PERCEIVED KNOWLEDGE AND PRACTICE IN PERSONAL DATA HANDLING

NURUL 'AIN BINTI AHMAD

UNIVERSITI TEKNOLOGI MALAYSIA

PERCEIVED KNOWLEDGE AND PRACTICE IN PERSONAL DATA HANDLING

NURUL 'AIN BINTI AHMAD

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia

DECEMBER 2020

DEDICATION

This thesis is dedicated to my beloved parents, *Ahmad bin Saad* and *Noriah binti Abdulah* who taught me that the best kind of knowledge to have is that which is learned for its own sake. Without their care and support, this thesis would not have been the same as presented here.

It is also dedicated to my husband, *Suri Mahyuni bin Mohd Ali* and my daughter, *Aleesya Surfina* who never left my side and have supported me throughout the process. Both of you are my cheerleaders.

ACKNOWLEDGEMENTS

First and foremost, I would to thank Allah (SWT) for giving me the strength and wisdom to complete this thesis.

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Associate Professor Datin Dr. Nooraini Othman, for her encouragement, guidance, critics and friendship. This thesis would not have been possible without her valuable help and support.

I am also very thankful to my lecturers, Professor Zamri, Associate Professor Dr Nor Asyikin, Associate Professor Dr Marhanum, Dr Mazlan, and Dr. Nahg Abd Majid for their guidance, advice and motivation.

I am also indebted to the Ministry of Higher Education (MOHE) for funding my Ph.D study. I would also like to thank the staffs at Razak Faculty of Technology and Informatics and UTM Library for providing all assistance requested.

My fellow postgraduate students should also be recognised for their support, Yuzlina, Siti Kamariah, Fazni, Rizawati, Hasliah and others. My sincere appreciation is also extended to all my colleagues and others who have provided assistance on various occasions. Their views and tips have been very useful indeed. Unfortunately, it is not possible to list all of them in this limited space. Last but not least, I am most grateful to all my family members.

ABSTRACT

The banking industry is one of the most active industries in collecting vast amounts of personal data daily. Advancements in information and communication technology have directly made the process of personal data handling, which encompasses the processes of collection, usage, storage and dissemination of personal data, to become a lot easier. These developments, however, posed new threats to the individual's liberty and information privacy in case of a data breach or data abuse. This study is conducted to gain further understanding of the situation by investigating the current practices used by banks while dealing with customers' personal data and also examines the level of perceived knowledge among bank personnel and customers regarding personal data handling. An individual with good perceived knowledge is believed to exercise the best practices to secure the data from unwanted threats. Moreover, this study observes whether good perceived knowledge has effects on practice, specifically in personal data handling. This study adopts a quantitative approach, in which primary data were collected through a survey method. The respondents are divided into two groups; with a total number of 228 and 263 bank personnel and bank customers, respectively. This study utilises the Rasch Measurement Model for research instrument validation and SEM AMOS version 22 for data analysis. The findings indicate that the Malaysian bank current practices comprise all seven data protection principles as stipulated under PDPA 2010; attesting that the institutions fulfil the regulations. Bank personnel were found to have good perceived knowledge in personal data handling as compared to bank customers who are not meeting the level of good perceived knowledge scale. These findings justify the increasing number of cases in data abused recently. The result of the findings also verifies the significant effects of perceived knowledge towards practice in personal data handling, as noted in both groups of respondents. Two models of personal data handling have been established as the outcome of this study. They are the 'Personal Data Handing Model for Bank Personnel' and the 'Personal Data Handling Model for Bank Customers'. The present study is useful as it highlights the efforts made by the banking industry to protect customers' personal data. The results of this study contribute to the improvement and implementation of the Personal Data Protection Act (PDPA) requirements within the banking industry.

ABSTRAK

Industri perbankan merupakan antara industri yang aktif mengumpul data peribadi pelanggan secara harian. Kemajuan dalam bidang teknologi maklumat dan komunikasi telah menjadikan pengendalian data peribadi seperti pengumpulan, penggunaan dan penyebaran data semakin mudah. Walaubagaimanapun, ia memberi ancaman baharu terhadap kerahsiaan maklumat mahupun individu itu sendiri jika terjadi kebocoran maklumat atau salah guna data peribadi. Dalam memahami situasi tersebut, kajian ini dijalankan bertujuan untuk mengenal pasti amalan semasa yang digunakan oleh bank semasa pengendalian data peribadi pelanggan di samping mengkaji tahap pengetahuan dalam kalangan kakitangan bank dan pelanggan bank terhadap pengendalian data peribadi. Individu yang mempunyai pengetahuan yang baik dipercayai mampu mempraktikkan pengendalian data daripada disalahguna oleh pihak tidak bertanggungjawab. Selain itu, kajian ini juga mengenalpasti sama ada pengetahuan yang baik dalam pengendalian data peribadi mempengaruhi amalan yang dipraktikkan. Kajian ini menggunakan kaedah kuantitatif iaitu data primer dikumpulkan melalui proses kajian tinjauan. Responden kajian ini terbahagi kepada dua kumpulan iaitu kakitangan bank seramai 228 orang dan pelanggan bank seramai 263 orang. Model Pengukuran Rasch digunakan untuk pengesahan instrumen kajian dan SEM AMOS versi 22 digunakan bagi analisa data kajian. Dapatan kajian menunjukkan bahawa amalan semasa bank-bank di Malaysia merangkumi kesemua tujuh prinsip perlindungan data peribadi seperti yang termaktub dalam Akta. Ini menunjukkan bahawa pihak bank telah mematuhi peraturan undang-undang dalam pengendalian data peribadi pelanggan. Dapatan kajian merekodkan kakitangan bank mempunyai tahap pengetahuan yang baik dalam pengendalian data peribadi berbanding dengan pelanggan bank yang tidak mencapai tahap pengetahuan yang baik. Ini memberikan gambaran jelas bahawa dengan pertambahan kes melibatkan data peribadi yang telah disalahgunakan pada masa ini. Hasil dapatan kajian mengesahkan bahawa pengetahuan yang baik dapat mempengaruhi amalan dalam pengendalian data peribadi. Ini dibuktikan dalam kedua-dua kumpulan responden. Dua model pengendalian data peribadi telah dihasilkan daripada kajian ini yang diberi nama 'Model Pengendalian Data Peribadi bagi Kakitangan Bank' dan 'Model Pengendalian Data Peribadi bagi Pelanggan Bank'. Kajian ini berjaya menyoroti usaha yang dilakukan oleh industri perbankan untuk melindungi data peribadi pelanggan. Dapatan kajian ini juga dapat menyumbang kepada peningkatan dan pelaksanaan persyaratan bagi Akta Perlindungan Data Peribadi (PDPA) dalam industri perbankan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AVE	-	Average Variance Extracted
CFA	-	Confirmatory Factor Analysis
CFI	-	Comparative Fit Index
DFI	-	Development Financial Institution
EFA	-	Exploratory Factor Analysis
KMO	-	Kaiser-Meyer-Olkin
MI	-	Modification Indices
MNSQ	-	Mean-Square
PDPA	-	Personal Data Protection Act
PCA	-	Principal Component Analysis
PtMC	-	Point Measure Correlation
RMSEA	-	Root Mean Square Error of Approximation
SEM	-	Structural Equation Modelling
SPSS	-	Statistical Package for the Social Sciences
Z-Std	-	Z-Standard

LIST OF SYMBOLS

χ^2 -   Chi-square

χ^2/df Relative chi-square

$\leq$ -   Less than or Equal to

α -   Alpha

LIST OF APPENDICES

xix

CHAPTER 1

INTRODUCTION

1.1 Introduction

The issue of privacy and disclosure of personal data are usually intertwined. The intertwining gets more complex in the digital era. The Internet, the computer, social media and online transactions alter the balance between privacy and disclosure, so much so, privacy rights have changed into serious threats (Wu, 2014). Personal data refers to any kind of private information about a person like the address, telephone number, identity card number, race, date of birth, occupation, gender, health record, financial income, political affiliation, usually only known to the owner, close family and friends (Noriswadi Ismail and Cieh, 2013). It is the very kind of information any individual prefers to always keep private. Despite their sensitivity, a lot of these data are surprisingly easily available, changing hands from one to another almost freely and used in daily transaction without much control (Warso, 2013; Capistrano and Chen, 2015; Kong and Xiao, 2015). These array of activities from applications for membership, registration or business activities (Jai and King, 2016) occur across multiple sectors such as banking, retails, service providers, educational and health organizations (Reidenberg, 2000; Graham *et al.*, 2016).

When accessibility to data is just a click away (Cellary and Rykowski, 2015) it may inadvertently encroach into the individual's privacy, exposing him more to data thefts, data breach, and data trades off (Caudill and Murphy, 2000). Everybody should have knowledge on how to protect their personal data from those threats. Individuals with knowledge especially in personal data handling are more aware in ensuring his personal data is treated in a reliable way and would be able to notice if something was amiss. According to Wiig, (2003) knowledge of the individual would enable him to perform sense making, decision making, problem solving, implementations as well as monitoring in any situation. It is important to have knowledge in handling personal

data because security, integrity and protection of personal data are the fundamental factors to shift our country from a manufacturing-based economy to high value knowledge economy through the support of information and communication technology (ICT) infrastructure (Rais Yatim, 2012).

The knowledge could be gained by observing, learning by example, as well as modelling of or following the practices of others (Hayes, 1978; Thorsten, 2015). As explained by Sarabia and Obeso, (2012), imitation is accepted in many businesses. He gave example of firms that imitate each other in the introduction of new processes and new products, in the adoption of management strategies and even in entry to new markets and timing of investments. The act of imitating or modelling is a learning process where knowledge is gained by observing the actions and practices of others. For instance, customers of a bank could acquire knowledge on personal data protection through dealings with the bank. Knowledge of personal data protection may guard a person from data abuse. Question remains on the level of individual knowledge regarding personal data protection especially among bank personnel and bank customers in Malaysia.

Chapter one of this study is organized in the following manner. The first part contains the introduction, background facts, and problem statement. The second part discusses the research objectives and research questions. The third part refers to the theoretical and conceptual framework of the thesis. The fourth part refers to the scope and significance of study as well the definition of terms.

1.2 Background of Study

Personal data handling in banks encompasses data collection to data use, data dissemination, data disclosure and data retention. Banks deal with personal data all the time, upon opening a bank account, applying for a loan, registering for a credit card and other services. Personal data are the must-give details requested by the bank and these data would be in bank database systems (Noriswadi Ismail, 2013). The data are processed by different divisions, departments, branches and corporate office of the

banks. The collaboration with other service providers in paying bills, loans, standing instructions and third-party transfers increase the risk of personal data to be misused.

In order to protect personal data in commercial transactions, all banks in Malaysia are required to comply with the Personal Data Protection Act 2010 (PDPA) in terms of customer personal data handling. Other than to comply with data protection principles stipulated in the Act such as general principle, notice and choice principle, disclosure principle, security principle, retention principle, integrity principle and access principle, banks also have to acknowledge customers on the data collection and processing activity through a written notice. The notice should be in the national language and the English language and is easily accessible to the customers.

