SMART HOME USERS' INFORMATION IN CLOUD SYSTEM: A COMPARISON BETWEEN MALAYSIAN PERSONAL DATA PROTECTION ACT 2010 AND EU GENERAL DATA PROTECTION REGULATION

Noor Ashikin Basarudin, Asmah Laili Yeon, Zuryati Mohamed Yusoff, Nuarrual Hilal Md Dahlan, Nazli Mahdzir Author
School of Law, Universiti Utara Malaysia, 06010, Sintok, Kedah

Abstract
Security of data in cloud system plays a significant role in ensuring trust from the users. It is also a method of warranting 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 analyses the Personal Data Protection Act 2010 on the aspect of protection conferred to the cloud users and with reference to additional point that is well addressed in European Union General Data Protection Regulation. The overall finding shows that there is still loopholes in the Act which need to be looked into for the purpose of improving as well as to cater the needs of legal policy in protecting personal data of smart home users in cloud.

Keywords: *component; cloud system; Smart Home; Personal Data Protection Act 2010; European Union General Data Protection Regulation*.

INTRODUCTION

Over the years, we have experienced phases of technology evolution which has a 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, and 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.

Keeping eyes on the technology per se may bring great disaster without taking precaution of the vulnerabilities of application deals on the internet. Cloud system is basically accessible through virtual system which may expose to various types of cyber threat. Network communication in a smart home is prone to hack due to its open system may expose to eavesdropping, Distributed Denial of Service (DDoS) attack, privacy intrusion, and attack against authentication (Li et al., 2016), hacking activity, data stolen and data manipulation. 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.

In addition to that, the implementation of cloud technology system raises several legal issues such as the sovereignty of law to govern the diverging function and responsibility of local ownership and management to third-party service provider and the data protection of users.

Issue of data protection over the cloud falls under the purview of Personal Data Protection Act 2010 (hereafter known as PDPA 2010) which is possible to provide protection for the smart home 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, and whether the PDPA 2010 adequately address matters relates to cloud system storage.

Thus, for the purpose of this writing, Malaysian Personal Data Protection Act 2010 which provide protection to the smart home users' information in cloud will be analysed to look into the loopholes that requires room for improvement. Reference also be made to the European Union General Data Protection Regulation (hereafter known as GDPR) on several related sections specifically on the issue of the coverage of personal data, agreement on consent required in processing data subject, and the issue of protection conferred to data which is processed outside the original source of data.

RESEARCH METHODOLOGY

This writing adopts a doctrinal research concept by analysing laws and regulations related to the issue of protection of security and personal data information of the smart home users in the cloud. An analytical and critical approach will be implemented to specifically analyse the relevant provisions contain in Malaysian Personal Data Protection Act 2010 and The European Union General Data Protection Regulation to come with possible conclusion in protecting personal data information of the smart home user in cloud.

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 of the owner which is known as 'smart home'. Smart home is a pattern of a house installed with advanced devices exists in a form of communications network, sensors, electronic and electrical devices as well as few appliances which are controllable, accessible and remotely monitored using a smart phone or tab as illustrated in Figure 1. 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 standalone technological devices 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 (Balta-Ozkan et al., 2013).

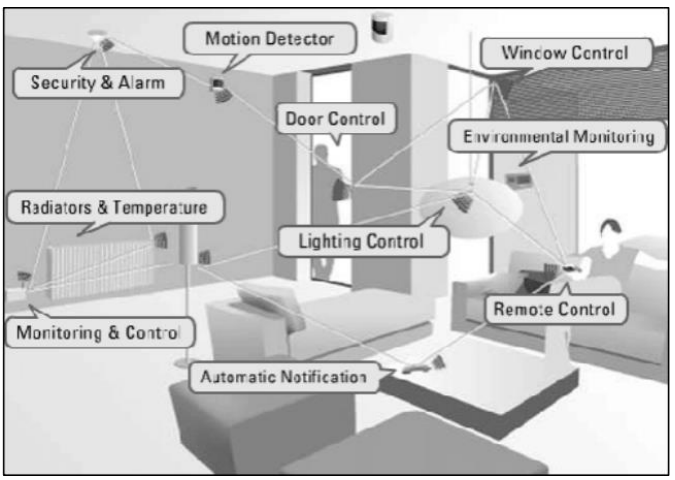

Figure 1. Smart Home Technology Automation

The systems and tools installed within the house will give full enjoyment and peace. The security system is regarded as the most important function in establishing a smart home. It holds a monitoring function to ensure the safety of people living in the house and the surroundings. Apart from that, smart home has potential in saving the energy efficiently. The system function as a medium for energy reduction which is able to automatically on or off based on the commands given through actuator or detector. Energy saving appliances may help in reducing the cost of electricity bills estimated one third lesser than the actual cost in the same size of a normal house by tracking the energy used and command it to use less. Smart home may also provide benefits for an elderly person who needs care and observation especially on medical rehabilitation. In an emergency, appliances within a smart home may alert the hospital directly to always ensure the safe condition of the residents (Robles et al., 2010).

