INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 8, Issue 12, (2018) E-ISSN: 2222-6990

Personal Data Privacy Protection: A Review on Malaysia's Cyber Security Policies

Mohd Amiruddin Hamzah, Abdul Rahman Ahmad, Norhayati Hussin, Zaharuddin Ibrahim

Faculty of Information Management, Universiti Teknologi MARA, UiTM Selangor, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v8-i12/5251 DOI:10.6007/IJARBSS/v8-i12/5251

Published Date: 06 January 2018

Abstract

Personal data privacy is a crucial aspect of information management. Strategic information management must consider the data security and must take all the necessary practices to ensure personal data protected in a closed or open network environment. Data privacy legislation has been formulated by the government to ensure the ethics of handling sensitive information such as personal, banking and another aspect of information like health and medical information must be according to law stipulated by the acts. Malaysia as a growing electronic government provider in the region has adopted several legislation to ensure the enforcement of the data protection achieved the international standard to ensure global recognition especially by international business in enhancing foreign direct investment (FDI) and to protect local enterprises.

Keyword Information Management, Privacy Protection, privacy legislation, Malaysia Legislation, Public Key Infrastructure.

Introduction

Privacy is a concept coined by western scholars to ensure each person enjoys their freedom and exclusive rights to be secluded themselves from public or information about themselves. Herring (2016), mentioned that privacy could be regarded as bodily integrity where personal information about someone has to be protected from public knowledge unnecessarily to refrain from humiliation for such a person. Modern politics uphold the privacy, and as a result, the privacy law has been enacted to ensure the public trust and protection of misuse of information that could be lead into criminal and offences. Most of the modern country has a dedicated law concerning privacy protection and country like Malaysia, also formulated the privacy law as part of the country effort to adopt international standard in controlling privacy especially in today's connected world.

Concept of Privacy

The concept of privacy can be found in ancient Greek scholars work. This can be found in Aristotle's distinction between the public sphere of politics and political activity, the *polis*,

and the private or domestic sphere of the family, the *oikos*, as two distinct spheres of life, is a classic reference to a private domain (DeCew et. al., 2018). Warren & Brandies wrote Right to Privacy in 1890 which is a influential writing in law, mentioned on "right to life" and "right to be alone", has used that phrase as a definition of privacy. (Warran, et al ,1890). This has been interpreted to mean right of a person to choose seclusion from the attention of public if they wish and the right to be immune from scrutiny or being observed in private (Solove, 2008). (Bygrave, 2010) mentioned that privacy is a value that has its roots in the Western world. There an individual is considered as self-autonomous. He or she can advance claims for privacy. In contrast, privacy is a value that is less developed in the non-Western world.

The application of privacy in modern-day broadens not only in society but also on the Internet. As technology has advanced, the way in which privacy is protected and violated has changed with it. In the case of some technologies, such as the printing press or the Internet, the increased ability to share information can lead to new ways in which privacy can be breached. As the technology move forward, the definition of privacy become broader in line with current technology. This can be seen in the United States; new technologies can also create new ways to gather private information. For example, in the United States it was thought that heat sensors intended to be used to find marijuana-growing operations would be acceptable. Prior to 2001, it was thought that heat sensor to detect marijuana-growing operation would be acceptable. However, it was concluded in a case Kyllo v. the United States (533 U.S. 27) that the use of thermal imaging devices that can reveal previously unknown information without a warrant does indeed constitute a violation of privacy. (DeCew et al, 2018).

The Internet also could bring a new dimension in the way the personal privacy has been conducted. The introduction of Google as the biggest meta-search engine with a huge database stored almost everything posted on the web including photos, articles, twits or Facebook post and everything could be retrievable within mili-seconds. This could bring the bad situation especially for those who has been falsely prosecuted or seduced or defame which could damage their reputation through out their life as the story about the thing stored almost permanently on the internet.

Privacy Information

Information privacy, or data privacy (or data protection), is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them (Micheal et al, 1976). Beginning in the 1970s, worldwide attention has been focused on information privacy.

As the years have passed, concerns about information privacy have only increased. Two surveys conducted in 2008 and 2011 indicate that consumers are worried about privacy. Consumers-Union in a 2008 poll found that ''72 per cent of consumers are concerned that their online behaviour [is] being tracked and profiled by companies''. Harris Interactive, in a spring 2011 survey found about 98 per cent of 1000 smartphone users indicated that privacy was an important concern when using a mobile device, and over one-third of them (38%) identified privacy as their top concern (Miltgen et al. 2015).

Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Prashant (2009) mentioned that data privacy issues may arise in response to information from a wide range of sources, such as Healthcare records, Criminal justice investigations and proceedings, Financial institutions and transactions, biological traits, such as genetic material, Residence and geographic records, Web surfing behavior or user preferences using persistent cookies and Academic research. Thus, as privacy is a wide subject and involved in many aspect of our life, it is extremely important for the government to regulate the law concerning on privacy to ensure the freedom and personal aspect of life guaranteed by law.