The security of personal data does not rely on the legal Act alone as everybody should play their roles. For instance, in banking services, bank customers need to know the purpose of data collection whilst the staff ought to ask for permission from the customer before collecting any personal information. The knowledge of bank customers could be gauged from their awareness on their rights as a customer in personal data handing. In the first place, the bank is the party that should deliver the information to its customers on these rights. Every customer has the right to access his personal data as stipulated under PDPA, the right to correct personal data if the data is out of date or inaccurate, the right to withdraw his consent for data processing, the right to prevent processing if it is likely to cause damage to the data subject and the right to decide whether or not they wish to give their personal data to be used for direct marketing purposes (Farah, 2014). The establishment of these rights for data subject who is the bank customer is intended to safeguard the personal data from any wrongdoing and abuse.

A lack of knowledge on the importance of personal data protection would harm the individual himself. Cases of personal data misuse and abuse could be reached anywhere and it happened almost every day. A distribution of breached data record across the world has portrays Malaysia is among the high cases in data breach. The records are compiled by Breach Level Index since 2013. It is stated, approximately 40 million cases of data breach since 2013 from Malaysia alone from the total of 9.7

billion worldwide. It is quite a big number for our country. As reported by New Straits Times online, the details for about 30 million passengers of Malindo Air, an Indonesian Lion Group Malaysian subsidiary have been posted in online forums and the leaked databases were up for sale on the dark web (Reuters, 2019). Two former employees of its e-commerce contractor were responsible for the information leakage. This is an example of data misuse by data users who were supposed to protect the data but did the exact opposite. Astro, a satellite television and radio operator in Malaysia reported a data breach exposing the customers' MyKad details such as names, identity card numbers, dates of birth, gender, race and address (Shankar, 2019). The company confirmed they were working with the authorities to address the breach and expressed regret when it happened for the second time. The breach in June 2018, involved 60,000 Astro IPTV customers' personal data. According to Utusan Malaysia (2015) there were 175,655,228 recorded cases involving data theft in the second quarter of 2014. Data thefts occur across industries with the retail industry suffering the biggest data lost. The million Ringgit land scam at various land offices at Kuala Lumpur, Johor and Penang revealed how the culprits invaded the privacy of targeted land owners (Nizam Yatim and Johari Syawal, 2007). In those cases, it was common for the accused to access the Land Registry Office to illegally access the file and data of targeted individuals in order to change the details of land tittles. Likewise , devious parties have no qualms in trading personal data such as the names, mobile telephone numbers, types of credit cards and issuing banks, and place of work of unsuspected consumers to third parties (Loh and Bedi, 2009). In Malaysia, these data are worth about RM100 for every 1000 names as in the case of the Citizen Declaration (Loh and Bedi, 2009). The list of one million names was allegedly extracted for the poll list of the last general election, where the accused served as a volunteer (P. Divakaran, 2016). Although the voters list is a public document, and available to all, the very basic principle remains. The culprit invaded the privacy of others and disrespected the citizens' human rights which is guaranteed by the law.

In October 2017, the Malaysian Communication and Multimedia Commission (MCMC) announced an investigation of personal data breach involving 46.2 million mobile number subscribers in Malaysia. The population of Malaysia is only around 32 million, but many have several mobile numbers. The list is believed to include inactive numbers and temporary ones brought by visiting foreigners. This leakage has

been described as one of the largest personal data breaches in the world and a lot was at stake in the incident (The Straits Times, 2017). From home addresses and MyKad numbers to SIM card information, the private details of almost the entire population may have fallen into the wrong hands. With this leak, Malaysians may be vulnerable to social engineering attacks and in the worst-case scenario, phones may be cloned. The MCMC also announced that 81,309 records from the Malaysian Medical Council (MMC), Malaysian Medical Association (MMA) and Malaysian Dental Association (MDA) were also breached. The MCMC identified the high probability of Jobstreet.com, Malaysian Housing Loan Application (MHLA) and the National Specialist Register of Malaysia as the places or sources of hacked personal data. Jobstreet database alone contains almost 17 million customer information, which includes the names, login names, passwords, email ids, nationalities, addresses and handphone numbers of candidates obtained between 2012 and 2013. Information of non-residents of Malaysia was also included. It is alarming that these data were advertised for sale on certain websites. The Inspector-General of Police (IGP) Tan Sri Mohamad Fuzi Harun said initial investigations revealed that the breach could have occurred during a data transfer, when a number of crooked employees of a company were able to take advantage of the situation (The Straits Times, 2017).

Invasion of privacy is a modern highway robbery in broad day light (Nor Ashikin *et al.*, 2016). Whilst the culprits make easy money, the victim suffers physically, mentally, socially and economically (Marcela Jr. and Menendex, 2008; Kong and Xiao, 2015). There is not much that consumers could do except to change their mobile phone numbers or SIM cards. Even that is almost futile since they cannot change or alter their other personal details. For example, the name, address, phone number, the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI), which are still tied to mobile phone devices are all out there (The Star Online, 2017b). According to Lai, Li, & Hsieh (2012) invasion of privacy is very capable of destroying the individual's personal credit and financial credibility. The unlawful leakage of information (Matzner, 2014) may unnecessary expose the victims (Ball *et al.*, 2012), leaving them vulnerable, and in many instances damage their reputation dignity, liberty and peace of mind (Tene and Polonetsky, 2013). They may lose their trust and confidence in people, the system and become less cooperative with the system or government. This also explains why the society in

general and private individuals in particular must be vigilant in ensuring their privacy rights are protected at all times. To be vigilant, one should prepare himself with good knowledge. By having good knowledge, it easier to practice the dos and don'ts while handling over personal data. The increasing numbers and seriousness of personal data breach and privacy issues in the digital era have been proven by various research conducted on personal data and invasion of privacy (Stone *et al.*, 1983; Jeff and Sandra, 1996; Earp and Payton, 2006), customer data disclosure (White, 2004), e-commerce (Weiber and Kollmann, 1998; Olivero and Lunt, 2004; Yang, 2011), on online customer privacy (Caudill and Murphy, 2000; Castañeda *et al.*, 2007) and cloud computing (King and Raja, 2012; Kshetri, 2013; Wei *et al.*, 2014).

The above concerns are very serious issues especially in the light of the rising number of data misuse, data abuse and data theft (Schermer, 2011). The seriousness of the problem has been highlighted by several studies on data protection and data privacy (Strauss and Rogerson, 2002; King and Raja, 2012; Barclay, 2013; Mohd Shoki Md Ariff *et al.*, 2013). However, most of these studies were focused on data protection issues from activities on the Internet. However, studies concerning customer personal data handling are rather limited. As far as Malaysia is concerned, there is yet a study that focuses on personal data handing and its relationship between perceived knowledge and practice. The matter to look into these two elements is whether having good perceived knowledge in personal data handling led to better practices or otherwise. This is important as the case on data breach is on rise and the culprits are among the individual who has the access to the data.

1.3 Problem Statement

Except for a few, most of the banks in Malaysia are private entity corporations answerable to shareholders and investors only. As corporate entities, they are normally profit-oriented. However, that does not mean that they can put less priority on the importance of personal data protection. Recent news in the media have highlighted some concerns on the safety of personal data collected and handled by financial institutions such as banks. How safe is public personal data kept by financial

institutions, credit card companies and banks? How competence bank personnel with regards to personal data handling? Are current practices in personal data handling is good enough to protect customers' personal data? Based on the requirements of "The Security Principle" clause of PDPA, it is high time for institutions to review their processes in data handling for a better and secured process of personal data. As far as customers are concerns, there is not much they can do other than to file a complaint with the Personal Data Protection Commissioner. However, customers could improve the situation by having better awareness and to be more alert of their rights. Generally, there is a need to know too, about how banks practice, implement and to what extent comply with the requirements of PDPA. There is still very little information available or research done on to the extent to which banks are specifically willing to assist their clients in preserving their rights while engaging in business transactions. Thus, this study investigates the current practice of banks on personal data handling whether the processes are according with the PDPA 2010.

In view of the abovementioned facts, a question arises whether this happens due to little perceived knowledge among bank personnel on personal data handling. Incompetence and unskilled personnel relatively correlated with the low perceived knowledge on the subject matter. It is important for bank personnel to possess good perceived knowledge in matters of personal data handling. Bank personnel especially the person who is responsible with data handling ought to be well-versed in the activities regarding personal data handling. He must understand each process and every detail and the steps to be taken as stipulated in the Act. There is a need to evaluate the perceived knowledge of bank personnel and with that this study examines the level of perceived knowledge among banks personnel on personal data handling.

Bank customer as well should know what it takes to secure his personal data starting from data collection to data processing. They should understand their rights as stipulated in the Act and know the channel to seek help should a problem arise. They should not only rely on other parties to secure their personal data because it could be seen some cases of data breaches were done by the individual who has access to the data. It is proven by the statement from the IGP on those matters as mentioned earlier under subheading 'Background of Study' above. Hence, this study as well investigates

the levels of perceived knowledge on personal data handling ranging from data collection to data use, data dissemination and data retention among banks customer in Malaysia.

The study also investigates whether there is effect of perceived knowledge towards practices in personal data handling. It be performed on both groups, banks personnel and banks customers. The result justifies whether it is a need to have good perceived knowledge in performing a good practice while dealing with personal data. The insight and the findings of this study are able to contribute in strengthening the protection of consumers' rights. It is useful for the academia and practitioners in firming the implementations on current practices by improving the areas with low practices and knowledge on it.

1.4 Research Objectives

The research objectives are as follows:

1. To determine the current practice by banks in Malaysia primarily in personal data handling consisting of consent, notice and choice, data disclosure, data security, data retention, data integrity and data access.

2. To identify the level of perceived knowledge among bank personnel in personal data handling ranging from consent, notice and choice, data disclosure, data security, data retention, data integrity and data access.

3. To identify the level of perceived knowledge among bank customers in personal data handling ranging from consent, notice and choice, data disclosure, data security, data retention, data integrity and data access.

