Faculty of Information and Communication Technology

MOTIVATIONAL FACTORS IN PRIVACY PROTECTION BEHAVIOUR MODEL FOR SOCIAL NETWORKING SITES

Nur Fadzilah Binti Othman

Doctor of Philosophy

2017

MOTIVATIONAL FACTORS IN PRIVACY PROTECTION BEHAVIOUR MODEL FOR SOCIAL NETWORKING SITES

NUR FADZILAH BINTI OTHMAN

A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I declare that this thesis entitled "Motivational Factors in Privacy Protection Behaviour Model for Social Networking Sites" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ……..

Name : NUR FADZILAH BINTI OTHMAN ……..

Date : ……..……

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Doctor of Philosophy.

Signature	:	……..
Supervisor Name	:	PROF. DR. RABIAH BINTI AHMAD ……..
Date	:	……..……

DEDICATION

To my beloved husband, daughter and parents

for all the supports and du‟as

ABSTRACT

Social Networking Sites (SNSs) have exponentially grown over the past decade. They offer a variety of tools that facilitates communication and information sharing. Despite its conveniences, uncontrolled sharing can lead to the loss and exploitation of privacy. Besides, privacy protection behaviour to protect oneself from SNS risks and threats must be emphasizes because more factor may be contribute to privacy protection behaviour, but issues of related to motivational factors of privacy protection behaviour are as of yet, unexplored. This study focuses on the motivational factors of privacy protection behaviour.This study utilised a quantitative research approach through questionnaires. The population of the study comprised of third-year undergraduates from Malaysian public universities. The minimum sample size was determined to be 355 although 497 quesionnaires were distributed. The respondents were selected based on proportional stratified sampling technique. The research instrument was adapted from previous studies, divided into three sections, and validated by a panel of experts from the field of information technology. The data was analysed using SPSS version 22.0 and AMOS version 20.0. The results reveal a moderate level of privacy protection behaviour. The perceived vulnerability was found to be the most salient factor in motivating the adoption of privacy protection behaviour with the mediation of information privacy concern, followed by perceived severity, anonymity of self and others, intrusiveness, self-efficacy and response efficacy. Rewards were also found to be mediated by information privacy concern towards privacy protection behaviour although in a negative fashion. The results attained from the analysis produced a model that predicts the motivational factors of privacy protection behaviour among undergraduates. The model was confirmed to account for 61% of the variance (adjusted R2) in privacy protection behaviour. Expert validation was conducted to better understand the survey results and to obtain validation from experts. Several implications were also drawn from the results of the study. The Protection Motivation Theory (PMT) was tested and expanded upon by the integration of the Hyperpersonal Communication theory (HCT). Through this amalgamation as one mediator, the proposed predictive model is definitive and provides a foundation to guide future research in related fields of study.

ABSTRAK

Laman Rangkaian Sosial (LRS) telah berkembang pesat sepanjang dekad yang lalu.Mereka menawarkan pelbagai alat yang memudahkan komunikasi dan perkongsian maklumat. Disebalik kemudahannya, perkongsian yang tidak terkawal boleh membawa kepada kerugian dan eksploitasi privasi. Selain itu, tingkah laku perlindungan privasi untuk melindungi diri daripada risiko dan ancaman di LRS harus ditekankan kerana banyak faktor yang menyumbang kepada tingkahlaku perlindungan privasi tetapi isu-isu yang berkaitan faktor-faktor yang memotivasikan tingkahlaku perlindungan privasi adalah belum diterokai. Kajian ini memberi tumpuan kepada faktor-faktor yang memotivasikan tingkah laku perlindungan privasi. Kajian ini menggunakan pendekatan kajian kuantitatif melalui soal selidik. Populasi kajian ini terdiri daripada pelajar tahun tiga dari universiti awam Malaysia. Saiz sampel minimum adalah 355, walaubagaimanapun 497 soal selidik telah diedarkan. Responden dipilih berdasarkan teknik persampelan berstrata dan rawak berkadar.Instrumen kajian yang telah diadaptasi daripada kajian sebelum ini, dibahagikan kepada tiga bahagian, dan disahkan oleh panel pakar-pakar dari bidang teknologi maklumat. Data dianalisis menggunakan perisian SPSS versi 22.0 dan AMOS versi 20.0. Keputusan mendedahkan tahap sederhana bagi tingkah laku perlindungan privasi. Tanggapan keterdedahan didapati menjadi faktor yang paling penting dalam memotivasikan penggunaan tingkah laku perlindungan privasi dengan perantaraan kebimbangan maklumat privasi, diikuti oleh tanggapan keseriusan, tanggapan ketanpanamaan diri,tanggpan ketanpanamaan orang lain,tanggapan campur tangan, keupayaan diri dan keberkesanan tindak balas. Ganjaran juga didapati dapat diperantarakan oleh kebimbangan maklumat privasi ke arah tingkah laku perlindungan privasi walaupun dengan hubungan yang negatif. Keputusan yang dicapai daripada analisis menghasilkan model yang meramalkan faktor motivasi tingkah laku perlindungan privasi di kalangan mahasiswa. Model ini disahkan mampu menjelaskan 61% daripada varians (selarasan dari R^2) dalam tingkah laku perlindungan privasi.Beberapa implikasi telah terhasil daripada hasil kajian itu. Teori Perlindungan Motivasi (PMT) telah diuji dan diperluaskan dengan mengintegrasikan Teori Hyperpersonal Komunikasi (HCT). Melalui penyatuan ini dan satu pengantara, model ramalan yang dicadangkan itu adalah sahih dan menyediakan asas untuk membimbing penyelidikan dalam bidang yang berkaitan pada masa hadapan.

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious, the Most Merciful.

Firstly, I would like to express my sincere gratitude to my supervisor, Prof. Dr. Rabiah binti Ahmad and MY co-supervisor, