Personal Data Protection Act 2010: Protection of Smart Home Users’ Information in Cloud System

Noor Ashikin Basarudin¹, Prof. Dr. Asmah Laili Yeon², Dr. Zuryati Mohamed Yusoff³, Assoc. Prof. Dr. Nuarrual Hilal Md Dahlan⁴ & Dr. Nazli Mahdzir⁵

School of Law, Universiti Utara Malaysia, Sintok, 06010 UUM Sintok, Kedah, Malaysia, noorashikin88@gmail.com¹, asmah485@uum.edu.my², zuryati@uum.edu.my³, hilal@uum.edu.my⁴, nazli@uum.edu.my⁵

Abstract: Cloud computing plays a significant role in ensuring well working system in a smart concept of house by offering numbers of services to the home owner especially in data management and data storage. However, immense of benefits offered by the cloud system are associated with numbers of uncertainties which has created the issue of confidentiality and data safety. This article adopts doctrinal legal study that analyzes the Personal Data Protection Act 2010 on the aspect of protection conferred to the cloud users. The overall finding shows that there is still loopholes in the Act which need to be looked into for the purpose of improvement as well as to cater the needs of legal policy in protecting personal data of smart home users in cloud.

Keywords: Smart Home, Protection of Personal Data, Cloud System.

Introduction

Over the years, we have experienced phases of technology evolution which has significant contribution in our life. The trend of technology application is not restricted to the usage of telecommunication alone, but has extended to the concept of housing development. Malaysia has introduced smart living concept that requires technology assistance in all aspect of daily routine from preparing meals, music entertainment, healthy lifestyle until the alertness of safety of the house. Installation of interconnecting devices in a house demand big data storage to enable massive amount of data information to be stored. Thus, the traditional of physical storage system is incapable of keeping such information for longer time and being managed in effective way due to its finite capacity. As an alternative, cloud storage system has been introduced to cater for the technology demand and needs in improving a great working system in a smart home. Nevertheless, cloud computing which is accessible through virtual system exposed to various types of cyber threat. It is among the big concern of smart home users when deal with technology devices due to numbers of personal data collected might leak out without their consent.

Issue of cybercrime and any hacking activity over the cloud falls under the purview of Computers Crimes Act 1997 while, in the aspect of data protection, the Personal Data Protection Act 2010 (hereafter known as PDPA 2010) is possible to provide protection for the users. Nevertheless, it has created a question whether the protection of personal data information and data stored in cloud will be treated the same way it is kept using the traditional physical storage system. Thus, for the purpose of this writing, laws related to personal data protection will be analyzed to look into the loopholes of the PDPA 2010 that requires room for improvement.

Methodology

This writing adopts doctrinal research concept by analyzing laws and regulations related to the issue of protection of security and personal data information of the smart home users in the cloud. A descriptive approach will be executed to examine PDPA 2010 and its compatibility to deals with the
issue. Whilst, an analytical and critical approach will also be implemented to specifically analyze the provisions contain in it and come with possible conclusion which is based on the facts established and the law considered.

**Results and Findings**

*(a) Technology in Smart Home*

Malaysian housing development has introduced a profound concept of a house equipped with technology devices to leave the best living experience to the owner which is known as 'smart home'. Smart home is a pattern of a house installed with advanced devices exist in a form of communications network, sensors, electronic and electric devices as well as few appliances which are controllable, accessible and remotely monitored using a smart phone or tab. The fundamental concept of smart home is referring to the ability of technological devices in linking with the existing network to ensure the good working system of a house. Smart home is distinguishable from a home that equipped with a standalone technological device operated via network connection in the house. A smart home may comprise of various devices that link to each other which can be accessed either from the central hub or outside the home.

The full function of devices in a smart home requires a complex embedded system to take in place which includes the communications network that allow the integration of devices, reliable sensors, intelligent system control management to collect and deliver the information, and smart features of the devices itself. In ensuring well working system in a smart home, central server that host the application must respond instantaneously without any interruption. Thus, cloud computing system comes into place to enable the auto-transformation and auto-switching of the tasks.

Smart home devices demand a reliability network to integrate among them to function according to what it should be. Due to that, Shaw in his opinion states, the most vital function of the devices requires higher speed connections as it fails to integrate, devices might work in a degraded manner which may lead to inconvenience of life of the owner. However, immense of fascinated benefits come along with the question of security. Security is the vital role in establishing a smart home due to its dependability on trusted network connection and massive personal data information collected and stored over the system. Security is a method of protection against any attacks on the system. In this aspect, security includes wide coverage of scope from confidentiality, information reliability, privacy protection and others. Network communication and cloud computing environment in a smart home is prone to hack due to its open system which may expose to wrongful activity such as unauthorized access, data leaks, eavesdropping, Dos attack, privacy intrusion, and attack against authentication. As the usage of cloud system and Internet of Things (IoT) are getting more compatible to cater the needs of network consistency, methods to mitigate the risk associated with cloud and IoT are important to ensure the system employed will run legally, ethically and in acceptable way as failure to address the implications attending these systems are potentially toxic.