4. To examine the effect of bank personnel's perceived knowledge towards personal data handling.

5. To examine the effect of bank customer's perceived knowledge towards personal data handling.

6. To propose a significant model on personal data handling among banks

1.5 Research Questions

1. What are the current practices by banks in personal data handling?

2. What is the level of perceived knowledge among bank personnel in personal data handling?

3. What is the level of perceived knowledge among bank customers in personal data handling?

4. Is there any significance effect of bank personnel perceived knowledge towards practice in personal data handling?

5. Is there any significant effect of bank customers perceived knowledge towards personal data handling?

1.6 Research Hypotheses

The purpose of a research hypothesis is to function as an empirical direction and benchmark in justifying the results and findings of the study (Bhattacherjee, 2012). It is also operated as a tentative answer to the research question (Senthilnathan, 2017). Hypotheses of study are generated into two types namely null hypothesis (H_0) and alternative hypothesis (H_1) (Mukesh *et al.*, 2013). The null hypothesis is a statement stated that there is no relationship exist between the value of parameter and the value of statistic. While the alternative hypothesis indicates there is a relationship between two selected variables in the study. In order to examine the effect of perceived

knowledge towards practice among the targeted respondents, this study develops two hypotheses as stated below. These hypotheses are predictions of the relationship between the variables. The prediction derived from the understanding of issues gathered in the study.

   i.   Hypothesis 1:

      H_0: There is no significant effect of bank personnel's perceived knowledge towards practice in personal data handing

  ii.   Hypothesis 2:

      H_0: There is no significant effect of bank customers' perceived knowledge towards practice in personal data handling

1.7 Conceptual Framework

A conceptual framework is an explanation of the main things to be studied such as key factors, concepts or variables either graphically or in narrative form (Miles and Huberman, 1994). The framework presumes there is a relationship among them. Meanwhile, Weaver and Hart (1988) defined the conceptual framework as the version of a researcher's map in his investigation; a useful tool (Leshem and Trafford, 2007). Through the conceptual framework, a researcher will be able to show the relationships of the different constructs to be investigated in the study (Mukesh *et al.*, 2013). The conceptual framework of this study is illustrated in Figure 1.1.
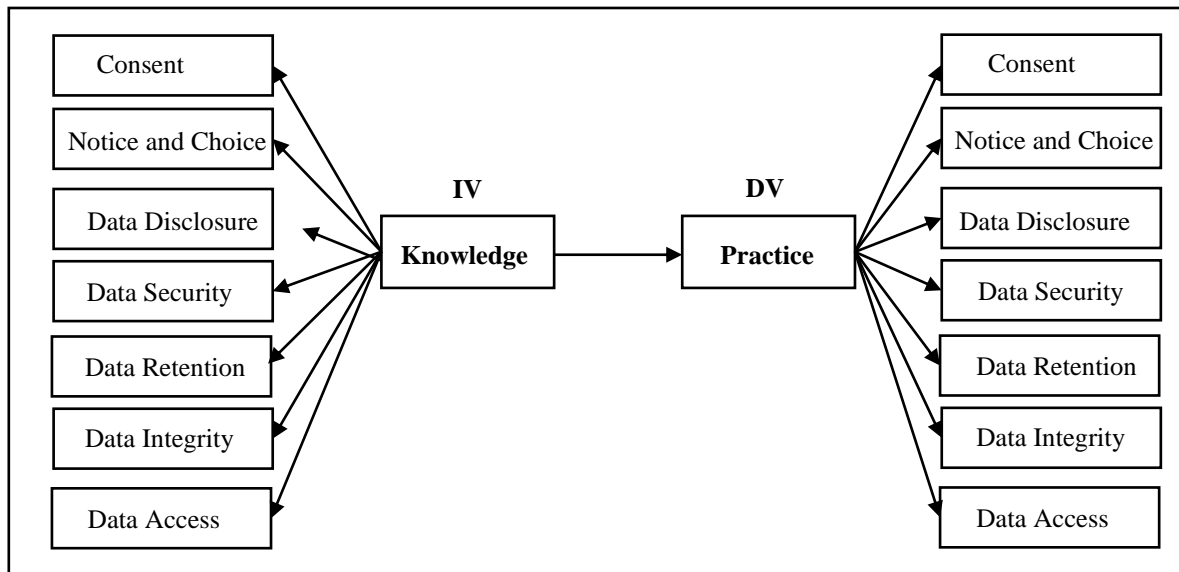
Figure 1.1   Conceptual Framework

To understand the overall picture, the study identifies the factors leading to personal data protection during bank transactions. Knowledge and practice on personal data handling among bank customers as well as bank personnel are the variables to be measured in this study. The knowledge is gained while experiencing the processes in various situations (Thorsten, 2015). The individual with knowledge should be capable of making more effective decisions as knowledge has been identified as an important component in decision-making (Robb and Woodyard, 2011). Stone et al., (1983) concluded that the more the individuals value information privacy, the less the control they believe they actually have over personal information. The study also revealed that the greater the degree of control the individuals believe they have over personal information, the more positive they are in their attitudes about such control. It shows knowledge has a significant impact on individual's belief towards his personal data protection.

Meanwhile, a study by Dawood, Hassali, & Saleem, (2017) summarized that the lack of knowledge among the public was associated with inappropriate practices by the practitioners. Although the study was carried out on medicinal use among patients in Malaysia, the key findings show a strong relationship between practice and knowledge. The study suggested that health policymakers design better strategies to help the public especially in raising their awareness on medicinal use while medical

11

practitioners should play a major role in educating their patients. In the context of this study, the perceived knowledge of bank customers could be influenced by the practices in banks itself from the beginning of data collection to the end of the transactions. When there are insufficient practices specifically during personal data handling, the gain in perceived knowledge among customers may be very little or insignificant.

However, bank personnel are not only required to have knowledge in protecting customer's personal information, they should also be highly experienced, practiced and equipped with the necessary skills since the performance of an organization is determined by the quality and availability of pertinent knowledge by its people (Wiig, 2003). This knowledge is essential in decision making, implementation and monitoring of every task. By having knowledgeable personnel in bank services generally and data protection specifically, it would be manifested by the good practices in day-to-day activities. Wiig, (2003) concluded that good knowledge produces good organization performance and better knowledge leads to even better performance.

A knowledgeable and skilled bank personnel may inevitably perform a good practice in their routine job generally. With assurance, they are able to carry out the best exercise while handling customers' data as regulates in the banks' policies. A day-to-day activity in banks, which demonstrates bank personnel do take serious on the security of customers' personal data would indirectly become a learning by example to the bank customers. They gained knowledge on the process and flow of personal data protection from the observation of bank personnel good practices. Observation learning is the process of learning through watching others, retaining the information and then replicating the behaviours that were observed (Kendra, 2019). The explanation on this matter is further discussed in the next subheading of 'Theoretical Framework'. Thus, it is important for bank personnel to practice it right and correct as it may be imitated by the customers and it has been proved incompetence personnel led to the failure of safeguarding data (Czechowski *et al.*, 2019). Furthermore, carelessness is among the root cause to data leak (Garrison and Ncube, 2011). This is the reason bank personnel requires to have good knowledge to makes them capable in performing good practice. Failure to do so, would not only jeopardize

the security of confidential data but sending a false information on the process of protecting personal data to customers.

In order to measure the variables of this study, seven attributes were extracted from the data protection principles as shown in Table 1.1 and will be used respectively. Those principles are consent, notice and choice, data disclosure, data security, data retention, data integrity and data access as stipulated under Section 6 to Section 12 under the PDPA 2010. The principles are put in place to ensure that there is no misuse of personal data by data users which starts from the collection, holding, processing and use of data in commercial transactions thereto (preamble of PDPA, 2010). Arguably, consent is the main key towards personal data protection. It is the first indicator whether the activity is done with the knowledge and approval of the owner or person concerned or otherwise. It too could defuse any allegations of illegal interferences or intrusion. All the principles consist of the elements and actions that data users must obey. Failure to do so would directly or indirectly render the consent null and void and as a result infringes the privacy right of the data subjects.

Table 1.1   The Principles of PDPA 2010

No	Principles	
1	General Principle on consent	Data user must acquire data subject's consent for personal data processing
2	Notice and Choice	Data user should prepare a written notice to inform the data subject on the personal data disclosure to third parties
3	Data Disclosure	No personal data shall be disclosed to the third-party others than mentioned in Notice and Choice Principle
4	Data Security	Data user should protect the personal data from any loss, misuse, modification, unauthorized or accidental access of disclosure, alteration or destruction during the processing of personal data
5	Data Retention	Data user should ensure to destroy or permanently deleted the personal data if it is no longer required for the original purposes
6	Data Integrity	Data user shall ensure the personal data is accurate, complete, not misleading and up-to-date
7	Data Access	Data subject shall be given an access to correct the personal data if it is inaccurate, incomplete, misleading and not up-to-date

The banks which comply with legal provisions as being enforced by PDPA during personal data processing has possibly reduced the risks from data breach and misuse of data. This possibly resulted in increased good branding in terms of services as well as improved customer knowledge on the purpose of protecting his own personal data. A customer with knowledge of personal data processing is able to choose which information to be processed or not. With the knowledge of both parties, customers and personnel become more aware and alert if something is not right during data handling. When the awareness and knowledge of protecting the personal data becomes a norm, it is much easier for regulators in their enforcement and the data always be in safe hands. The development of personal data protection in Malaysia undergo great expansion and this country feasibly be a source of reference for other countries in personal data protection.

1.8 Theoretical Framework

The Social learning Theory is most commonly associated with Albert Bandura based on the studies of the principal causes of human behavior. This theory suggests that people has learnt new behaviors through reinforcement, punishment as well as observation learning of the social factors in the environment (Bandura, 1971). According to Decker (1986) this theory emphasizes on learning by consequences and becomes an integral part of behavioral change. The process of learning by direct experience is performed not only through the responses but is observed from the differential consequences as well. In other words, all these elements help in determining the desired behaviors of others.

There are three factors highlighted for this theory in determining human behavior namely cognitive factors, behavioral factors and environmental factors (Figure 1.2). Bandura described cognitive skills such as knowledge, expectations and attitudes, enable an individual to profit more extensively from experience. Song, Bij, & Weggeman (2005), defines knowledge as information validated by experience that has entered the human belief systems as rules for guiding actions. Thus, individuals with knowledge react accordingly with their experiences which may lead to positive

actions. An individual develops thoughts about which type of behavior is most likely to succeed among his actions. This kind of behavior successfully prevent the individual from performing the unwanted actions.

Thus, the second factor is behavioral factors which comprise skills, practices and self-efficacy of an individual. From the scope of this study, the more the customer experiences himself on the best practices by banks in personal data handling, the more the knowledge he gains in protecting his personal data from being misused. The practices of bank personnel in this context of study ranging from how they require consent from the customers for data collection, do customers understand the purpose of data processing, how long the data be in the bank database and do banks explain the safety measures for data security. These activities in the bank especially in personal data handling should be understood by the customer as well as it is their right to protect their personal data. Banks which are transparent with their customers may lose nothing, instead, they gain more respect and trust and become more reputable. Learning by examples as explained in the Social Learning Theory is be the base of the study. The customer learnt from examples set by the personnel or in other words they learnt from the practices by the personnel during any transaction thus enabling them to gain a clearer understand regarding personal data protection. In contrast, the low practice by personnel degrades the knowledge among customers who use their services and products. It is important for banks in practicing the correct procedure during data handling.