Privacy Protection Framework

Mason (1986) in his work Four Ethical Issues of the Information Age has mentioned about 4 areas of privacy issues, namely privacy, accuracy, property and accessibility. Each of these substances provide the dimension on why the information has to be handled in proper way. Privacy refers to what information is held about the individual or an entity and weather the purpose of the information been kept. Accuracy refers to the correctness of the information as the inaccurate information could lead into disadvantage of an individual. For example, if the government is looking for a candidate that has a professional certificate in certain area for a post, inaccurate information in database could deny someone's opportunity to be appointed to that post. It is very important to have the system to cater all the information submitted and maintain its data integrity for accurate references. Mason also mentioned about the concept of data property to see who owns it and how far the ownership can be transferred. This is crucial to avoid the personal data or entity information being scammed or smuggled to other entity without permission. The last one is accessibility to see who is allowed to access the information, and under which conditions. The access is very important to ensure the purposes of the data kept are inline to the organization function. For example, misuse of the vehicle ownership in transport department could lead to criminal or misuse of information. These four (4) substances of privacy concern could be a solid framework for the government to formulate the protection policy towards data and information gathered electronically by government of private entity.

Fletcher (2001) provides an alternative perspective, raising these issues of concern for both the individual and the marketer in privacy. The first concern is transparency on which party is collected what information. The security of the information also an important concern to see how the data and information been protected once it collected by company. The third concern is about the liability to see who is responsible if data is abused or misuse. Although these three (3) substances was developed in the Fletcher work to study the privacy in marketing purposes, it can also been included in government perspective of handling data.

Data Protection, Legislation and Policies

As we discussed earlier, privacy is almost in every single aspect of people life. As government, by implementing the electronic approach in doing government business or regulating private sector, the government itself must be well prepared to ensure the

electronic approach is not turn into security threat to the country. Malaysia has enacted several legislations to control the digital activities to ensure its security and national digital agenda runs smoothly. Among the acts are Digital Signature Act, 1997, Communication and Multimedia Act 1998, Copyright (Amendment) Act 1997, Computer Crimes Act 1997, Telemedicine Act 1997, Electronic Government Activities Act 2007 and Malaysian Personal Data Protection Act 2010 ("the Act") came into force on 15 November 2013. Personal Data Protection Act 2010 came into force on 15 November 2013. The act aims to legislate the requirement to protect consumer information and put the liability to data user by law. The act has 146 sections in 11 parts. The act lays the 7 personal data protection principles.

General principle indicates that the personal data can only be processed with the data subject's consent. The act also requires the data subjects must be informed by written notice of, among other things, the type of data being collected and the purpose, its sources, the right to request access and correction, and the choices and means by which the data subject can limit the processing of their personal data. The protection of the data uphold in the third principle, disclosure in which personal data may not be disclosed without the data subject's consent for any purpose other than that which the data was disclosed at the time of collection, or to any person other than that notified to the data user.

The security principle where the data users must take practical steps to protect the personal data from any loss, misuse, modification or unauthorized access or disclosure, alteration or destruction. The personal data shall not be kept longer than is necessary for the fulfillment of its purpose to define retention principle and the act also provided that the data users must take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up to date to ensure its data integrity. The act also provides the access principle where data subjects must be given access to their personal data and be able to correct any personal data that is inaccurate, incomplete, misleading or not up to date.

The act governs personally identifiable data that is collected in respect of a commercial transaction. The employment related data would come to the purview of this act. The act however does not apply to credit reporting business carried on by a credit-reporting agency under the Credit Reporting Agencies Act 2010. The Malaysian Federal and State governments are also exempted by the act. In addition, the PDPA does not apply to personal data processed outside Malaysia unless such data is intended to be further processed in Malaysia. The act does, however, apply to parties not established in Malaysia but using equipment in Malaysia to process personal data other than for purposes of transit through Malaysia.

The act required certain data users group to be registered to use the data under approval of the commissioner. The user data class is Communications, Banking and Financial institutions, Insurance, Health, Tourism and Hospitalities, Transportation, Education, Direct Selling, Services, Real Estate and Utilities. The act also stipulated the fee required to be paid by the data user in order to register them under this legislation.

Since the act is not applicable to federal government agencies and state government agencies, how does the privacy of the citizen dealing with e-government application can

ensure their personal data protected by the government? Actually, there are several acts by Malaysia authority to ensure the government protection over their personal data to avoid misuse by the government agency upon their personal data. Malaysian Government, with it main agency in communication and multimedia industry, known as Malaysian Communications and Multimedia Commission play it key role in the regulation of the communications and multimedia industry based on the powers provided for in the Malaysian Communications and Multimedia Commission Act (1998) and the Communications and Multimedia Act (1998). Pursuant to these Acts, the commission is responsible to implement and promote the Government's national policy objectives for the communications and multimedia sector. It is government agenda to ensure data and information in e-government environment are safe and for the private perspective, the government has formulated legislation to ensure the privacy protection to the consumers.

