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

Sidi Mohamed Sidi Ahmed **&** Sonny Zulhuda

The Sixth International Conference on Internet Applications, Protocols and Services (NETAPPS2020)

Conference Date:

2 & 3 December 2020

The Outline of the Presentation

- An Introduction
- **A**n Overview of the Roadmap
- Security & Privacy as Emerging Legal Issues
- Current Legal Response
- Concluding Remarks

I. INTRODUCTION

- 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 that rise 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. 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 Malaysian 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.

II. AN OVERVIEW OF THE ROADMAP

- According to the Roadmap, IoT is "Intelligent interactivity between human and things to exchange information and knowledge for new value creation". It is …encompassing three main technology components namely connected things with embedded sensors, connectivity and infrastructure, and most importantly analytics and applications"

- **IoT Advantages**: **IoT** economic potential is forecast to reach RM 9.5 billion in 2020 and the growth will continue to RM 42.5 billion thereafter. **IoT** could also serve the research community and help them commercialise R&D outputs. **IoT** **was also estimated to create more than 14000 high-skilled employment opportunities by 2020**

- **IoT Obstacles**: according the Roadmap obstacles include, among others, barriers to free market competition exist, rural adoption, technology phobia, technology complexity, data accessibility and security and privacy concerns.
- **The Roadmap 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, &
- (2) instituting a centralised regulatory and certification body to address privacy, security, quality and standardisation concerns.

III. SECURITY AND PRIVACY AS EMERGING LEGAL ISSUES

A. *IoT Security Concern*

Conventionally, information security aims to ensure availability, integrity and confidentiality of data. In the IoT, this is not easy to be done because

-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) &

-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."

Why IoT Security is a concerning issue?

-The complex of IoT security could explain the stress of the Roadmap on security of IoT.

-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.

SECURITY AND PRIVACY …cont…

B. IoT Privacy Concern

Privacy in the IoT sphere has also been seriously considered by the Roadmap among the concerning issues that could impede implementation of IoT. 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 to discover people's interests and visited places.

-IoT challenges the social norms and expectations that distinguish between privacy in public and private places. 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.

These and other privacy challenges justifies the concern expressed by the Roadmap 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."

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).

CURRENT LEGAL… cont…

- *Principles of Personal Data Protection as established by PDPA 2010*
- **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.

V. CONCLUDING REMARKS

- The paper is devoted to investigate the notion of security and privacy in the Malaysian IoT Strategic Roadmap and the challenges of IoT on 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 issues 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 PDPA 2010 is one of the primary laws that help to achieve data security and privacy in Malaysian IoT environment despite the limited scope of this Act as it only applies to personal data in the commercial sphere.
- It calls for more research on how other legislation can help to achieve the objectives of IoT in Malaysia in near future.

THE END

Thank you

&

السلام عليكم ورحمة الله وبركاته