The final factor is the environmental factors namely social norms, access in the community and influence on others. The theory suggests that the environment or surroundings cause people to behave in certain ways. These factors may influence an individual to change his own environment. The example could be seen in learning by consequences. If the individual sees positive consequences from a particular type of behavior, he is more likely to repeat the behavior himself. On the other hand, if negative consequences are the result, he is less likely to perform that behavior. All these three factors describe how different factors determine human behaviors. The human behavior does not depend on any single factor alone but it is derived from different experiences or situations.
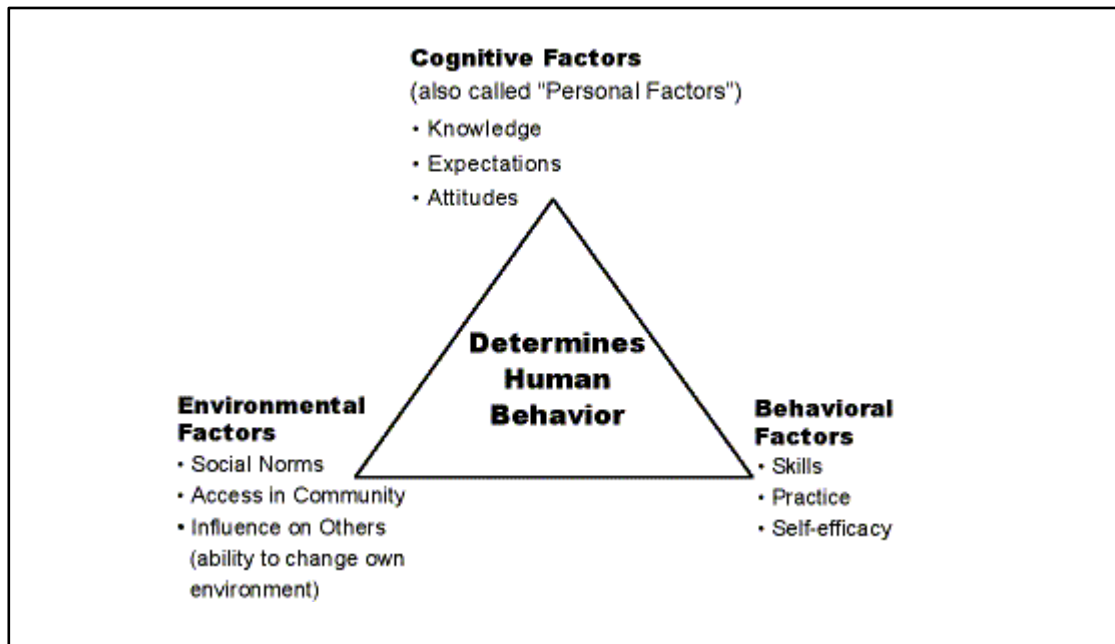
Figure1.2   Social Learning Theory (Bandura, 1977)

1.9 Scope of Study

The alarming issues in data privacy especially data breaches in the banking industry motivates this study to mainly investigate the current practices of personal data handling and to what extent these activities protect or encroach on the privacy of the data subject. It also investigates to what extent data users are willing to protect the privacy of data subjects and to what extent the proposed balance between rights of privacy and personal data disclosure is upheld whether in public or private domain. It assesses to what extent the banking industry, as a profit-oriented and monetary motivated industry in Malaysia is discharging their legal duties and responsibilities under PDPA in protecting the personal data of their customers and in so doing protect the customers' privacy.

The banking industry has been chosen because banks are amongst the organizations and business entities that offer both offline and online services to customers. Furthermore, in their daily business affairs, banks collect personal data from customers in almost every transaction for "official" purposes before that very transaction could be processed or proceed. The focus of this study is to examine the

16

current approach practiced by banks in acquiring customer's personal data as pre-requisite requirements for services and products of the banks. The study investigates whether there is an effect of perceived knowledge towards practice in personal data handling. The findings then verify whether the Social Learning Theory is synchronized with the study or otherwise.

This study focuses on individual customers only rather than business entities or organizations since individual customers are more vulnerable and most likely to succumb to pressures than business entities. To be more specific, this study wants to know how well the customers comprehend personal data handling. This has been done by measuring the level of perceived knowledge of personal data handling among the customers. Therefore, the study also examines the effect of perceived knowledge towards personal data handling. Quality and reliable work is always delivered by employees who have a comprehensive understanding and are thus knowledgeable about personal data handling.

The focus of this study is on the participants consisting of bank customers and bank personnel working in Kuala Lumpur, Selangor and Putrajaya. The region is selected because most bank headquarters of Malaysia are located there. The headquarters of banks provide all types of banking services and products compared to the bank branches in other states.

1.10 Significance of the Study

The study shall reveal whether information privacy is being upheld or encroached in the banking industry and whether data subjects as clients of the banks have good or poor perceived knowledge of information privacy. This study measures the level of perceived knowledge amongst bank customers as well as bank personnel in personal data handling. Thus, it contributed to the expansion of knowledge and understanding on the ways to protect personal information. An increase in knowledge could improve conditions and prevent any misuse by third parties. This study also revealed whether the current practices of commercial banks are in compliance with

PDPA requirements during bank transactions. By fulfilling the requirements of PDPA it somewhat relates to the perceived knowledge of bank personnel in personal data handling.

From the aspect of banks, this study disclosed the current practices being used in banking starting from data collection to data processing and until data retention. The study revealed to what extent customer's personal data is protected under bank supervision. The outcome from the study is hoped to create awareness among bank customers as well as bank personnel on data protection and could be used to improve the current practices to the better practices. Both parties may benefit from these developments.

The findings from this study as well established a Personal Data Handling Model for both groups; bank personnel and bank customers. Even though banks can apply different approaches to improve perceived knowledge and practice in its services, it is still imperative to establish a model, verify it and examine the variables involved. As explained before, the attributes for each variable in the study are the seven data protection principles namely Consent, Notice and Choice, Data Disclosure, Data Security, Data Retention, Data Integrity and Data Access as stipulated in the PDPA 2010. Therefore, the model has revealed which attributes strongly contribute to the variables. Besides, the model too benefits the banks and other related agencies that have planned to spread awareness on personal data protection. It functioned as a guideline for them in assessing certain areas that may improve the perceived knowledge and practice. The model may assist any repetitive study in future on examining the effects of perceived knowledge towards practice. By employing the model, it helps banks in strengthening the perceived knowledge and practice of its personnel when dealing with personal data and sensitive information. In that manner, individuals feel safer and more confident in their daily transactions and businesses and the bank personnel become more comprehensive in performing any data processing.

Bank Negara Malaysia (BNM) could use the insight on current practices by the banking industry on personal data protection generally. Thus, the outcomes of this study could assist BNM in improving existing regulations. Other than that, policy-

makers, decision-makers, researchers and the public could use the information gathered from this study for the betterment of personal data protection. Thereby, hopefully, Malaysia is placed among other countries such as EU countries which actively protect the personal information from being misused.

1.11 Operational Definition

To be precise, the description and meaning of several frequently used key terms in this study are explains below.

1.11.1 Privacy

Abdul Rahman Saad (2005) defines privacy as an identification of the virtues or norms that a society is built upon. Caloyannides (2004) describes privacy as a right for any individual in controlling the collection and use of his personal information. While Westin (2003) explained privacy as the limit in which an individual needs and desires others to know about him and his information. Ghosh (2001) describes privacy as aspects of individuals, businesses and organization which shall remain confidential so they could remain anonymous and away from public attention. Those aspects comprise of every aspect of their life including data, personal information, properties, behavioral characteristics and habits (Patent,1983).

Privacy is a state of condition that allows the individual to have certain "sphere" of solitude and feels safe against unwanted prey and for this study, privacy is the right and privilege of keeping details of personal life including personal information to remain inaccessible by the outside world. As to how much the secrecy is kept and when or with whom to share it with.

1.11.2 Personal Data

Section 4 of the Personal Data Protection Act 2010 (hereinafter referred to as PDPA) defines personal data as any information used in commercial transactions such as purchasing products, booking of flight tickets or hotel reservations and use of credit cards. The information relates directly or indirectly to a private individual, referred to as data subject (s 4). Under section 4, personal data as well includes sensitive data such as physical or mental health, political opinions, religious beliefs, and commission of any offence by data subject.

In the context of this study, personal data refers to the definition in PDPA as stipulated under section 4. An individual's name, address, identification card number, passport number, bank account and closed-circuit television (CCTV) image are considered as personal data.

1.11.3 Bank Practices

Practice is an application or procedure in doing something. The act of getting works done and knowing how to do it also defines a meaning of practice (McIver *et al.*, 2016). Practice in organization normally tasks that were carried out by individual or in a group (Brown *et al.*, 2001; Orlikowski, 2002). As explained in the *Dictionary of Law* (1998), bank practice refers to the various ways a bank can help customers, such as doing money transfer, paying standing orders and selling foreign currencies.

For the purpose of this study, bank practice is discussed on the personal data handling in the bank from the moment of collecting customer's personal data to the use of the data as well as the dissemination and disclosure of that particular data. Garner, (2004) defines personal data handling as an action of coordinating operations regarding personal data.

1.11.4 Level of Knowledge

Knowledge is defined as a justified true belief and it is understood as information validated by experience that has entered the human belief systems as rules for guiding actions (Song *et al.*, 2005). It as well described as an awareness gained by experiences (Hume, 1957; Gibson, 1968; Yolton, 1970). Knowledge could also be viewed as a set of organized statements or facts of ideas, presenting a reasoned judgment or an experiment result, which is transmitted to others through some communication medium in some systematic form (Castells, 2010). Thus, level of knowledge is the position of knowledge in a scale of values. This study identifies to what extent the respondents who are bank customers and bank personnel are able to comprehend matters in relation with personal data handling. The study however uses the terms 'Perceived Knowledge' to represent the variable of knowledge as our perception depends on the interpretation of the data we received through our senses (eyes, ears, skin, etc.) and the knowledge we possess (Hunt, 2003).

1.11.5 Consent

According to Le Métayer & Monteleone (2009), the definition of consent could be divided into two, one is an agreement between two entities and the other is used in the sense of a single manifestation of will. While the EU Directive defines consent as any freely given, specific and informed indication by a subject as a symbol of agreement for his personal data to be processed (Suri *et al.*, 2001). Consent could also be in writing or implied. Data subject has to be clearly informed in advance about the proposed processing of his personal data (Abu Bakar Munir *et al.*, 2014).

In this study, the definition of consent is as stipulated under Section 4 of PDPA 2010 which stated data users shall not be allowed to process any personal data unless the data subject has consented the processing of personal data. Although the Act does not specify whether the consent should be in express or implied consent (Ong, 2012), but the bottom line is the data subject has to be informed and understands the process.

1.11.6 Social Learning Theory

This is a model developed by Albert Bandura in 1970 which suggesting individual would learn new behaviour through reinforcement, punishment and observation through social environment. The model emphasis on the learning phenomena resulting from direct experiences through observation of other people's behaviour and its consequences for them. The study thereby employs the main concept of the theory in assessing the relationship between variables of study.

1.11.7 Data User

As stated under the Personal Data Protection Code of Practice for Banking and Financial Sector (2015), a data user is a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data. For the purpose of this study, data user is the bank itself as explained by Abu Bakar Munir (1999) that data user could be a person or an organization that holds and control the data.

1.11.8 Data Subject

An individual who is the subject or the owner of the personal data or a living individual referred in the data is recognized as data subject (Abu Bakar Munir, 1999). In the context of this study, a bank customer is a data subject.

1.12 Summary of the Chapter

This chapter provides the background of study including the issues arising and related provision of laws in personal data protection. It discusses the privacy threats faced by every individual, business and government agency while handling the

personal data for day to day activities. This chapter also describes the importance of protecting personal information in today's digital age as now every single data and information is being stored in computer software and it is easy to access. In the context of Malaysia, the Personal Data Protection Act is a new legislation and it becomes a new phase for businesses to adopt and comply with the Act including the banking sector. In addition, in this chapter, the 'Social Learning Theory' has been reviewed and proposed as the conceptual framework for this study. Apart from the framework, provisions of the Personal Data Protection Act 2010 are also applied as the scope of this study is on personal data protection by Malaysian banks.