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 (Robles et al., 2010). 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 require 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 (Shaw, 2015). 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 (Li, 2016) as failure to address the implications attending these systems are potentially toxic (Lillard, 2010).

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 (Anantwar et al., 2012) happened especially in virtual form. Among the issues that has caused concern of the cloud users includes data confidentiality, data integrity [8], 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 involve 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 (Personal Data Protection Act, Sec 11), 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 centre miles away from the original place of data sources (Jaiswal et al., 2015). 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 (Ryu & Kwak, 2015).

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 the evidence (Ravin, 2006). 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 datacentre 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 (Shrinivas, 2011). The concept of "data sovereignty" which refers to

the specific data sovereignty laws limiting cross-border data transmission (Vogel, 2014) has to be determined due to the difficulties in acquiring information and evidence from cloud service providers caused by geographical nature of datacentre that placed outside the country of origin creates uncertainty on the applicable jurisdiction.

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 (Ravin, 2006). 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. Security is a method of protection against any attacks on the system and the data itself.

In the absence of solid security of Internet of Things application, system attacks may lead to malfunctions of the devices and outweigh its benefits. In the concept of IoT, all devices will be connected to each other may possibly reveal flaws that can be exploited by the hackers. It has been predicted that a large number of integrated devices will be compromised to allow the well function of all devices. As 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 (Li et al., 2016). Thus, safeguard to ensure the robust security, privacy and reliability of the devices must be in place to ensure a long life cycle of it (Abomhara & Koien, 2014).

Apart from the issue of security of individual data in smart home, protection of such information is significant to be considered upon due to the status of individual information that is considered private in nature. It is well known that the nature of technology adopted in a home is invasive and the cloud system employed to hold bulk of individual information is inevitable to be hacked. The blending status of different concept of situation requires a balance between technology and its consequences which probably be protected through the enforcement of law. In terms of privacy, the concept of it comprised of various ways including right to confidentiality of communications, a right to be left alone, a right to control one's own life or a right to the protection of one's personal data [16]. Thus, in any issue of data intrusion will lead to the issue of privacy which possible of exposing someone's life and cause the degradation of the standard of the information. The grievance consequence will not only revolve on the information itself but may hamper someone's life in a way of injuring their credibility and reputation and also cause other defamation issue. Therefore, it is important to highlight on the protection addressed by the legislations to lessen the effect of it.

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 (Foster, 2008). It inspired by the cloud symbol to represent the virtual internet flow that simulates 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 data centers 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 (Anantwar, 2012). 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 (Yuan, 2015). The interconnecting devices may react independently by initiating action either with or without human involvement (Kalmar, 2016).

Smart meter and smart grid system is currently used and able to metering electricity in smart home. Its integrating system with the devices may help in reducing energy through details feedback of energy use, providing tips for saving energy and identifying high energy usage of certain equipment. These meters are also able to transmit information directly from the metered property to the utility company, potentially in near-real time and with a much higher detail of data with the assistant of the cloud system (Papakonstantinou & Kloza, 2015). Cloud may capture information delivered by the home devices and will be automatically uploaded into system as response to the actual activities in the home.

Smart home system requires high capacity of technology in bridging the infrastructure and clouds to ensure embedded devices function efficiently. Adoption of cloud in smart home encompasses of several infrastructures such as internal system connection, intelligent control and uniformity of interface which operated based on the cloud available services model such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Zissis & Lekkas, 2012) to help users to run applications and store data online. System connection is the core component in smart home to integrate all appliances either through Ethernet, Bluetooth and Wi-Fi. Connection of all devices relied so much on the fast speed of the wireless network for example to trigger an emergency alarm, it needs the information sent from the sensor and actuator which is able to detect any unwanted situation such as any movement or any unusual thing happened in the house.

