2)]. As an illustration, this Principle mentions that personal data shall not be processed unless the processing is (1) for legitimate purposes related to the activity of the data user; (2) the processing is necessary for that purpose and (3) the data itself is adequate and not excessive for the said purpose [PDPA 2010, S 6 (3)].

2-The Notice and Choice Principle

This particular principle could be considered as the most important principle in the virtual world. In fact, it "has been the dominant approach to regulate the Internet." The importance and relevance of the notice and choice principle is that it obliges the data user to give 'written notice' to the data subject informing him about the processing of his personal data, the purposes of such processing, rights and obligation of the data subjects and how to contact the data user for executing these rights, the means available for limiting data processing, the third parties to whom the personal data is disclosed or might be disclosed and such like [PDPA 2010, s 7 (1)]. Moreover, this principle asserts that the written notice shall be given as soon as practicable when the data subject is firstly asked to provide the personal data and when the data is firstly collected by the data user. In other scenarios, the written notice shall be given to the data subject before the personal data is used for new purposes or disclosed to a third party [PDPA 2010, s.7 (2)].

3- The Disclosure Principle

This principle prohibits disclosing personal data for new purposes or a new third party or parties without the consent of the data subject or other legal grounds mentioned in section 39 of the PDPA [PDPA 2010, s 8 (a&b)].

4- The Security Principle

This principle provides that the data user shall implement practical steps to protect personal data under his hands. The details of it will be discussed later on.

5- The Retention Principle

This principle prohibits keeping personal data after the purposes of its collection are fulfilled and obliges the data user to take reasonable steps to ensure destruction and deletion of personal data after the purposes of its collection are fulfilled [PDPA 2010, s.10 (1&2)].

6- The Data Integrity Principe

Data integrity mentions that the data user shall take reasonable steps to ensure the accuracy, completion, etc., of the personal data in his hand [PDPA 2010, s.11].

7- The Access Principle

This principle revolves around the necessity of giving the data subject the right to access, correct, up-date, etc., his personal data kept by the data user where such activities are acceptable under the PDPA [PDPA 2010, s.12]. See the table below for details of the seven Principles of PDPA 2010.

TABLE V. THE 7 PRINCIPLES OF PDPA 2010

Principle	Rules
General Principle	Personal data includes sensitive and non-sensitive data. Data shall not be processed without the consent of the data subject or other legal grounds. It shall also be adequate and not excessive in relation to its processing purpose.
Notice and Choice Principle	The data user shall give 'written notice' to the data subject informing him about the processing of his personal data, the purposes of processing, rights and obligation of the data subjects and how to contact the data user for executing these rights…
Disclosure Principle	Personal data shall not be disclosed for new purposes or a new third party/parties without the consent of the data subject or other legal grounds.
Security Principle	The data user shall implement practical steps to protect personal data under his hands.
Retention Principle	Data user shall take reasonable steps to destroy data after its collection purposes is fulfilled.
Data Integrity Principe	Data user shall take reasonable steps to ensure the accuracy, completion, etc., of the personal data in his hand.
Access Principle	The data subject has the right to access, correct, up-date, etc., his personal data kept by the data user in accordance with rules of PDPA.

The Roadmap counts "security and privacy challenges and data governance policies" [3, p. 25] among threats that should be dealt with to open the door for implementation of IoT in the country. This could be understood as acknowledgement from the Roadmap that the existing laws in the country need to be improved to cope with IoT challenges. This could be true as PDPA 2010 only applies to data processed in commercial transactions and excludes governmental bodies from its scope. (s. 2 & 3 of the Act). Moreover, the Act also exempts data processed by individuals for personal or household purposes and data processed for other specific purposes (s. 45 of the Act). All these and the challenges of compliance with data protection principles in the IoT environment lead the present researchers else where [14] to call for improvement of the current data protection regime in the country, especially the PDPA 2020, to enable it to over suitable protection to personal data processed in the IoT atmosphere.

It is also noted that the concern of data security can be addressed legally in several ways. Firstly, by imposing the principle of data security during the processing of personal information as ruled under section 9 of the PDPA 2010. By virtue of this provision, the whole cycle of data processing in IoT, be it data collection, storage, disclosure, usage and disposal, shall protect such data from any threat. Both technical and organisational security measures will need to be taken. That arguably includes all those security measures such as encryption, access control, data risk management and organisational data due diligence. While this provision is a great introduction to data security law in Malaysia, yet it has a limited scope, namely only restricted to personal data security.