The first chapter introduces the research topic and presents the justifications of the research at large. Chapter two serves as the backbone of this thesis and discusses past researches on personal data at international and domestic levels, findings from other scholars on the same area of discussion as well as the related policy and acts to the area of personal data protection. The insights from chapter two were used in building up the focus area, constructs and items needed for this research.

REFERENCES

Abdul Ghani Azmi, I. M., Zulhuda, S. and Wigati Jarot, S. P. (2012) 'Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks', *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, pp. 306–311.

Abdul Rahman Saad (2005) *Personal Data & Privacy Protection*. LexisNexis.

Abdullah, S. (2013) 'The Bank's Duty of Confidentiality, Disclosure Versus Credit Reference Agencies; Further Steps for Consumer Protection: "Approval Model".', *European Journal of Current Legal Issues*, 19(4).

Abu Bakar Munir (1999) *Cyber Law Policies and Challenges*. 1st edn. Butterworths Asia.

Abu Bakar Munir and Siti Hajar Mohd. Yasin (2002) *Privacy and data protection : a comparative analysis with special reference to the Malaysian proposed law*. Sweet & Maxwell Asia.

Abu Bakar Munir, Siti Hajar Mohd Yasin and Md. Ershadul Karim (2014) *Data Protection Law in Asia*. 1st edn. Hong Kong: Sweet & Maxwell Asia.

Acharya, R. N., Kagan, A. and Lingam, S. R. (2008) 'Online Banking Applications and Community Bank Performance', *International Journal of Bank Marketing*, 26(6), pp. 418–439.

Adams, K. A. and Lawrence, E. K. (2015) *Research Methods, Statistics and Applications*. SAGE Publication, Inc.

Adeleke, I. T., Adekanye, A. O., Adefemi, S. A., Onawola, K. A., Okuku, A. G., Sheshi, E. U., James-Adeniran, J. A., Francis, M., Elegbe, T. R., Ayeni, A. M. and Tume, A. A. (2011) 'Knowledge, attitudes and practice of confidentiality of patients' health records among health care professionals at Federal Medical Centre, Bida', *Nigerian Journal of Medicine: Journal of the National Association of Resident Doctors of Nigeria*, 20(2), pp. 228–235.

Adibah A.Latif (2013) *Moral Evaluation Instrument Among Malaysian IPTA Students*. Universiti Teknologi Malaysia.

Ali Al-Ajam, A. S. (2013) *Factors Affecting Customer Usage Intention of Internet Banking Services in Yemen*. Universiti Teknologi Malaysia (UTM).

Antikainen, A. (2014) *Risk-Based Approach as a Solution to Secondary Use of Personal Data*. University of Helsinki.

Arni Abdul Gani, Norhayati Mohd Mat Yusoff, Norhidayah Abdullah, Noriza Ishak and Rosmaliza Mohammad (2018) 'Assessing the Knowledge , Attitude and Practice among Food Handler towards Assessing the Knowledge , Attitude and Practice among Food Handler towards Effective Waste Management System in Bandar PuncakAlam , Selangor , Malaysia', *International Journal of Latest Research in Humanities and Social Science (IJLRHSS)*, 1(9).

Azrilah Abdul Aziz, Mohd Saidfudin Masodi and Azami Zaharim (2013) *Asas Model Pengukuran Rasch: Pembetukan Skala & Struktur Pengukuran (Pertama)*. Bangi, Selangor: Penerbit UKM.

Baker, M. J. and Susan, H. (2016) *The Marketing Book*. Routledge.

Baker, T. L. (1994) *Doing Social research*. 3rd edn. California: McGraw-Hill.

Ball, K., Daniel, E. M. and Stride, C. (2012) 'Dimensions of employee privacy: an empirical study', *Information Technology & People*, 25(4), pp. 376–394.

Ball, S. J. (2015) 'What is policy? 21 years later: reflections on the possibilities of policy research', *Discourse*, 36(3), pp. 306–313.

Bandura, A. (1971) *Social Learning Theory*, *Social Learning Theory*. General Learning Press.

Bandura, A. (1977) 'Self-efficacy: Toward A Unifying Theory of Behavioral Change', *Psychological Review*, pp. 191–215.

Bandura, A. (1994) 'Self-Efficacy', *Encyclopedia of human behavior*, 4(1994), pp. 71–81.

Banking Tech (2015) *Data Integrity and Post-Crisis Regulatory Reform*, *Banking Technology*.

Barclay, C. a. (2013) 'A comparison of proposed legislative data privacy protections in the United States', *Computer Law and Security Review*. Elsevier Ltd, 29(4), pp. 359–367.

Barclay, L. (1982) 'Social Learning Theory: A Framework for Discrimination Research.', *Academy of Management Review*, 7(4), pp. 587–594.

Bartlett, J. E., Kotrlik, J. W. K. J. W. and Higgins, C. (2001) 'Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research', *Information technology, learning, and performance journal*, 19(1), p. 43.

Bentler, P. M. (1990) 'Comparative Fit Indexes in Structural Models', *Quantitative Methods in Psychology*, 22(4), pp. 541–562.

Berdie, D. R. (1973) 'Questionnaire length and response rate.', *Journal of Applied Psychology*, 58(2), pp. 278–280.

Bernama (2017) 'IGP: CIMB data loss due to negligence, not sabotage', *New Straits Times*, 17 November.

Bhattacherjee, A. (2012) *Social Science Research: Principles, Methods, and Practices*. University of South Florida, USA.

Biggam, J. (2001) 'Defining knowledge: An epistemological foundation for knowledge management', in *Proceedings of the Hawaii International Conference on System Sciences*, p. 198.

Blaxter, L., Hughes, C. and Tight, M. (2006) *How to research*. 3rd edn. Open University Press.

Bobby, S. and Sandblom, C. L. (1989) *Quantitative Analysis for Business Decision*. 1st edn. McGraw-Hill.

Bond, T. G. and Fox, C. M. (2007) *Applying The Rasch Model: Fundamental Measurement in the Human Sciences*. 2nd edn. London: Lawrence Erlbaum Associates.

Boon, O. K. (2013) *Total Quality Management and Knowledge Management in Malaysian Manufacturing and Service Firms : A Structural Equation Modeling Approach*. University of Malaya.

Bose, R. (2004) 'Knowledge management metrics', *Industrial Management & Data Systems*, 104(6), pp. 457–468.

Brown, J. S., Duguid, P., Seely, J. and Paul, B. (2001) 'Knowledge and Organization', *Organization Science*, 12(October 2015), pp. 198–213.

Browne, M. W. and Cudeck, R. (1992) 'Alternative Ways of Assessing Model Fit', *Sociological Methods & Resarch*, 21(2), pp. 230–258.

Caloyannides, M. A. (2004) *Privacy Protection and Computer Forensics*. 2nd edn. Artech House Inc.

Capistrano, E. P. S. and Chen, J. V. (2015) 'Information privacy policies: The effects of policy characteristics and online experience', *Computer Standards and Interfaces*. Elsevier B.V., 42, pp. 24–31.

Castañeda, J. A., Montoso, F. J. and Luque, T. (2007) 'The dimensionality of customer privacy concern on the internet', *Online Information Review*, 31(4),

pp. 420–439.

Castells, M. (2010) *The Information Age: Economy, Society and Culture*. 1st edn. Wiley-Blackwell.

Caudill, E. M. and Murphy, P. E. (2000) 'Consumer Online Privacy: Legal and Ethical Issues', *Journal of Public Policy & Marketing*, 19(1), pp. 7–19.

Cellary, W. and Rykowski, J. (2015) 'Challenges of Smart Industries - Privacy and payment in Visible versus Unseen Internet', *Government Information Quarterly*. Elsevier Inc., pp. 1–7.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S. and Raghav Rao, H. (2016) 'Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults', *Decision Support Systems*. Elsevier B.V., 83, pp. 47–56.

Champion, M. A. (1959) 'Reinforcement and Learning Theory', *Australian Journal of Psychology*, 11(2), p. 214.

Cheah, D. (2016) *Up Close and Personal: The Malaysian Personal Data Protection Act*, *HG.org Legal Resources*. Kuala Lumpur.

Chen, A., Lu, Y. and Wang, B. (2017) 'Customers ' purchase decision-making process in social commerce : A social learning perspective', *International Journal of Information Management*. Elsevier, 37(6), pp. 627–638.

Chew, K. Y. (2015) *Data Protection Compliance in Malaysia Set to Cause Headanches to Businesses*, *b:INFORM Legal Insights on Data & Technology Trends*.

Christl, W. (2017) *How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information*. Vienna.

Chua, H. N., Herbland, A., Wong, S. F. and Chang, Y. (2017) 'Compliance to personal data protection principles: A study of how organizations frame privacy policy notices', *Telematics and Informatics*, 34(4), pp. 157–170.

Chua, H. N., Wong, S. F., Chang, Y. and Libaque-Saenz, C. F. (2017) 'Unveiling the coverage patterns of newspapers on the personal data protection act', *Government Information Quarterly*. Elsevier Inc., 34(2), pp. 296–306.

Cieh, E. L. Y. (2012) *Personal Data Protection Act 2010: An Overview Analysis*. Heidelberg: Springer.

Clifford, D. and Van Der Sype, Y. S. (2015) 'Online dispute resolution: Settling data

protection disputes in a digital world of customers', *Computer Law & Security Review*. Elsevier Ltd, 32(2), pp. 272–285.

Colebatch, H. K. (2009) *Policy*. 3rd edn. Berkshire: McGraw-Hill.

Collis, J. and Hussey, R. (2013) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*. Palgrave Macmillan.

Creswell, J. W. (2009) *Research design: Qualitative, quantitative, and mixed methods approaches*. 3rd edn. California: SAGE Publication, Inc.

Creswell, J. W. and Clark, V. L. P. (2011) *Designing and Conducting Mixed Methods Research*. 2nd edn. SAGE Publication, Inc.

Culnan, M. J. (1995) 'Consumer awareness of name removal procedures: Implications for direct marketing', *Journal of Direct Marketing*. Elsevier, 9(2), pp. 10–19.

Czechowski, K., Sylvestre, J. and Moreau, K. (2019) 'Secure data handling: An essential competence for evaluators', *Canadian Journal of Program Evaluation*, 34(1), pp. 139–151.

Daher, A. M., Ismail, N. M. and Agarwal, R. (2013) 'Knowledge, practices and attitudes towards adverse drug reaction reporting by private practitioners from klang valley in Malaysia', *Malaysian Journal of Medical Sciences*, 20(2), pp. 53–62.

Dalla Pozza, V., Limited Anna Di Pietro, M., Limited Sophie Morel, M., Limited Emma Psaila, M. and Limited, M. (2016) *Cyberbullying Among Young People Study*.