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 (Jaiswal, 2015). Whilst, '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 (Zissis & Lekkas, 2012). One such example of this is the Amazon web service (Jaiswal et al., 2015) 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.

Though the cloud usage in storing smart home users' data is significantly beneficial, as it is susceptible, method of mitigating it risk has to be introduced which among that would be in a form of enforcement of law and policy.

MALAYSIAN PERSONAL DATA PROTECTION ACT 2010

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 (IoT privacy). Information security is the basic requirement in the provision of cloud and IoT system that should be addressed and made available in the provisions of law rather than added on later once needed in place.

As response to the needs, Malaysia has taken steps in introducing the Personal Data Protection Act 2010 to regulate the processing of personal data collected and processed for commercial purposes and all other matters connected or incidental to consumers' personal data. Cloud data system is an emerging method of data collected virtually that possibly addressed by PDPA 2010. Section 4 of the Act states on the definition of "personal data" to include the meaning of any information in respect of commercial transactions, any information in respect of a commercial transaction which is: a) being processed; b) recorded with the intention that it should be processed; or c) recorded as part of a relevant filing system (Personal Data Protection Act 2010, Sec 4). The "relevant filing system" is referring to the personal data including any information or opinion as far as it relates to an identified or identifiable living person and processed both manually and automatically (General Data Protection Regulation 2016, Sec 4). Automatic means any data gathered or stored in a traditional computer or on the online database (Munir, 2010). Though the Act does not specifically direct its applicability on cloud system, the nature of data processed electronically makes it falls within the scope of the PDPA 2010.

The main aim of introducing the PDPA 2010 is to prohibit any person who processes and has control over the processing of any personal data which is referred to cloud service provider (Personal Data Protection Act 2010, Sec 4) 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 (Personal Data Protection Act 2010, Sec 8) 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 (Personal Data Protection Act 2010, Sec 4). 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 in which the data processed is not excessive in relation to that purpose (Personal Data Protection Act 2010, Sec 6).

The processing of personal data should be commercial in nature regardless of its contractual or non-contractual form which may include exchange of goods or services, agency, investments, financing, banking and insurance. However, it creates an issue of determining the commercial matters in the processing of personal data due to the circumstances of difficulties in drawing lines between the commercial and non-commercial activities (Munir, 2010).

Such matters have been illustrated in European case concerning Article 8 of the European Court of Human Rights (ECtHR) which shows that it may be difficult to completely separate matters of private and professional life case. In *Amann v. Switzerland*, authorities intercepted a business-related telephone call to the applicant. Based on that call, the authorities investigated the applicant and filled in a card on the applicant for the national security card index. Although the interception concerned a business-related telephone call, the ECtHR considered the storing of data about this call as relating to the private life of the applicant. It pointed out that the term 'private life' must not be interpreted restrictively, in particular, since respect for private life comprised the right to establish and develop relationships with other human beings. Furthermore, there was no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life'. Such a broad interpretation corresponded to that of Convention 108. The ECtHR further found that the interference in the applicant's case had not been in accordance with the law since domestic law did not contain specific and detailed provisions on the gathering, recording and storing of information. It thus concluded that there had been a violation of Article 8 of the ECHR.

In light of the above case, we might presume that individual data stored in cloud system is considered as personal data alluded to the status of private capacity. However, in the Malaysian context, since the PDPA 2010 excluded the protection for the processing purpose of personal data for non-commercial matters, it might be presumed that there is no protection granted to the smart home users' information in cloud in the situation whereby data is stolen or misused. Rather smart home user would choose to have contract and agreement with cloud service provider to bind both parties with certain obligations, terms and conditions, still the processing of such data does not fall within the scope of commercial purpose. Thus, such personal data is not justified to be protected under the PDPA 2010.

The idea of the intended agreement is to entitle the cloud provider with an authorized access over certain data to be processed and to provide protection of smart home users' data stored in datacentre from being misused, manipulated, transferred or altered without consent of the data owner. However, it must be borne in mind that, most of the cloud users are not aware on the significant of concluding of agreement between cloud service provider which consequently may waive their right in terms getting protection or in recovering any damages if data being manipulated.

Besides that, establishing a contract or any agency relationship between cloud service provider and cloud users is significant for the process of obtaining document as evidence. Courts have determined the legal right to obtains documents or information from another is through contract relationship as emphasized in the case of *Covad Communs Co., v. Revonent, Inc.*, 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, in *Shcherbakovskiy* it has made it clear 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.