V. CONCLUDING REMARKS

This short paper is devoted to investigate the notion of security and privacy in the Malaysian IoT Strategic Roadmap and the challenges posed by IoT to security and privacy of data. This achieved by analysing and examining the content of the Roadmap with focussing on the magnitude of the attention paid in the Roadmap to the issue of privacy and security and the reason behind that. The discussion also includes the existing legal framework available to the country to deal with concerning issues such as privacy and security of data in the digital age and the efficiency of such framework in the era of IoT. It finds that the Personal Data Protection Act is one of the primary legislations that help to achieve data security and privacy in Malaysian IoT environment despite the limited scope only to personal data. It calls for more research on how other legislation can help to achieve the objectives of IoT in Malaysia in near future.

ACKNOWLEDGMENT

The Authors acknowledge the use of grant No. FRGS17-018-0584 from the Ministry of Higher Education of Malaysia for the purpose of this publication.

REFERENCES

[1] O. Vermesan and P. Friess, Internet of Things- From Research and Innovation to Market Development, Aalborg: River Publisher, 2014, pp.243-244.

[2] M. Mardonova and Y. Choi, "Review of Wearable Device Technology and Its Applications to the Mining Industry," Energies, vol. 11, no. 3, 2018, p.547.

[3] Ministry of Science, Technology and Innovation, National Internet of Things (IoT) Strategic Roadmap, Kuala Lumpur: MIMOS Berhad, 2014.

[4] The International Telecommunication Union (ITU), "Recommendation ITU-T Y.2060, Overview of the Internet of things," (Geneva: the author, 2013), at 2 , ITU, https://www.itu.int/rec/T-REC-Y.2060-201206-I (accessed 15 Aug, 2020).

[5] Malaysian Communications and Multimedia Commission (MCMC), "*Internet Users Survey 2018*," (Cyberjaya, Selangor Darul Ehsan: MCMC, n.d.), at 4, MCMC, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf (accessed 15 Aug, 2020).

[6] N. Gillord, Information Security Management the Legal Risks, Sydney: CCH Australia Limited, 2009, p.7.

[7] M. Abomhara and G.M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security, vol. 4, 2015, p.65.

[8] K. Sailaja and M. Rohitha, "Literature Survey on Real World Applications Using Internet of Things," SSRN: https://ssrn.com/abstract=3165327 (accessed 15 Aug, 2020).

[9] U.S. Department Of Homeland Security, "Strategic Principles for Securing the Internet of Things (IoT)," Homeland Security, https://www.dhs.gov/sites/default/files/publications/strategic_principles_for_securing_the_internet_of_things-2016-1115-final....pdf (accessed 29 may, 2019).

[10] Malaysian Communications and Multimedia Commission (MCMC), "Internet of Things (IoT) Technical Regulatory Aspects & Key Challenges Technical Report" (2018), SKMM, https://www.skmm.gov.my/skmmgovmy/media/General/pdf/IOT-Technical-Regulatory-Aspects-Key-Challenges.pdf (accessed 15 Aug, 2020).

[11] Malaysian Communications and Multimedia Commission (MCMC), "Regulatory Challenges of Internet of Things (IoT)-White Paper" (2018), at 12, SKMM, https://www.skmm.gov.my/skmmgovmy/media/General/pdf/WHITE-PAPER-REGULATORY-CHALLENGES-OF-INTERNET-OF-THINGS-(IOT).pdf (accessed 15 Aug, 2020)

[12] C. Maple, "Security and privacy in the Internet of Things," Journal of Cyber Policy, vol. no. 2, 2017, p.172.

[13] K. Rose, S. Eldridge and L. Chapin, "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World," Internet Society, https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf (accessed 15 Aug, 2020).

[14] S.M.S. Ahmed and S. Zulhuda, “Data Protection Challenges in the Internet of Things Era: An Assessment of Protection Offered by PDPA 2010,” International Journal of Law, Government and Communication. 2019, pp.1-12.