Daniel, J. (2012) *Sampling Essentials Practical Guidelines for Making Sampling Choices*. 1st edn. SAGE Publication, Inc.

Dawood, O. T., Hassali, M. A. and Saleem, F. (2017) 'Factors affecting knowledge and practice of medicine use among the general public in the State of Penang, Malaysia', *Journal of Pharmaceutical Health Services Research*, 8(1), pp. 51–57.

Decker, P. J. (1986) 'Social Learning Theory and Leadership', *Journal of Management Development*, 5(3), pp. 46–58.

Delak, B., Majewski Marek, G. and Damji, N. (2014) 'How To Identify Knowledge and Evaluate Knowledge Management in Organization', *Online journal of Applied Knowledge Management*, 2(2), pp. 162–171.
Dictionary of Statistics & Methodology A Nontechnical Guide for the Social Sciences. 4th edn (2011). SAGE Publication, Inc.

Donald, W. (1997) *Quantitative Methods for Business*. 2nd edn. Addison Wesley Longman Publishers Ltd.

Donalson, M. and Lohr, K. (1994) *Health Data in the Information Age: Use, Disclosure, and Privacy*. Washington DC: National Academies Press (US).

Downer, K. and Bhattacharya, M. (2015) 'BYOD security: A new business challenge', *Proceedings - 2015 IEEE International Conference on Smart City, SmartCity 2015, Held Jointly with 8th IEEE International Conference on Social Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communic*, pp. 1128–1133.

Duncan, P. W., Bode, R. K., Lai, S. M. and Perera, S. (2003) 'Rasch analysis of a new stroke-specific outcome scale: The stroke impact scale', *Archives of Physical Medicine and Rehabilitation*, 84(7), pp. 950–963.

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

Edinyang, S. D. (2016) 'The Signifiance of Social Learning Theories in the Teaching of Social Studies Education', *International Journal of Sociology and Anthropology Research*, 2(1), pp. 40–45.

Eileen Ng (2018) 'Malaysia's data breaches stem from weak security, say experts', *Today Online*, 11 February.

Falmagne, J. C. J.-C., Thiéry, N., Cosyn, E., Doignon, J.-P. and Thiery, N. (2006) 'The Assessment of Knowledge, in Theory and in Practice', *Formal Concept Analysis*, 3874(949), pp. 61–79.

Farah, S. (2014) 'Personal Data Protection Act 2010: Taking the First Steps Towards Compliance', *Synergizing Knowledge on Management and Muamalah*, (May), pp. 978–983.

Fink, A. (1995a) *How to Design Survey*. California: SAGE Publication, Inc.

Fink, A. (1995b) *How to Sample in Surveys*. California: SAGE Publication, Inc.

Fisher, W. P. (2007) 'Rating Scale Instrument Quality Criteria', *Rasch Measurement Transactions*, 21(1), p. 1095.

Flick, U. (2009) *An Introduction to Qualitative Research*. 4th edn. SAGE Publication Ltd.

Fotiadis, A. K. and Stylos, N. (2017) 'The effects of online social networking on

retail consumer dynamics in the attractions industry: The case of "E-da" theme park, Taiwan', *Technological Forecasting and Social Change*. Elsevier Inc., 124, pp. 283–294.

Garland, R. (1991) 'The Mid-point on a Rating Scale: Is it Desirable?', *Marketing Bulletin*, 2, pp. 66–70.

Garner, B. A. (ed.) (2004) *Black's Law Dictionary*. 8th edn. West Group.

Garrison, C. P. and Ncube, M. (2011) 'A Longitudinal Analysis of Data Breaches', *Information Management & Computer Security*, 19(4), pp. 216–230.

George, D. and Mallery, P. (2003) *SPSS for Windows step by step: A simple guide and reference*. 4th edn. Boston: Ally & Bacon.

Ghosh, A. K. (2001) *Security and Privacy for E-Business*. Canada: Wiley Computer Publishing.

Gibson, J. (1968) *Locke's Theory of Knowledge and its Historical Relations*. Cambridge.

Graham, F. S., Gooden, S. T. and Martin, K. J. (2016) 'Navigating the Transparency-Privacy Paradox in Public Sector Data Sharing', *The American Review of Public Administration*, 46(5), pp. 569–591.

Graham, I. D., Logan, J., Harrison, M. B., Straus, S. E., Tetroe, J., Caswell, W. and Robinson, N. (2006) 'Lost in knowledge translation: time for a map?', *The Journal of continuing education in the health professions*, 26(1), pp. 13–24.

Griethuijsen, R. A. L. F. Van, Eijck, M. W. Van, Haste, H., Brok, P. J. Den, Skinner, N. C., Mansour, N., Gencer, A. S. and Boujaoude, S. (2014) 'Global Patterns in Students ' Views of Science and Interest in Science', *Research in Science Education*, 4(45), pp. 581–603.

Guptil, J. (2005) 'Knowledge Management in Health Care', *Journal of Health Care Finance*, 31(3), pp. 10–14.

Hair, J. F., Black, W. C., Babin, B. J. and Anderson, R. E. (2010) *Multivariate Data Analysis*. 7th edn, *Vectors*. 7th edn. Pearson Education.

Hair, J. F., Black, W. C., Babin, B. J. and Anderson, R. E. (2014) *Multivariate Data Analysis (MVDA)*. 7th edn, *Pharmaceutical Quality by Design: A Practical Approach*. 7th edn. Pearson New International Edition.

Hamin, Z., Othman, M. B. and Mohamad, A. M. (2012) 'ICT Adoption by the Malaysian High Courts: Exploring the Security Risks Involved', *ICIMTR 2012 - 2012 International Conference on Innovation, Management and*

Technology Research, pp. 285–289.

Hansen, R. E. (2000) 'The Role of Experience in Learning: Giving Meaning and Authenticity to the Learning Process in Schools', *Journal of Technology Education*, 11(2), pp. 23–32.

Harris, K. D. and General, A. (2016) *California Data Breach Report*. California.

Hartley, J. (2014) 'Some Thoughts on Likert-type Scales', *International Journal of Clinical and Health Psychology*. Elsevier, 14(1), pp. 83–86.

Hashim, E. M. A. B. A., Talib, N. A. and Alamen, K. M. (2014) 'Knowledge Management Practice in Malaysian Construction Companies', *Middle-East Journal of Scientific Research*, 21(11), pp. 1952–1957.

Hayes, R. F. (1978) *Learning by Example*. Boston: Springer.

Hempel, G. H. and Simonson, D. G. (1999) *Bank Management Text and Cases*. 5th edn. John Wiley & Sons, Inc.

Henry, G. T. (1990) *Practical Sampling*. Edited by G. T. Henry. Thousand Oaks: SAGE Publication, Inc.

Hinton, P. R., McMurray, I. and Brownlow, C. (2004) *SPSS Explained*. Routledge.

Ho, S. and Mallick, S. (2010) 'The impact of information technology on the banking industry', *Journal of the Operational Research Society*, 61, pp. 211–221.

Ho, V., Dehghantanha, A. and Shanmugam, K. (2010) 'A Guideline to Enforce Data Protection and Privacy Digital Laws in Malaysia', *2nd International Conference on Computer Research and Development, ICCRD 2010*, pp. 3–6.

Horsburgh, J., Ippolito, K. (2018) 'A skill to be worked at: using social learning theory to explore the process of learning from role models in clinical settings', *BMC Med Educ 18*, 156.

Huberts, L. W. J. C. (2018) 'Integrity: What it is and Why it is Important', *Public Integrity*, 9922.

Hume, D. (1957) *Enquiries concerning the Human Understanding and the Principles of Morals*. Oxford.

Hunt, D. P. (2003) 'The concept of knowledge and how to measure it', *Journal of Intellectual Capital*, 4(1), pp. 100–113.

Hunter, P. (2016) 'The Big Health Data Sale', *EMBO reports*, 17(8), pp. 1103–1105.

Hurley, A. E., Scandura, T. A., Schriesheim, C. A., Brannick, M. T., Seers, A., Vandenberg, R. J. and Williams, L. J. (1997) 'Exploratory and confirmatory factor analysis: Guidelines, issues, and alternatives', *Journal of Organizational*

Behavior, 18(6), pp. 667–683.

Ibrahim, R., Boerhannoeddin, A. and Bakare, K. K. (2017) 'The effect of soft skills and training methodology on employee performance', *European Journal of Training and Development*, 41(4), pp. 388–406.

ICO UK (2016) *Direct Marketing*. United Kingdom.

Jackson, L. E. and Lim, M. W. (2011) 'Knowledge and practice of confidential data handling in the Welsh Deanery: a brief report.', *Journal of medical ethics*, 37(1), pp. 58–60.

Jackson, S. L. (2012) *Research Methods and Statistics A Critical Thinking Approach*. 4th edn. Wadsworth Cengage Learning.

Jai, T. M. and King, N. J. (2016) 'Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers?', *Journal of Retailing and Consumer Services*. Elsevier, 28, pp. 296–303.

Jeff, H. and Sandra, J. (1996) 'Information privacy : Measuring individuals ' concerns about organizational practices', *MIS Quarterly: Management Information Systems*, 20(2), pp. 167–215.

Juffer, F., Bakermans-kranenburg, M. J. and Ijzendoorn, M. H. Van (2017) 'Pairing attachment theory and social learning theory in video-feedback intervention to promote positive parenting', *Current Opinion in Psychology*. Elsevier Ltd, 15, pp. 189–194.

Kamal Halili Hassan (2012) 'Personal data protection in employment: New legal challenges for Malaysia', *Computer Law & Security Review*. Elsevier Ltd, 28(6), pp. 696–703.

Kendra, C. (2019) *How Observational Learning Affects Behavior*, *VeryWellMind*.

Keshavarzi, B. (2011) 'Social and The Impact of Information Technology in Banking System (A Case Study in Bank Keshavarzi Iran)', *Procedia - Social and Behavioral Sciences*, 30, pp. 13–16.

Khairul, M., Ahmad, A., Rosalim, R. V., Yu, L. and Fun, T. S. (2010) 'Security Issues on Banking Systems', *International Journal of Computer Science and Information Technologies*, 1(4), pp. 268–272.

Khanal, L. and Raj Poudel, S. (2017) 'Saudi Journal of Business and Management Studies Knowledge Management, Employee Satisfaction and Performance: Empirical Evidence from Nepal', *Saudi Journal of Business and Management*

Studies, 2(2), pp. 82–91.

Kim, H., Ku, B., Kim, J. Y., Park, Y. J. and Park, Y. B. (2016) 'Confirmatory and exploratory factor analysis for validating the phlegm pattern questionnaire for healthy subjects', *Evidence-based Complementary and Alternative Medicine*.

King, N. J. and Raja, V. T. (2012) 'Protecting the privacy and security of sensitive customer data in the cloud', *Computer Law and Security Review*. Elsevier Ltd, 28(3), pp. 308–319.

Kingsford, K. M., Fengli, Z. and Komlan, G. (2017) 'Patient knowledge and data privacy in healthcare records system', *2017 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA)*, pp. 154–159.

Kline, R. (2013) 'Exploratory and confirmatory factor analysis', *Applied Quantitative Analysis in Education and the Social Sciences*, pp. 171–207.

