Penerbit Akademia Baru

Journal of Advanced Research in Business and Management Studies
ISSN (online): 2462-1935 | Vol. 2, No. 1. Pages 39-49, 2016

A Study on Collection of Personal Data by Banking Industry in Malaysia

N. A. Mohamed Yusof[a], *N. A. Ahmad*[b] *and Z. Mohamed*[c]

UTM Perdana School of Science, Technology And Innovation Policy, Universiti Teknologi Malaysia Kuala Lumpur, Jalan Semarak, 54100 Kuala Lumpur, Malaysia

[a]*ashikin.kl@utm.my*, [b]*nurulain@iium.my*, [c]*zamrimohamed@utm.my*

Abstract – *Personal data is supposed to remain private to the person concern and only known to his close family and friends. The advancement of technology and invention of internet and information technology alter the balance between privacy and disclosure. Many personal data are surprisingly easily available, changing hands from one to another almost freely and are use in daily transaction without much control nowadays so much so personal data has become a commodity and tradeable asset. Data thefts, data breach, unlawful use of personal data as well as data trades off are among the examples of new problems stem from exchange of personal data. Banks are one of the industries that commonly ask customers for their personal details for official purposes before any transaction could be processed. The study examines the practice of banking industries in obtaining personal data, whether they comply with the legal provisions, whether customers given their consent freely and voluntarily free from any undue influence or duress.*

Keywords: Personal data, Privacy, Data sharing, Consent, PDPA 2010

1.0 INTRODUCTION

Article 12 of the Universal Declaration of Human Rights 1948 (UNHR)[1] declares that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." As a member country to United Nation, Malaysia has adopted the UNHR declaration at domestic level. Section Two of the Federal Constitution [2] being the highest law of the land duly acknowledges that right. Starting with Article 5 until Article 13, the Constitution grants every Malaysian for example the right to personal liberty, freedom of speech, right to assemble, freedom to form an association, free movement, right to life, and right to property. Though the provision on right to privacy is clearly missing from the Constitution, it does not mean that such right is less important or totally disregarded. Arguably the right to privacy is still guaranteed by inference of Article 5. Conversely in order to respect the liberty of a person or individual, one must also respect his privacy [3] Apart from that Malaysia does have legislations and common law principles protecting privacy-related interests on ground of trespass, breach of confidence, defamation, breach of contract and passing off.

The promulgation and enactment of Personal Data Protection Act (PDPA) in 2010 solidifies the above claims. The PDPA could be regarded as one of major breakthrough in Malaysian

legal scene especially in the context of cyber law and preservation of privacy. The law gives greater right to the individual with regard to their personal data and how it is handled or transmitted and shall ultimately lead to more secure, trustworthy electronic surroundings. Through the PDPA, Malaysia is arguably able to fill the long-standing gap in relation to protecting an individual's personal data. The PDPA now expects every party involves to protect the personal data of others as a legal socio obligation and by so doing strengthen the management of personal data.

The objective of protecting the privacy of an individual is important. Apart from the objective of producing integrated and responsible daily practice of e-commerce use, privacy helps to avoid unwanted and potentially intrusive interference in an individual's personal affairs. It could be divided into two categories, namely physical and mental. Physically, it determines the private sphere of an individual and to what extent the presence of third party may reduce that individual's independence as well as solitude [4]. This privacy is known as intimacy or solitude [4,5] Mentally privacy determines when, where, what and amount of information a third party may or should know about a person [6]. This type of privacy is called secrecy or anonymity [4,5]. In context internet lifestyle, privacy cannot be construed and limited to intimacy or secrecy any longer. Internet handles a vast number of quantities of information relating to individuals making it increasingly difficult and harder to maintain anonymity and privacy. Once the personal data is collected, processed, used, disseminated, shared or downloaded within the private and public domains they could be used in all kinds of ways. It is therefore the important for individual to have control and monitor his personal information or data. Internet and digital era offers a new dimension to privacy. In this context, privacy means informational autonomy or informational self-determination and it must allow individual to have autonomy and the right to choose and control over which of their personal data or information would or could be disclosed to whom and for what purposes [4] Summarily, information privacy has four main characteristics namely information, autonomy, personal identity or physical access.