Another main obstacle of the PDPA 2010 is due to its non-applicability to govern personal data processed outside Malaysia (Personal Data Protection Act 2010, Sec 3(2). Smart home users' information seems not to be that important as compared to the information of big organization, yet the individual's information is still valuable and through the protection given shows the law recognize the individual's right to privacy which is the fundamental right of human being. Thus, ignoring this issue may waive the obligation of cloud service provider to ensure the confidentiality of the data since most of the cloud datacentre and cloud service provider is located outside Malaysia.

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

General Data Protection Regulation was proposed by European Commissioner as EU legal framework for data protection to replace Data Protection Directive (hereafter known as DPD) of the European Union. GDPR is seen as the current and influential regulation in the field of data processing legislation that addresses the protection of personal data. The introduction of new regulation is important in ensuring the compliance of common cloud computing usage patterns with legal constraints and requirements to protect the consumers against any data misuse and to preserve their data privacy. The main objectives of reforming the data protection rules is to modernize the EU legal system for the protection of personal data to respond to the use of new technologies; to strengthen users' influence on their personal data and to reduce administrative formalities; as well as to improve the clarity and coherence of the Member States' rules for personal data protection (Kalmar et al., 2016).

Reference to EU legal framework is significant in terms of adopting guidelines to protect personal data transferred over the cloud system. However, for the purpose of this discussion, comparison will only be made on three main aspects which are the coverage of GDPR to include personal data, the need of creating agreement between parties and the law that address the transfer of data across country.

GDPR is enacted to protect personal data of individual regardless of it connection to commercial matters. It is more relevant to protect personal data of individual in this aspect is referred to data of smart home users as GDPR applies to the processing of personal data wholly or partly by automated means and in a form of manual filing system (General Data Protection Regulation 2016, Art 2). In *Bodil Lindqvist*, the Court of Justice of the European Union (CJEU) held that: "the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions or hobbies, constitutes the 'processing of personal data wholly or partly by automatic means' within the meaning of Article 3 (1) of Directive 95/46."

GDPR has stipulated the meaning of personal data which includes any information relating to a natural person who can be identified, directly or indirectly, by any reasonable means used by the controller or by any other natural or legal person, in particular to an identification number, location data, online identifier or to one or more factors specific to the

physical, physiological, genetic, mental, economic, cultural or social identity of that person (General Data Protection Regulation 2016, Art 4). Continuance from that, Article 9 of GDPR also has listed the 'special categories of personal data' that is prohibited from being process unless with several condition that allow the processor to do so (General Data Protection Regulation 2016, Art 9(2)). These exemptions include explicit consent of the data subject, vital interests of the data subject, legitimate interests of others and public interests (General Data Protection Regulation 2016, Art 9(2)). The special categories of personal data includes revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Unlike in the process of non-sensitive data, a contractual relationship with the data subject is not viewed as a general basis for the legitimate processing of sensitive data. Therefore, if sensitive data are to be processed in the context of a contract with the data subject, use of these data requires the data subject's separate explicit consent, in addition to agreeing to enter into the contract. An explicit request by the data subject for goods or services which necessarily reveal sensitive data should be considered to be as good as explicit consent. The extension of definition is significant to include data processed using advance technological methods which reflects changes in technology. Thus, the applicability of protection to cover matters not only confined to commercial purpose makes the GDPR relevant to significantly address protection and safeguard of the data of smart home user in cloud.

Pertaining to the contract or agreement that will require processor of the personal data to be putting alert on has also been highlighted in the GDPR which states consent of the owner of personal data should be freely given, specific, informed and unambiguous either through written statement, including by electronic means, or an oral statement. Consent is also considered in a form of ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct the data subject's acceptance of the proposed processing (General Data Protection Regulation 2016, Art. 32). Thus, the service provider will be an unauthorized person if there is indication that data owner is not consented to the processing of his or her personal data.

Another issue that creates fear of the smart home users is relating to the cross border transfer of information to cloud provider's country where the data is processed. The former DPD stated on the applicability of local low of the location of cloud data processed to govern matters arise. However, the inconsistency of the law of different countries and inadequacy of local law to govern that issue will cause variable. Thus, GDPR is introduced to uniformly govern the protection of data flow across country (Kalmar et al., 2016). Matters relate to information transfer to third countries or international organisations other than EU country are mentioned in Article 44 of GDPR. Any transfer of personal data shall take place only if the conditions laid down are complied with by the controller and processor. The conditions require data controller and data processor (Personal Data Protection Act 2010, Sec 2 to ensure the adequacy of the protection level of the country in terms of (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation,

data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data (General Data Protection Regulation, Art 45).