Kong, G. and Xiao, Z. (2015) 'Protecting privacy in a clinical data warehouse', *Health Informatics Journal*, 21(2), pp. 93–106.

Kothari, C. R. (2004) *Research Methodology: Methods & Techniques*. 2nd edn. New Age International (P) Limited.

Kshetri, N. (2013) 'Privacy and security issues in cloud computing: The role of institutions and institutional evolution', *Telecommunications Policy*. Elsevier, 37(4–5), pp. 372–386.

Kulas, J. T. and Stachowski, A. A. (2013) 'Respondent Rationale for Neither Agreeing Nor Disagreeing: Person and Item Contributors to Middle Category Endorsement Intent on Likert Personality Indicators', *Journal of Research in Personality*. Elsevier Inc., 47(4), pp. 254–262.

Kumar, R. (2011) *Research Methodology_A Step by Step Guide for Beginners*. 3rd edn. SAGE Publication Ltd.

Lackey, N. R. and Wingate, A. L. (1998) *Advanced Design in Nursing Research*. 2nd edn. California: SAGE Publication, Inc.

Lai, F., Li, D. and Hsieh, C. T. (2012) 'Fighting identity theft: The coping perspective', *Decision Support Systems*. Elsevier B.V., 52(2), pp. 353–363.

Lenderking, W. C. W., Jin, Y., Wyrwich, K. W., Gelhorn, H. and Revicki, D. A. (2014) 'Is Rasch model analysis applicable in small sample size pilot studies for assessing item characteristics ? An example using PROMIS pain behavior item bank data', *Quality of LIfe Research*, 23(2).

Leon, A., Davis, L. and Kraemer, H. (2011) 'Role and interpretaion of pilot studies in clinical research', *J Psychiatr Res*, 45(5), pp. 626–629.

Leshem, S. and Trafford, V. (2007) 'Overlooking the conceptual framework', *Innovations in Education and Teaching International*, 44(1), pp. 93–105.

Li, Y., Stewart, W., Zhu, J., Ni, A. and Rohm Jr., C. E. T. (2012) 'Online Privacy Policy of the Thirty Dow Jones Corporations: Compliance with FTC Fair Information Practice Principles and Readability Assessment.', *Communications of the IIMA*, 12(3), pp. 65–89.

Linacre, J. M. (1994) 'Sample Size and Item Calibration Stability', *Rasch Measurement Transactions*, 7(4), p. 328.

Linacre, J. M. (2002) 'What do infit and outfit, mean-square and standardized mean', *Rasch Measurement Transactions*, 16(2), p. 878.

Linacre, J. M. (2019) *Winsteps Rasch Measurement Computer Program User's Guide*, *Winsteps*.

Ling, G. M., Fern, Y. S., Boon, L. K. and Huat, T. S. (2016) 'Understanding Customer Satisfaction of Internet Banking: A Case Study In Malacca', *Procedia Economics and Finance*. Elsevier B.V., 37(16), pp. 80–85.

Linn, R. L. (2000) *Measurement and Assessment In Teaching*. 8th edn. New Jersey: Prentice Hall.

Litwin, M. S. (1995) *How to Measure Survey Reliability and Validity*. California: SAGE Publication, Inc.

Logemann, J. (2012) *The Development of Consumer Credit in Global Perspective*. Palgrave Macmillan.

Loh, J. and Bedi, R. S. (2009) 'Data Sales Racket', *The Star*, 3 May.

Maccallum, R. C., Browne, M. W. and Sugawara, H. M. (1996) 'Power Analysis and Determination of Sample Size for Covariance Structure Modeling', *Psychological Methods*, I(2), pp. 130–149.

Majid, M. (2013) 'Cybercrime: Malaysia', *Royal Malaysia Police*. Malaysian Communication and Multimedia Commission, p. 19.

Mangiaracina, R., Perego, A., Perotti, S. and Tumino, A. (2016) 'Assessing the environmental impact of logistics in online and offline B2C purchasing processes in the apparel industry', *International Journal of Logistics Systems and Management*, 23(1), p. 98.

Mantelero, A. (2014) 'The future of consumer data protection in the E . U . Re-

thinking the " notice and consent " paradigm in the new era of predictive analytics', *Computer Law & Security Review*. Elsevier Ltd, 30(6), pp. 643–660.

Marcela Jr., A. J. and Menendex, D. (2008) *Cyber Forensics*. 2nd edn. New York: Auetbach Publications.

Matoskova, J. (2016) 'Measuring Knowledge', *Journal of Competitiveness*, 8(4), pp. 5–29.

Matzner, T. (2014) 'Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data"', *Journal of Information, Communication and Ethics in Society*, 12(2), pp. 93–106.

Mazzini Muda, Rohani Mohd and Salwana Hassan (2016) 'Online Purchase Behavior of Generation Y in Malaysia', *Procedia Economics and Finance*. Elsevier B.V., 37(July), pp. 292–298.

McDonald, R. P. and Ho, M. H. R. (2002) 'Principles and practice in reporting structural equation analyses', *Psychological Methods*, 7(1), pp. 64–82.

McIver, D., Fitzsimmons, S. and Flanagan, D. (2016) 'Instructional Design as Knowledge Management: A Knowledge-in-Practice Approach to Choosing Instructional Methods', *Journal of Management Education*, 40(1), pp. 47–75.

Le Métayer, D. and Monteleone, S. (2009) 'Automated consent through privacy agents: Legal requirements and technical architecture', *Computer Law and Security Review*, 25, pp. 136–144.

Miles, M. B. and Huberman, A. M. (1994) *Qualitative data analysis: An expanded sourcebook*. 2nd edn, *SAGE Publications*. 2nd edn.

Milne, G. R. and Culnan, M. J. (2004) 'Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't read) Online Privacy Notices', *Journal of Interactive Marketing*. Elsevier, 18(3), pp. 15–29.

Mohd Shoki Md Ariff, Yun, L. O., Norhayati Zakuan and Ismail, K. (2013) 'The Impacts of Service Quality and Customer Satisfaction on Customer Loyalty in Internet Banking', *Procedia - Social and Behavioral Sciences*. Elsevier B.V., 81, pp. 469–473.

Mukesh, K., Salim, A. T. and Ramayah, T. (2013) *Business Research Methods*. 1st edn. Oxford Fajar Sdn Bhd.

Munir, A. B., Mohd Yasin, S. H. and Muhammad-Sukki, F. (2015) 'Big Data: Big Challenges to Privacy and Data Protection', *XIII International Conference on*

Big Data Computing (ICBDC 2015), 9(1), pp. 1–9.

Murata, K. and Orito, Y. (2008) 'Rethinking the concept of the right to information privacy: a Japanese perspective', *Journal of Information, Communication and Ethics in Society*, 6(3), pp. 233–245.

Nizam Yatim and Johari Syawal (2007) 'Jawatankuasa Siasat Sistem PTG Diceroboh', *Utusan Malaysia Online*, 15 May.

Noe, R. A., Hollenback, J. R., Gerhart, B. and Wright, P. M. (2010) *Human Resource Management*. McGraw-Hill.

Nor Ashikin, Nurul Ain and Zamri (2016) 'A Study on Collection of Personal Data by Banking Industry in Malaysia', *Advanced Business in Research and Management Studies*, 2(1), pp. 39–49.

Noriswadi Ismail (2013) *Understanding Personal Data Protection*. 1st edn. LexisNexis.

Noriswadi Ismail and Cieh, E. L. Y. (2013) *Beyond Data Protection*. Berlin Heidelberg: Springer.

NST Online (2017) 'CIMB reveals several magnetic tapes containing back-up data "lost in transit", heightens security', *New Straits Times*, 13 November.

Olivero, N. and Lunt, P. (2004) '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, pp. 243–262.

Ong, R. (2012) 'Data protection in Malaysia and Hong Kong: One step forward, two steps back?', *Computer Law & Security Review*, 28(4), pp. 429–437.

Orlikowski, W. J. (2002) 'Knowing in Practice: Enacting a Collective Capability in Distributed Organizing', *Organization Science*, 13(3), pp. 249–273.

Othman Talib (2014) *Tulis Tesis Cepat*. 3rd edn. Bangi: MPWS Rich Resources.

P. Divakaran (2016) 'Man Claims He Sold Over A Million Names for Citizens Declaration', *The Star Online*, 26 May.

Parahoo, K. (2014) *Nursing Research: Principles, Process and Issues*. 3rd edn. Palgrave Macmillan.

Peterson, K., Novak, D., Stradtman, L., Wilson, D. and Couzens, L. (2015) 'Hospital respiratory protection practices in 6 U.S. states: A public health evaluation study', *American Journal of Infection Control*. Elsevier Inc, 43(1), pp. 63–71.

Pinsent Masons (2004) *Data retention is the main compliance headache for banks*.

Polit, D. F. and Beck, C. T. (2004) *Nursing research:Principles and methods*. 7th

edn. Philadephlia: Lippincott Williams & Wilkins.

PrivacySense.net (2016) *Different Types of Consent*.

Quinn, M. J. (2015) *Ethics for the Information Age*. 6th edn. Pearson Education Limited.

Rahim, N. H. A., Hamid, S. and Kiah, M. L. M. (2019) 'Enhancement of Cybersecurity Awareness Program on Personal Data', *Malaysian Journal of Computer Science*, 32(3), pp. 221–245.

Rais Yatim (2012) *Protecting your personal data*, *The Star Online*.

Randall E. Schumacker and Lomax, R. G. (2004) *A Beginner's Guide to Structural Equation Modeling*. 2nd edn. Lawrence Erlbaum Associates,.

Reidenberg, J. R. (2000) 'Resolving Conflicting International Data Privacy Rules in Cyberspace', *Stanford Law Review*, 52(5), pp. 1315–1371.

Remar, N. (2020) '"Be on your guard"', *The Star Online*, 15 June.

Reuters (2019) 'Malindo data leak: Breach caused by ex-staff', *The New Straits Time Online*, 24 September.

Richard A. Swanson and Holton, E. F. (2005) *Research in Organizations: Foundations and Methods in Inquiry*. Berrett-Koehler Publishers.

Robb, C. A. and Woodyard, A. S. (2011) 'Financial Knowledge and Best Practice Behavior', *Journal of Financial Counseling and Planning*, 22(1), pp. 60–70.

Rocereto, J. F., Puzakova, M., Anderson, R. E. and Kwak, H. (2011) 'The Role of Response Formats on Extreme Response Style: A Case of Likert-Type vs. Semantic Differential Scales', *Advances in International Marketing*. Emerald Group Publishing Ltd, 22, pp. 53–71.

Rohana Yusoff and Roziah Mohd Janor (2014) 'Generation of an Interval Metric Scale to Measure Attitude', *SAGE Open*, 4(1), pp. 1–16.

Rudner, L. and Wright, B. (1995) 'Diagnosing person misfit', *asch Measurement Transactions*, 9(2), p. 434.

Rusuli, M. and Tasmin, R. (2010) 'Knowledge Sharing Practice In Organization', *International Conference on Ethics and Professionalism*, pp. 797–803.