Personal data refers to any kind of private information about a person, usually only known to owner, close family and friends [7]. The information may consist of his address, telephone number, identity card number, and race, date of birth, occupation, gender, health record, financial income, political affiliation and so forth. Some information like physical and mental health, political affiliation, religious beliefs, commission or alleged commission of any offences are more sensitive than others. Despite the sensitive nature of these data, they are surprisingly easily available, changing hands from one to another almost freely and use in daily transaction without much control nowadays. These activities widely array from applications for membership, registration or business activities. It becomes worse when these transactions occur across multiple sectors such as banking, retails, service providers, educational and health organizations. For instance, American Express has practicing a joint marketing venture with its partners such as hotel and airline companies [8]. A frequently travel cardholders will be offered a promotion from those companies for their next trip. How did American Express, the hotel and airline companies know that person and where did they get all those supposedly private information? The above example merely shows a tip of the iceberg about movement and flow personal data of upon collection.

As days pass by, the level of data privacy and security has become a matter to be concerned with [9]. New types of social problem and criminal offences never seen before during the pre-digital and computerized era began to emerge. Data thefts, data breach, unlawful use of

personal data as well as data trades off are among the examples of new problems stem from exchange of personal data [10]. This current situation raises questions as to whether the data subject knows his legal rights pertaining to the data, under what circumstances did he give the data away, does he give the data voluntarily, what happen to his personal data after releasing them to second party, can he change his mind, can he retract his consent and data, whether the manner of data collection complies with the legal provisions, how long could the second party keep the personal data, can owner and can a third party make profits from the data, if so can the data owner has a share to those data?

2.0 BACKGROUND FACTS

Across the globe numerous incidents have highlighted cases that relate to personal data and data privacy breach. According to the United States of America Identity Theft Resource Centre (US ITRC) data breaches occur across the sectors and the most affected sector is business (34.5%), followed by medical and healthcare sector (26.4%) in the last 10 years [11]. These sectors has a very large number of customers and naturally an equally very large if not bigger number of transactions involving exchange of personal data on daily basis. If care is not exercise, poor handling of data will lead to increase number of data breaches. For example America Online as a well-known mass media corporation has been condemned in their attempts to sell subscribers' telephone numbers to third party [10].Intel a semiconductor manufacturing company, another well -known brand name on worldwide basis was criticized for inserting a program capable of identifying users during the development of a new Pentium chip [10].

Data hacking and data on the move are the most common causes and types of data breaches. This shows personal data has certain financial value and hackers as a new type of professional criminals make monetary gain from hacking and invading the privacy of others [12]. The above findings is echoed and strengthened by various research conducted on the personal data and invasion of privacy [13-15] and customer data disclosure [16]. There are also studies which focused on e-commerce [17-19], on online customer privacy [20,10] and cloud computing [21-23] So far there is yet a study specifically focuses on the practice of banks in getting, collecting and storing personal data of their customers and the manners they collected the data from customers as data subjects.

2.1 The Impact from Data Abuse or Data Breaches

To a layman, the small and personal details about himself might not be important and have no commercial or financial value. This may explain of their relaxed and take for granted attitude in exercising care or protection towards protecting their personal data especially when the data merely contains his address, age or social background. As far as they are concerned, these data looks so "ordinary" and they are an open secret amongst friends or colleagues. It is unknown whether the public ever sees personal data as raw material, valuable and are tradeable like business organizations who do [24]. Those data helps them to identify their potential customers in terms of age group, income, social or financial background and so on. Such information helps them to strategize appropriate business strategy in targeting the intended group. It is unsurprising when some regard personal data as the new gold [25]. This also one of the pushing factors for rampant data theft, data abuse and data breaches [25]

Malaysia is not excluded from facing the same predicament. According to Utusan Malaysia [26], in the second quarter of 2014, there are 175,655,228 recorded cases involving data theft.

Journal of Advanced Research in Business and Management Studies
ISSN (online): 2462-1935 | Vol. 2, No. 1. Pages 39-49, 2016

It occurs across industries where retails industry shows the biggest data lost. The highest cases reported for data theft are for bad intention. According to Lai, Li, & Hsieh [27] data theft or abuse would leave a profound impact on the victim, particularly, business and security of the nation generally. As far as the victim is concerned, data breach and data abuse are tantamount to invasion of privacy and broad day light highway robbery. Naturally nobody likes to be a victim to both. For example through data theft, hacker could steal a person's identify, destroy his personal credit credibility, hinder online transactions or to take over his bank account. Such experience could be very traumatizing for the individual as an innocent victim. He may lose trust and confident in people, the system, less cooperative and feeling invaded, expose and vulnerable.