---

2. Ibid.
(b) **Cloud System in Smart Home**

Cloud computing is a large-scale distributed computing paradigm simulated real traditional computer. It is massively abstracted in the aspect of service offered to the users, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet. It inspired by the cloud symbol to represent the virtual internet flow that simulate the physical computers to run any software, from operating system to end-user applications. Cloud’s structure comprises of hardware and software to ensure the effective management of the servers. Hardware tools include number of physical devices such as processors, hard drives and network devices being operated for storage and processing needs at the datacenters independent from geographical location. While, the software system is operating on virtual-based which function locationally independent, resource pooling and rapid elasticity. With the infinite capacity possessed by cloud computer, it is able to support the traffic congestion problem in the server. Thus, in the context of smart home, cloud function as a server resembles the usage of communication network which is able to receive and collect data from sensors or actuators, continue to be processed and the result will be carried out by the devices or any home appliances.

The control system of a smart home is based on intelligent control which would enable the house owner to manage and coordinate the devices through tab or smart phone. In this level, cloud offer services known as 'Software as a Service (SaaS)' and 'Infrastructure as a Service (IaaS)' to run smart home’s controlling software to adjust the devices according to the needs of the users. Software as a Service (SaaS) is a software deployment model where applications are remotely hosted by the application or service provider and made available to customers on demand, over the Internet which could be accessed from various client devices. Whist, 'Infrastructure as a Service (IaaS)' enables the user with processing, storage, networks, and other fundamental computing resources, and allow the consumer to deploy and run arbitrary software, which can include operating systems and applications. One such example of this is the Amazon web services which is considered as a cloud service provider (CSP) who is responsible in managing and maintaining data stored in the cloud server (CS). In most of the situation, cloud service provider is trusted and authorized to handle massive of personal data of individual or business entity either to back it up, update or managing the storage.

**Cloud and Legal Security Protection**

Security is a method of protection against any attacks on the system. In this aspect, security includes wide coverage of scope from confidentiality, information reliability, privacy protection and others. In spite of the fact that technology is playing a significant role in establishing a smart home, the issue of privacy, security and confidentiality of individual data information should not be compromised. Information security is the basic requirement in the provision of cloud and IoT system that should be

---

8 Yuan, L. (2015, December). Study of Smart Home System Based on Cloud Computing and the Key Technologies. In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on (pp. 968-972). IEEE.
Personal Data Protection Act 2010 is treated as the main framework in protecting data of smart home users in the cloud system. Malaysia has taken steps in introducing the PDPA 2010 on 15 November 2013 to govern personal identifiable data collected in respect of a “commercial transaction”. Individual data stored in cloud service provider is considered as personal data alluded to the status of private capacity. However, the question of the applicability of the Act to cover on the protection of data in cloud is justified in reference to the nature of the exchange services of cloud system on a contract term, based on the agreement between cloud service provider and smart home users which bind both parties on certain obligations, terms and conditions. The agreement of both parties entitled the cloud provider with an authorized access over certain data to be processed. Thus, this Act is relevant to provide protection of any smart home users’ data stored in datacenter from being manipulated, transferred or altered.

The main aim of introducing PDPA 2010 is to prohibit any person who processes and has control over the processing of any personal data in this aspect is referring to cloud service provider (data processor) or any data user who jointly in common with other persons processes any personal data such as licensed insurer; legal, auditing, accounting, engineering and architecture firms; housing developers; medical and dental clinics from processing an individual’s personal data without their consent. In protecting the confidentiality of the personal data, express consent is required from data subject to make aware of data processing purpose, especially in the situation of any involvement of any sensitive personal data such as health, political opinion, religious beliefs, or any commission of offence. The Act prohibits individual’s personal data from being processed without consent of the owner unless it is for a lawful purpose directly related to the activity of the data user; the data processed is not excessive in relation to that purpose.

Establishing a contract or any agency relationship between cloud service provider and cloud users is significant for the process obtaining document as an evidence. Courts have determined that the legal right to obtains documents or information from another is through contract relationship as emphasized in the case of Covad Communs Co., v. Revonet, Inc., (2009), the courts provide some guidance on practical ability requiring that ‘balancing factors’ be taken into account including whether the discovery is “unreasonably cumulative or duplicative” and (2) whether the party seeking discovery had ample opportunity to obtain the information by discovery in the action.

Thus, Shcherbakovskiy on points that cloud users should make certain that the contracts they enter into with providers clearly explain the providers’ responsibilities with respect to discovery and other litigation subjects.