Sandhu, M. S., Jain, K. K. and Ahmad, I. U. K. bte (2011) 'Knowledge sharing among public sector employees: Evidence from Malaysia', *International Journal of Public Sector Management*, 24(3), pp. 206–226.

Sarabia, M. and Obeso, M. (2012) 'Knowledge Gained from Action and Reaction Learning in Small and Medium-sized Enterprises: Two Sides of the Same

Coin', *Bulletin of the American Society for Information Science and Technology (Online)*, 38(2), pp. 58–63.

Schaefer, D. R. and Dillman, D. A. (1998) 'Development of a Standard E-Mail Methodology: Results of an Experiment', *Public Opinion Quarterly*, 62(3), p. 378.

Schermer, B. W. (2011) 'The limits of privacy in automated profiling and data mining', *Computer Law and Security Review*. Elsevier Ltd, 27(1), pp. 45–52.

Schwartz, P. M. (2004) 'Property , Privacy , and Personal Data', *Harvard Law Review*, 117(7), pp. 2056–2128.

Sekaran, U. (2003) *Research Methods for Business_A Skill Building Approach*. 4th edn. John Wiley & Sons, Inc.

Sen, R. and Borle, S. (2015) 'Estimating the Contextual Risk of Data Breach: An Empirical Approach', *Journal of Management Information Systems*, 32(2), pp. 314–341.

Senthilnathan, S. (2017) 'Relationships and Hypotheses in Social Science Research', *SSRN Electronic Journal*, pp. 1–14.

Shadfar, S. and Malekmohammadi, I. (2013) 'Application of Structural Equation Modeling (SEM) in restructuring state intervention strategies toward paddy production development', *International Journal of Academic Research in Business and Social Sciences*, 3(12).

Shahrudin, H. S. (2017) 'MCMC Probing Report About Personal Data of Malaysians Up For Sale', *New Straits Times*.

Shankar, A. C. (2019) 'Astro suffers data breach exposing customers' MyKad data', *The Edge Markets*.

Shau, T. V. (2017) 'The Confirmatory Factor Analysis (CFA) of Preschool Management Model in Sarawak', *International Journal of Academic Research in Business and Social Sciences*, 7(6), pp. 221–231.

Slocum-Gori, S. L. and Zumbo, B. D. (2011) 'Assessing the Unidimensionality of Psychological Scales: Using Multiple Criteria from Factor Analysis', *Social Indicators Research*, 102(3), pp. 443–461.

Smith (2018) '2 Canadian banks hacked, 90,000 customers' data stolen', *CSO Online*, 29 May.

Smith and D., A. (2004) 'Cybercriminal impacts on online business and consumer confidence', *Online Information Review*, pp. 224–234.

Song, M., Bij, H. van der and Weggeman, M. (2005) 'Determinants of the Level of Knowledge Application: A Knowledge-Based and Information-Processing Perspective', *The Journal of Product Innovation Management*, (22), pp. 430–444.

Sonny, Z. (2012) 'The state of e-government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft', in *1st Taibah University International Conference on Computing and Information Technology (ICCIT 2012)*.

Soursourian, M. and Joyce, M. (2018) 'Data Privacy and Protection', *New Straits Times*, 13 April, p. 17.

Spiekermann, S., Acquisti, A., Böhme, R. and Hui, K. L. (2015) 'The challenges of personal data markets and privacy', *Electronic Markets*, 25(2), pp. 161–167.

Spruce, R. and Bol, L. (2015) 'Teacher beliefs, knowledge, and practice of self-regulated learning', *Metacognition and Learning*, 10(2), pp. 245–277.

Steve, C. (2020) 'For Banks, Safeguarding Consumer Privacy is More Important Than Ever', *Forbes*, April.

Stewart, C. . (2009) *Multidimensional Measure of Professional Learning Communities: The Development and Validation of the Learning Community Culture Indicator (LCCI)*. Brigham Young University.

Stone, E. F., Gueutal, H. G., Gardner, D. G. and McClure, S. (1983) 'A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations.', *Journal of Applied Psychology*, 68(3), pp. 459–468.

Strauss, J. and Rogerson, K. S. (2002) 'Policies for online privacy in the United States and the European Union', *Telematics and Informatics*, 19(2), pp. 173–192.

Suri, R. K., Diwan, P. and Kapoor, S. (2001) *Information Technology Laws*. 1st edn. Kuala Lumpur: International Law Book Services.

Tavakol, M. and Dennick, R. (2011) 'Making sense of Cronbach's alpha', *International journal of medical education*, 2, pp. 53–55.

TechWorld (2018) *The Most Infamous Data Breaches*, *IDG*.

Van Teijlingen, E. and Hundley, V. (1998) 'The importance of pilot studies.', *Nursing standard : official newspaper of the Royal College of Nursing*, pp. 33–36.

Tene, O. and Polonetsky, J. (2013) 'A Theory of Creepy: Technology, Privacy and Shifting Social Norms', *Yale Journal of Law & Technology (…*, 16(1), pp. 1–32.

Thakur, R. and Srivastava, M. (2015) 'A study on the impact of consumer risk perception and innovativeness on online shopping in India', *International Journal of Retail & Distribution Management*, 43(2), pp. 148–166.

The Star Online (2017a) 'No security breach at banks, says ABM', *Star Media Group Berhad*, 22 August.

The Star Online (2017b) 'SayaKenaHack.com Only Provides Information, Does Not Allow Data Download', 18 November.

The Straits Times (2017) 'Malaysia Data Breach Puts Personal Details of 46.2 Million Mobile Subscribers At Stake', 31 October.

Thibaud, A., Riccardo, S. and Gerardo, S. (2016) 'A Privacy-Aware Conceptual Model for Handling Personal Data', in *International Symposium on Leveraging Applications of Formal Methods*, pp. 942–957.

Thorsten, A. (2015) 'How teachers' practice knowledge is used and challenged in a Learning Study using Variation Theory as a tool', *International Journal for Lesson and Learning Studies*, 4(3), pp. 274–287.

Timothy, R. (2002) 'Collecting and using personal data : Consumers ' awareness and concerns', *The Journal of Consumer Marketing*, 19(4/5), pp. 302–318.

Tun Firzara, A. M. and Ng, C. J. (2016) 'Knowledge and practice of prostate cancer screening among general practitioners in Malaysia: A cross-sectional study', *BMJ Open*, 6(9), pp. 4–10.

Ullman, J. B. (2001) *Structural Equation Modeling. In B. G. Tabachnick & L. S. Fidell (Ed.): Using Multivariate Statistics*. 4th edn. MA: Allyn & Bacon.

Umeh, A. and Nkombua, L. (2018) 'A study of the knowledge and practice of lifestyle modification in patients with type 2 diabetes mellitus in Middelburg sub-district of Mpumalanga', *South African Family Practice*. Taylor & Francis, 60(1), pp. 26–30.

Utusan Malaysia (2015) 'Data Intrusion', *Utusan Malaysia*, 5 March.

Vega-Encabo, J. (2016) 'The Concept of Knowledge: What is it for?', *Disputatio*, 8(43), pp. 187–202.

Vogt, W. P., Gardner, D. C., Haeffele, L. M. and Vogt, E. R. (2014) *Selecting The Right Analyses for Your Data: Quantitative, Qualitative, and Mixed Methods*.

New York: Guilford Publications.

Wan Nur Ameera (2015) 'Data and Identity Theft', *Harian Metro*, 28 October.

Warkentin, M., Johnston, A. C. and Shropshire, J. (2011) 'The influence of the informal social learning environment on information privacy policy compliance efficacy and intention', *European Journal of Information Systems*. Nature Publishing Group, 20(3), pp. 267–284.

Warren, S. and Brandeis, L. (1890) '"The Right to Privacy"', *Harvard Law Review*, IV(5).

Warso, Z. (2013) 'There's more to it than data protection – Fundamental rights, privacy and the personal/household exemption in the digital age', *Computer Law & Security Review*, 29(5), pp. 491–500.

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y. and Vasilakos, A. V. (2014) 'Security and privacy for storage and computation in cloud computing', *Information Sciences*. Elsevier Inc., 258, pp. 371–386.

Weiber, R. and Kollmann, T. (1998) 'Competitive advantages in virtual markets –', *European Journal of Marketing*, 32(7/8), pp. 603–15.

Westin, A. F. (2003) 'Social and political dimensions of privacy', *Journal of Social Issues*, 59(2), pp. 431–453.

Westland, J. C. (2015) 'An introduction to structural equation models', *Studies in Systems, Decision and Control*, 22, pp. 1–8.

White, T. B. (2004) 'Consumer Disclosure and Disclosure Avoidance: A Motivational Framework', *Journal of Consumer Psychology*, 14(1–2), pp. 41–51.

Wiig, K. M. (1997) 'Knowledge management: Where did it come from and where will it go?', *Expert Systems with Applications*, 13(1), pp. 1–14.

Wiig, K. M. (2003) 'A knowledge model for situation-handling', *Journal of Knowledge Management*, 7(5), pp. 6–24.

Wirth, C. and Kolain, M. (2018) 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data', in *In Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET)*, p. 6.

Wu, Y. (2014) 'Protecting personal data in E-government: A cross-country study', *Government Information Quarterly*. Elsevier Inc., 31(1), pp. 150–159.

Xia, Y. and Yang, Y. (2019) 'RMSEA, CFI, and TLI in structural equation modeling

with ordered categorical data: The story they tell depends on the estimation methods', *Behavior Research Methods*. Behavior Research Methods, 51(1), pp. 409–428.

Xie, K. L. (2011) *Examining Structural Relationships among Cognitive Destination Image, Destination Personality and Behavioural Intentions; The Case of Beijing*. The Hong Kong Polytechnic University.

Yahui, H. C. and Swaminathan, N. (2017) 'Knowledge, attitudes, and barriers towards evidence-based practice among physiotherapists in Malaysia', *Hong Kong Physiotherapy Journal*. Elsevier Ltd, 37, pp. 10–18.

Yang, C. (2011) 'Analysis on protection of e-commerce consumer network privacy', *Procedia Engineering*, 15, pp. 5519–5524.

Yechiam, E., Haruvy, E. and Erev, I. (2002) 'Reinforcement Learning and the Prevention of Data Catastrophes.', *Journal of Managerial Psychology*, 17(7), pp. 599–611.

Yolton, J. W. (1970) *Locke and the Compass of Human Understanding*. Cambridge.

Ziegeldorf, J. H., Morchon, O. G. and Wehrle, K. (2014) 'Privacy in the Internet of Things : Threats and Challenges', *Security and Communication Networks*, (June 2013), pp. 2728–2742.

LIST OF PUBLICATIONS

Nurul 'Ain Ahmad & Nooraini Othman (2019). Information Privacy Awareness Among Young Generation in Malaysia. *Journal of Science, Technology and Innovation Policy*. Vol 5. No 2.

Nor Ashikin Mohamed Yusof, **Nurul 'Ain Ahmad** & Zamri Mohamed (2016). A Study on Collection of Personal Data by Banking Industry in Malaysia. *Journal of Advanced Research in Business and Management Studies.* Vol 2. No 1. Pages 39-49