Business confidence is important for any business organization. It builds business value, reputation, brand name and subsequently loyalty amongst customers as well as business partners. Once a business organization losses the customers' confidence specifically the loyalty would evaporate too. In the long run, the customers would potentially leave and change to another service providers, affecting the business organization's financial incomes, interest and value of stock prizes, loss of existing market and competitiveness. It is therefore very important and crucial for business organization to protect their customers' or personal data from falling unto third party.

Undoubtedly sharing of personal data could promote, facilitate and ease the process for e-commerce and other online transactions. Not only it is convenient, the same also promotes efficiency and cost saving in terms of time, money and resources. All these are winning points for any ruling government. However since it is plausible to send personal information worldwide, those personal data would be equally shared on worldwide basis by unknown third parties. If the same is not regulated or controlled properly, it could become the biggest nightmare to the government in terms of public confidence, national and defense security and other forms of cyber-attacks [28].

3.0 PERSONAL DATA PROTECTION ACT 2010

The PDPA [29] was introduced in order to speed up the development of electronic connection and transactions such as e-commerce and e-business and in turn promotes Malaysia as a communication and electronic trade centre for multimedia and communications industries [30]. It is part of Malaysian grand plan to become a knowledge-based economy and society and achieve a fully developed status by 2020. The PDPA regulates the collection, holding, processing and use of personal data in commercial transactions and also to prevent malicious use of personal information. The PDPA is crucial for safeguarding the interest and privacy of individual by making it illegal for anyone, be it corporate entities or individuals, to sell personal information or allow such use of data by third parties.

The PDPA focusses on protection of personal data, defined as any information in respect of commercial transactions which:

a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

Journal of Advanced Research in Business and Management Studies
ISSN (online): 2462-1935 | Vol. 2, No. 1. Pages 39-49, 2016

c) is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system,

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of the data user, including any sensitive personal data and expression or opinion about the data subject (sec. 6).

Personal data may include any information or opinion as far as it relates to an identified or identifiable living person, processed both manually and electronically. PDPA therefore does not cover personal data used for non-commercial purposes (sec.4). To invoke protection under the PDPA, data must relate to any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance. According to Abu Bakar [31] the test to determine whether data is "personal data" is: can an individual be identified from the data, or from the data which is in possession of the data user? If the answer is "yes", it is likely that the data is personal data.

The processing of personal data is comprehensively defined in the PDPA to include all activities of a data user. It defines "processing" to mean collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data including-

a) the organisation, adaptation or alteration of personal data;
b) the retrieval, consultation or use of personal data;
c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or
d) the alignment, combination, correction, erasure or destruction of personal data.

As such, all data and confidential information of online consumers fall under the meaning of "commercial transactions". If a customer gives the name, address, contact number and other information to complete a transaction, that data or personal information is protected under the PDPA. The company receiving the information is under an obligation to keep the data and is only allowed to use or disseminate it with the consent of the data subject. Conversely, the data of a patient in relation to medical treatment does not fall under this definition as it does not have commercial features. Nevertheless, that data merits similar protection for the reason that it is easily abused and misused through online transactions. Similarly, the PDPA has no application to personal data collected through social media networking websites such as Facebook, Twitter and MySpace because that data is not a result of commercial transactions [32] The fact that this data is stored and held by foreign online providers which do not have local centres of data-processing, justifies its exclusion from the scope the Act (sec. 3(2).

4.0 SEVEN PRINCIPLES OF PERSONAL DATA PROTECTION

The PDPA provides seven core principles as outlined in Part II of the Act. These principles are framed by reference to international instruments governing the protection of privacy and trans-border flows of personal data. In any processing and handling of personal data the PDPA expects all data users to observe all data protection principles and any contravention of the principles results in an offence committed by the data user. Briefly the seven principles are as the followings;

4.1 Consent

A data user cannot process any sensitive personal data about an individual unless that individual is consenting to the processing of his personal data (sec. 6). The processing of the data must be in accordance with the provision of section 40. Data user has the obligation not to disclose the data except where the disclosure is in connection with what it was collected for or is directly related to the data user's activity (sec. 6(2)(a)-(f) and sec. 6(3)(a)-(c). Consent is the crux in processing personal data. The PDPA does not define consent. Consent in the PDPA could mean any freely given specific and informed indication of a data subject's wishes and his agreement to his personal data being processed and whether oral or implied [31]

4.2 Notice

A data user must give a written notice informing the individual data subject that his personal data is being processed by, or on behalf of the data user (sec.7). It must be given at the earliest opportunity to data subject. The notice shall include the purpose for which the personal data is being collected, and whether it is obligatory or voluntary for the data subject to provide his personal data.