GDPR has significantly provided further protection on the data information especially to cater the needs of extra protection due to the emerging of technology usage. Thus, the new amendment of GDPR may give ideas on improving the law of personal data protection in Malaysia.

RECOMMENDATION AND CONCLUSION

Data information stored that relate to an official organisation and in the private individual home is different based on the weightage of its privacy status, in the situation whereby cloud storage system is vulnerable to hacking, personal data information in a house is important to be protected. The definition of personal data is not only limited to the name, identification card, address but deliberately a very broad one such as traceable information that will bring to the real person. In principle, it covers any information that relates to an identifiable living individual. Furthermore, data may also become personal from information that could likely come into the possession of a data controller. Thus, there is a need for individual information to be protected regardless of the status of the information. In the aspect of smart home, the system that hold information on the output behaviour of the owner that work to provide fully housing automation may store a lot of information about people which if exposed may prejudice their life. For example, the system has captured their daily routine, whereabouts, financial transaction that has been made and several other information. This type of information is vulnerable if intruded may open up to other criminal cases. For example, in the situation whereby the data processor reveal smart home user's information may leave traceable information to the other person, later give opportunity for the system of the home to be hacked which will later cause other types of problems.

In discussing the provisions provided by Malaysian Personal Data Protection Act 2010 and European Union General Data Protection Regulation, there are several significant differences between provisions in which some part of the PDPA 2010 are lacking of to provide protection to the cloud users. Thus, some of the provisions in the GDPR is suitable to be referred to for the purpose of extending the scope of protection to the cloud users in the smart home particularly. The most important part in highlighting the lacunae in the PDPA 2010 will be on the need to include the applicability of the Act to protect not only commercial data but also the non-commercial transaction. Non-commercial transaction is also known as 'personal

data' which bring the meaning of any data relating to a living individual which can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller (Information Commissioner's Office). Developing a smart concept of home deals with bulk of information relates to personal, family and household affairs in which all of the information is categorized as non-commercial transactions which is not applicable under the protection provided by PDPA 2010. Thus, the needs of inclusion of protection on personal data under the PDPA 2010 is significant to protect smart home user's information from any misuse of information and also to protect the fundamental right of individual as well as maintaining the right to privacy of natural persons during the processing of personal data. Besides, the idea of including the personal data under the said Act is to prevent from individual personal data from being transferred for the benefits of the other party without consent of the data owner.

Apart from the inclusion of the coverage for personal data to include non-commercial purpose in the PDPA 2010, it is also suggested that the employment of cloud service in the smart home system should be included in the contract and agreement specifying the duty and obligation of both parties including cloud service provider and cloud users. As referred to the method of implementation of agreement by GDPR, it has been made compulsory on the data processor to reach consent from the data owner which is freely given, specific, informed and unambiguous either through written statement, including by electronic means, or an oral statement before the processing of any personal data in which PDPA 2010 should give emphasis on. Although housing developer seems waved from bearing any obligation in securing the data of smart home user, yet they are still under the obligation of providing a reliable cloud service provider. Cloud service provider will normally be selected based on the requirements that suit the needs of types of data saving. In ensuring the protection of data, the developer has to be certain in choosing aspect of data location as it will determine the level of protection granted by the law of that jurisdiction or it should be based on the contract that clearly states the choice of territorial jurisdiction and the choice of law that is applicable in determining any dispute. The term of the contract must not favour only one side. It should be opened up to the negotiation so that the real objective of protecting the data of the cloud user will not be hindered. Among the matters that should be certain is on the intellectual property rights of the data, roles and responsibility of the cloud provider and data provider, and the liabilities of the cloud provider and remedies (Mohd, 2012).

The issue of data location is critical as it is an often regulated issue, which does somewhat go against the transparency principle of cloud computing and the concept of pooling storage resources (Fitzpatrick et al., 2012). It is significant to address the location of the service provider due to inapplicability of the local Act to govern the processing of data outside Malaysia which may hinder the purpose of protecting the information of smart home user in cloud. Information which is in intangible form, once transferred outside Malaysia will no longer protected by Malaysian law and it is subject to the country in which it currently resides. Thus, in the issue whereby the data will reside outside Malaysia, vendor of the smart home cloud provider must ensure the third country having kept all the data must have adequate level of protection during the processing data as suggested by GDPR. Although it may not seem like a significant issue, but when it comes to individual personal data, it is not something that would be considered secure. In suggesting that, cloud providers have to provide access to data to customers, regulators and auditors. It is because of the fact that they are holding all that information and these groups would like the ability to see where the information is being held.