Besides the government legislation, the government also provides the blueprint in handling with the electronic government to ensure the public and country safety. Government of Malaysia, by its various agencies has issued national blueprint on security concern in information management. Ministry of Science, Technology And Innovation (MOSTI) has endorsed National Cyber Security Policy (NCSP) as a blue print in handling cyber security concern of Malaysia.

This National Cyber Security Policy has been designed to facilitate Malaysia's move towards a knowledge-based economy (K-economy). The policy was based on National Cyber Security Framework that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects. The policy also addressed the risks to the Critical National Information Infrastructure (CNII) in which comprises the networked information systems of ten critical sectors: National Defence and Security, Banking and Finance, Information and Communications, Energy, Transportation, Water, Health Services, Government, Emergency services, Food and Agriculture. This national level security policy governs all moves taken by the government in their facility to ensure the government data and information are safe in this connected world.

Government Public Key Infrastructure (GPKI)

GPKI is the latest government initiatives to straighten security measure towards government data and information security to support government digital service initiative. Public Key Infrastructure is a combination of software, encryption technologies and services to help the government organization to ensure data and information are kept safe while online. The PKI protect the data and information secrecy, data integrity from tempering and to ensure the data readiness to be accessed. PKI has been implemented by the government since 2002 in electronic government projects. Government has appointed Malaysian Administrative consolidate all requirements on PKI under the GPKI flagship.

GPKI implementation is based on Government Public Key Infrastructure Policy which stipulated as all the implementation of GPKI in public sector govern by two main aspect or dimension which is technical implementation in digital certificate usage that concludes on risk assessment, technical requirement and evaluation. The other aspect is the

governance in managing the implementation in all level including the issuance of the certificate to the government agencies. The details on the implementation of GPKI has been circulated by MAMPU by a government circular dated 23rd Oct 2015 by the Chief Secretary to the Government. (PKPA Bil 3/2015). All the contractors that developed the government project need to embrace with this policy to ensure the software developed fulfilled with the security requirement in all stages of its implementation.

Conclusion

Government plays a vital role in ensuring the privacy of people. Government has formulated all necessary legislation to ensure the data protection become major focus in implementing electronic government to ensure the data and information remains intact to ensure privacy protection to the citizen. Government has enacted all requirements for the private sectors to ensure the privacy of data and information. On the other hand, the government also formulated the government strategy to ensure the implementation under the e-government flagship is safe to protect national interest. There are several other things that government to consider in future including the introduce special act for the electronic government to ensure the data both in public sector and private sector fully protected by the law to ensure protection on personal data privacy.

References

Bygrave, L.A (2010), 'Privacy and Data Protection in an International Perspective', Scandinavian Studies in Law, Vol. 56, pp. 165-200.

Gutwirth, S, (2002) Privacy and the Information Age, Lanham/Boulder/NewYork/Oxford/Rowman & Littlefield Publ.

Miltgen, H.C.L. & Smith. J. (2015), Exploring information privacy regulation, risks, trust, and behavior, Information & Management, (52)6, 741-759

Judith, D.C (2018), "Privacy", The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.), retrienved from https://plato.stanford.edu/archives/spr2018/entries/privacy/ on 11thNovember 2018

Dhillon, G., Oliveira, T., & Syed, R. (2018), Value-based information privacy objectives for Internet Commerce, Computers in Human Behavior, (87),292-307, https://doi.org/10.1016/j.chb.2018.05.043.

Herring, J. (2016), Medical Law and Ethics, London, Oxford University Press

Fletcher, K. (2001), Privacy: The Achilles' heel of the new marketing;. Interactive Marketing. (3)2 . 141-153 retrieved online at https://link.springer.com/content/pdf/10.1057/palgrave.im.4340123.pdf on 11 November 2018.

Alshehri, M. & Drew. S (2010), Implementation of e-Government: Advantages

and Challenges IASK E- ALT2010 CONFERENCE PROCEEDINGS. Retrieved at https://core.ac.uk/download/pdf/143886366.pdf on 11 September 2018

Mason, R. O. (1986). Four Ethical Issues of the Information Age.

MIS Quarterly, 10, 5-12. http://dx.doi.org/10.2307/248873

Mittal, Prashant (2009) Programme Management Managing Multiple Projects Successfully, India: GlobalIndia Pubns.

Ahmad, M. & Othman, R. (2006) Implementation of Electronic Government In Malaysia: The Status And Potential For Bettewr Service To The Public In Public Sector ICT Management Review, Oct 2006- Mar 2007 (1) 1, 2-9

Daniel, J.S. (2008). Understanding Privacy. Cambridge, Massachusetts: Harvard University Press. Warren and Brandeis (1890) "The Right to Privacy", Harvard Law Review Vol. IV, December 15, 1890 No. 5, retrievehttp://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html on11 November 2018.

MCMC, Our Responsibility. Retrieved online https://www.mcmc.gov.my/about-us/our-responsibility on 11 November 2018