4.3 Disclosure

If the data subject refuses to give his consent, the PDPA prohibits the data user from disclosing his personal data (sec.8). The data user may only disclose the personal data for the purpose or directly related purpose, which the data was disclosed at the time of collection. Also, the data user can only disclose the personal data to a third party or a class of third parties if data subject is informed of their existence at the time of data collection. The data subject's consent must be obtained before the personal data is processed by the third parties. However, section 39 provides for circumstances in which personal data may be disclosed like for crime prevention measures or legal investigation purposes even when such disclosure may contravene section 8.

4.3 Security Measures

The data user has legal duties to protect and safeguard data subjects' personal data by taking practical steps to implement appropriate security measures (sec.9). It is their legal responsibilities to take all necessary steps to protect any loss, misuse, modification, unauthorised and accidental access or disclosure, alteration or destruction of personal data. The precautionary steps must commensurate with the risk of processing the data while having regard to the cost of its implementation.

4.4 Deletion and Destruction

Processed personal data cannot be kept longer than is necessary (sec.10). Data user must take all reasonable steps to destroy personal data no longer required. However, this provision does not specifically mention the lifespan of personal data. Reasonably all personal data must be permanently deleted and destroyed once the purpose for which it was processed is done or achieved.

4.5 Data Accuracy

Data user must ensure that personal data is accurate, complete, not misleading, kept up to date, and related to the purpose (sec.11). It is the duty of the data user to guarantee the accuracy,

completeness and correctness of the data collected. The data user must also maintain that the data is current for its purpose, including any directly related purpose, for which the personal data was collected and further processed. It is essential to preserve the integrity of a data because inaccurate and incomplete data may have a direct or indirect effect on data subjects.

4.6 Withdrawal of Consent

A data subject must be given access (sec.12) to the personal data held by the data user and be able to correct, amend or delete personal data whenever it is inaccurate, misleading or not up-to-date. However, access or correction may be refused under the Act. (sec. 36 and sec.37).

5.0 COLLECTION OF PERSONAL DATA IN BANKING INDUSTRY

Banking industry is one the industries that commonly ask customers for their personal details and data so much so there would not exchanging personal data is regarded one of the core activities in banking sector. Apart from bank, retail industry, educational system, government agencies and health organizations are also among the industries actively collect, use and disseminate personal data [13,32]

There are several types of bank in Malaysia. Some of them are enacted under Banking and Financial Institutions Act 1989 (BAFIA) [33]and some others under the Development Financial Institutions Act 2002[34]. According to Bank Negara Malaysia [35], the licensed financial institutions are commercial banks, Islamic banks, international banks, international Islamic banks and other financial institutions such as ERF Sdn Bhd and Pengurusan Danaharta Nasional Berhad. Unfortunately the core businesses of these two institutions these are unrelated to this scope of study. Their activities are mainly in managing non-performing loan from financial institutions. Other type of banks in Malaysia is Development Financial Institutions (DFIs) which is enacted under the Development Financial Institutions Act 2002 [34]. The DFis is different from commercial banks since DFis are established for specific targets and markets. For instance SME Bank is set to help small and medium enterprise while EXIM Bank is to assist import and export businesses [35].

Most of the banking institutions in Malaysia except ERP Sdn Bhd and Pengurusan Danaharta Nasional Berhad provided almost the same services and products to the public. The usual and common bank services and products are retails banking, trade financing, treasury services, cross border payment, services as well as custody services [32,36]. As businesses expands and technology advances, these banks have wide their product and services to the public to include mobile banking, internet banking, credit and debit cards, auto pay and online shopping [38-40]. These activities directly or indirectly ask customers to disclose their personal data on almost every transaction for “official purpose” before their transaction could be processed. This also has excessively increased the burden on the banks to invest in tightening their data security in order to safeguard and protect the customers’ personal data from any data breach. Associated with these activities are the rising in data misuse, data abuse and data theft [41]. The seriousness of the above problem could be mapped from numerous previous studies in the area of personal data protection[21,42-44]. Most of these studies are noticeably focused on the issues arising from online privacy and internet usage.