Thus, in this situation, the data whereabouts should be addressed by the Act to ensure information of the cloud user is safe and the owner of the data may have accessed to their own information.

The most important thing is on the security system employed by the cloud service provider to trace any hacking or theft matters occurred in the system and the way of solving it. Although it is not within the power of home developer to monitor the cloud service provider system, still the service provider should be able to provide their web standards and details of the security features such as user authentication and authorization or administration controls known as encryption (Mohd, 2012). 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 (Li et al., 2016). Thus, the PDPA 2010 should be made comprehensive to make the parties involved aware of their duty and obligation to ensure their right is protected. A revision on the PDPA 2010 is also 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 law.

ACKNOWLEDGMENT

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

REFERENCES

"Determining what is personal data". Information Commissioner's Office. Retreived at https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf

Abomhara, M., & Koien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on* (pp. 1-8). IEEE.

Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 65. (ECtHR, 2000)

Anantwar, R. G., Chature, P. N., & Anantwar, S. G. (2012). Cloud Computing and Security Models: A Survey. *International Journal of Engineering Science and Innovative Technology (IJESIT) Vol*, *1*.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). The development of smart homes market in the UK. *Energy*, *60*, 361-372.

Bodil Lindqvist, CJEU, C-101/01, 6 November 2003, para. 27.

Covad Communs. Co. v. Revonet, Inc., 2009 U.S. Dist. LEXIS 75325 (D.D.C. Aug.25 2009)

Fitzpatrick, A., Mcgrath, M., & Lennon, R. G. (2012, October). Legal issues surrounding Data Storage on the cloud. In *Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania* (pp. 53-56). IEEE.

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008, November). Cloud computing and grid computing 360-degree compared. In *2008 Grid Computing Environments Workshop* (pp. 1-10). Ieee.

General Data Protection Regulation 2016.

Jaiswal, S., Patel, S.C. & Singh, R.S., (2015). Security Challenges in Cloud Computing. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1485-1492). IGI Global.

Kalmar, E. E., Kertesz, A., Varadi, S., Garg, R., & Stiller, B. (2016, August). Legal and Regulative Aspects of IoT Cloud Systems. In *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on* (pp. 15-20). IEEE.

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: a security point of view. *Internet Research*, *26*(2), 337-359.

Lillard, T. V. (2010). *Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data*. Syngress Publishing

Mohd N. F. A., 2012. "The cloud" is not a "black cloud", *Current Law Journal*, 1 LNS(A) xliii.

Munir, A B., 2010. The personal data protection bill 2009. *Malayan Law Journal Articles*. 1 MLJ cxix.

Vogel, P.S. (2014). "Is data localization a threat to privacy or the cloud?" *Internet, Information Technology and e-Discovery Blog* 28 January 2014, Retreived at www.vogelitlawblog.com.

Papakonstantinou, V., & Kloza, D. (2015). Legal Protection of Personal Data in Smart Grid and Smart Metering Systems from the European Perspective. In *Smart Grid Security* (pp. 41-129). Springer London.

Personal Data Protection Act 2010.

Robles, R. J., Kim, T. H., Cook, D., & Das, S. (2010). A review on security in smart home development. *International Journal of Advanced Science and Technology*, *15*.

Ryu, H. S., & Kwak, J. (2015, January). Device-based Secure Data Management Scheme in a Smart Home. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 231). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Shaw, S., (2015). Smart homes need reliable connectivity. *Smart Technology & Living*. Retrieved from http://raconteur.net/technology/future-of-smart-homes-across-the-world 15 / 04 / 2015

Shcherbakovskiy v. Da Capo Al Fine Ltd. The Second Circuit U.S. COURT OF APPEALS, (June 11, 2007).

Shrinivas, D. (2011). Privacy-preserving public auditing in cloud storage security. *International Journal of computer science nad Information Technologies*, *2*(6), 2691-2693.

Ravin, V. (2006). "Information technology & litigation: a general introduction to computer crime, information security and computer forensics." *Malayan Law Journal Articles 5 MLJ lvi.*

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.

Ziegeldorf, J.H., Morchon, O.G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728-2742.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.