Although the provisions mention in PDPA 2010 is exhaustive to protect personal data of smart home users, however the main obstacle in applying this law is due to its non-applicability of it to govern

13 Malaysia, 2010, Personal Data Protection Act (Act 709), Section 4
15 Malaysia, 2010, Personal Data Protection Act (Act 709), Section 2.
16 Section 4 of PDPA 2010 defines data processor as any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.
17 Malaysia, 2010, Personal Data Protection Act (Act 709), Section 8.
18 Malaysia, 2010, Personal Data Protection Act (Act 709), Section 4.
19 Ibid, Section 6.
personal data being processed outside Malaysia.\textsuperscript{23} In this situation, it has waived the obligation of cloud service provider to ensure the confidentiality of the data since most the cloud datacenter and cloud service provider is located outside Malaysia.

Thus, a revision of the PDPA 2010 is necessary to cope with the advance of technology application in order to protect the technology users from being victimized by it. This issue, if not properly addressed, may impede the successful deployment of the cloud architecture as well as the objective of introducing the Act.

**Challenges Occasioned by the Cloud System**

The arising of cloud application together with the Internet of Things in today’s life has created changes in the cyber threat landscape. The massive scale of data exchanged over the internet has directed to a number of attacks and has introduced to an exponential exposure to security risks\textsuperscript{24} happened especially in virtual form. Among the issues that has caused concern of the cloud users includes data confidentiality, data integrity, data management by the cloud provider, and the tracing of criminal activity over the transferring of data. Cloud and IoT faced external and internal attacks that may obstruct the functions and its benefits. Internal attacks will give more effect compared to external attacks because it might involved with valuable and secret information, and also encompass of privileged access rights.

Data confidentiality is referring to the accessibility of authenticated and authorized information over the cloud from leak to the outsiders. The protected information includes personal data of individual in a smart home either the home owner itself or any visitors may also include sensitive information which should not be revealed regardless of request from parties that have interest over the data. In most of the situation confidentiality of data will be questioned whenever various integrating devices and applications are being placed together involved process of data management, data exchange or updating phase may open up to risks.

While on the issue of data integrity\textsuperscript{25}, it is upon cloud service provider to ensure data received will not be modified, fabricated or deleted. Smart home users relied wholly on the service provider to ensure their data is properly managed and protected from unauthorized access because data has been kept in center miles away from the original place of data sources.\textsuperscript{26} However, attack on data might also occurs during the process of data transfer which is known as eavesdropping attacks. In this situation, attacker may intercept the network and falsify the data before it reaches the recipient. It is more dangerous if attackers have control over the system which made the integrity of important information is no longer secured.\textsuperscript{27}

Due to changing nature of technology, criminals now are able to commit more high-tech crimes and such nature seems to be more complex as it increases created challenges in tracing the attackers and

---

\textsuperscript{23} Malaysia, 2010, *Personal Data Protection Act* (Act 709), Section 3(2).


\textsuperscript{25} Section 11 of PDPA 2010 states on data integrity which is referring to the data user that shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.


Criminal activity perpetrated over the internet is difficult to be tracked even if the criminals are able to be identified, the evidence will no longer be found with them which make the enforcement of law is getting complicated. Furthermore, on the matter of checking on the accuracy of data seems difficult because the cloud datacenter that receive bulk of information in every second is not being able to be audited at all time to trace its correctness as well as the possession of the data storage is no longer with the users has made the verification of correctness of outsourced cloud data becomes a big challenge. The concept of "data sovereignty" which refer to the specific data sovereignty laws limiting cross-border data transmission has to be determined due to the difficulties in acquiring information and evidence from cloud service providers caused by geographical nature of datacenter that placed outside the country of origin creates uncertainty on the applicable jurisdiction.

**Conclusion**

As the reliance of technology in managing today’s life is continuing to grow, an upsurge of security legal protection is also significant to be considered. Security is a framework consists of several components such as principles, policies, procedures, concepts, beliefs, and techniques necessary to protect system and data of the users against any threat. It is the vital role in establishing a smart home due to its dependability on trusted network connection. Since the usage of cloud system and the Internet of Things are getting more compatible to cater the needs of network consistency, methods to mitigate the risk associated with cloud and IoT is important to ensure the system employed will run legally, ethically and in acceptable way. Thus, the existing law should be made comprehensive to make the parties involved aware of their duty and obligation to ensure their right is protected.

**References**


Yuan, L. (2015, December). Study of Smart Home System Based on Cloud Computing and the Key Technologies. In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on (pp. 968-972). IEEE.


Malaysia, 2010, Personal Data Protection Act (Act 709)


Acknowledgement: the authors wish to thank the Ministry of Education Malaysia for funding this study under Trans-Disciplinary Research Grant Scheme.