So far there is no research on consent for data disclosure activities to third parties on either in online or offline platform. As correctly observed by Ong [45], there is no specific guidance

under PDPA specifically on the method of obtaining customer consent whether it's oral, written or implied. The legal silent may open an opportunity to irresponsible data user in abusing customers' ignorance or trust to gather and sell the information to third parties like retailers or marketers at certain price for their benefits. In this context, it is important to determine whether banks indeed as data users comply with the legal requirements of PDPA in dealing with personal data and if so, to what extend they protect the privacy and interests of data subjects in their commercial transactions.

6.0 PROBLEM STATEMENT

Logically the protection of personal data should increase along with the rapid advancement of technology and aggressive activities of collecting, use and disseminating the data. In view of the above, this research shall investigate the method or mechanism used by banks in Malaysia in getting customer consent for data disclosure.

7.0 RESEARCH OBJECTIVES

1. To investigate the current practice or mechanism used by commercial banks in acquiring customer consent for personal data disclosure to the third party.
2. To examine and determine whether the practice/mechanism is in accordance with the law provisions

8.0 RESEARCH QUESTIONS

1. What is the current practice or mechanism used by banks in obtaining consent from customer for their personal data?
    a. Is the method commonly practice by banks?
    b. Does the bank provide written privacy notice?
    c. Is the written privacy notice adequate?
    d. Does customer has the option to opt-out or to refuse?
    e. Does customer feel he does not have any option?
2. To determine whether the practice/mechanism is in accordance with the law requirements:
    a. What is the law applicable?
    b. What does the provision say about consent, disclosure, retention and use of personal data by third party?
    c. Does the bank comply with the requirement of the law?

9.0 CONTRIBUTION OF STUDY

The study could increase customers' level of understanding especially on their rights in protecting personal data. Such knowledge is important to reduce abuse or misuse of their consent and personal data by other parties. The outcome of this study shall be useful to Bank Negara Malaysia (BNM). It shall shed some lights on the current practices of the banking industries in protecting personal data, observes and analyses the full extent of legal compliance and detection of weakness in the management of personal data, if any. Thus, the outcomes of this study will assist BNM in improving the banks' regulations particularly in data protection

area. The result of this study is equally useful to decision maker and policy maker in improving existing policies, laws and regulation on protecting individual from any bias contracts or agreements as well as creating a more efficient and conducive environment for e-commerce and online transactions.

REFERENCES

[1] Universal Declaration of Human Rights 1948 (UNHR)

[2] Federal Constitution 1956

[3] M.N. Murni Wan, M.A. Ratnawati,Technology and the deterioration of right to privacy. International Journal of Asia Pacific Studies 7 (2) (2011) 35-50.

[4] N.M. Richards, (2005) "The Puzzle of Brandeis, Privacy, and Speech", Vanderbilt Law Review, 63(5) (2005)1295-1352, 1295-1296.

[5] M. Cooray, G. Radhakrishna, M.F. Mohd Emir Feizal, Right to automatic deletion of data in the electronic environment vs the privacy laws of Malaysia. Proceeding - Kuala Lumpur International Business, Economics and Law Conference 6, Vol. 4. April 18 – 19, 2015. Hotel Putra, Kuala Lumpur, Malaysia" ISBN 978-967-11350-4-4 (2015).

[6] G.R. Ferrera, S.D. Lichtenstein, M.E.K. Reder, R.C. Bird, W.T. Schiano, CyberLaw Text and Cases (2nd ed.). Thomson South-Western West.(2004)

[7] N. Ismail, E.L.Y. Cieh, Beyond Data Protection. Berlin Heidelberg: Springer.(2013)

[8] E.R. Foxman, P. Kilcoyne, Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues, Journal of Public Policy & Marketing 12 (1993) 106-119.

[9] A.J. Marcela Jr., D. Menendex, Cyber Forensics (2nd Editio.). New York: Auetbach Publications. (2008)

[10] E.M. Caudill, P.E. Murphy, Consumer Online Privacy: Legal and Ethical Issues. Journal of Public Policy & Marketing 19(1)(2000) 7-19.

[11] United States of America Identity Theft Resource Centre, 2015. www.usitrc.org/theft/data

[12] D.W. Wang, C.J. Liau, T.S. Hsu, J.K.P. Chen, Value versus damage of information release: A data privacy perspective. International Journal of Approximate Reasoning 43(2006) 179-201.

[13] J.B. Earp, F.C. Payton, Information Privacy in the Service Sector: An Exploratory Study of Health Care and Banking Professionals. Journal of Organizational Computing and Electronic Commerce 16(2) (2006)105-122.

[14] H. Jeff, J. Sandra, Information privacy : Measuring individuals ' concerns about organizational practices. MIS Quarterly: Management Information Systems 20(2)(1996)167-215.

[15] E.F. Stone, H.G. Gueutal, D.G. Gardner, S. McClure, A field experiment comparing

information-privacy values, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology 68(3)(1983) 459-468.

[16] E.M. Caudill, P.E. Murphy, Consumer Online Privacy: Legal and Ethical Issues. Journal of Public Policy & Marketing 19(1)(2000) 7-19.

[17] N. Olivero, P.Lunt, Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology 25 (2004) 243-262.

[18] R. Weiber, T. Kollmann, Competitive advantages in virtual markets –. European Journal of Marketing 32(7/8)(1998) 603-615.

[19] C. Yang, Analysis on protection of e-commerce consumer network privacy. Procedia Engineering 15 (2011) 5519-5524.

[20] J.A. Castañeda, F.J. Montoso, T. Luque, The dimensionality of customer privacy concern on the internet. Online Information Review 31(4) (2007)420-439.

[21] N.J. King, V.T. Raja, Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Review 28(3) (2012) 308-319.

[22] N. Kshetri, (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy 37(4-5) (2013) 372-386.

[23] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing. Information Sciences 258 (2014) 371-386.

[24] T.R. Peltier, Information Security, Policies, Procedures, and Standards. Boca Raton: Auetbach Publications (2002).

[25] M. Brandel, Spinning Data Into Gold. ComputerWorld. New York (2001).

[26] Utusan Malaysia,2014.www.utusanonline.my/archeve/2014/jenayahsiber. [1.18.2015]

[27[D. Lai, C.T. Hsieh, Fighting identity theft: The coping perspective. Decisio, F., Li, n Support Systems 52(2) (2012) 353-363.

[28] Y. Rais “Protecting your personal data” The Star Online. www.thestar.my (Malaysia, 12 February 2012).

[29] M.Y. Zuryati “The Malaysian Personal Data Protection Act 2010: A Legislation Note” (2011) 9 New Zealand Journal of Politics and International law 119.

[30] Parliamentary Hansard Report on PDPA, 2010.

[31] M. Abu Bakar “Personal Data Protection Act: Doing Well By Doing Good” [2012] 1 MLJ lxxxiii. xxx).

[32] J. Phelps, G. Nowak, E. Ferrell, Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing 19(1)(2000) 27-41.

[33] Banking and Financial Institutions Act 1989 (BAFIA)

[34] Development Financial Institutions Act 2002.

[35] Bank Negara Malaysia 2015

[36] Bank Negara Malaysia.The Central Bank and The Financial System in Malaysia - A Decade of Change (1st ed.). Kuala Lumpur: Bank Negara Malaysia.(1999)

[37] M.P. Lee, D. Samen, Banking Law (3rd ed.). Petaling Jaya: Malayan Law Journal.(2006).

[38] I. Akhisar, K.B. Tunay, N. Tunay,The Effects of Innovations on Bank Performance: The Case of Electronic Banking Services. Procedia - Social and Behavioral Sciences 195 (2015) 369-375.

[39] A.N. Berger, The Economic Effects of Technological Progress: Evidence from the Banking Industry. Journal of Money, Credit, and Banking 35(2)(2003)141-176.

[40] S. Mokhlis, Commercial Bank Selection : Comparison between Single and Multiple Bank Users in Malaysia. International Journal of Economics and Finance 1 (2009) 263-273.

[41] B.W. Schermer, The limits of privacy in automated profiling and data mining. Computer Law and Security Review 27(1)(2011), 45-52.

[42] M.S.M. Ariff, L.O. Yun, N. Zakuan, K. Ismail, The Impacts of Service Quality and Customer Satisfaction on Customer Loyalty in Internet Banking. Procedia - Social and Behavioral Sciences 81 (2013) 469-473.

[43] C. Barclay, C. a., A comparison of proposed legislative data privacy protections in the United States. Computer Law and Security Review 29(4) (2013) 359-367.

[44] J. Strauss, K.S. Rogerson, Policies for online privacy in the United States and the European Union. Telematics and Informatics 19(2)(2002) 173-192.

[45] R. Ong, Data protection in Malaysia and Hong Kong: One step forward, two steps back? Computer Law & Security Review 28(4)(2012) 429-437.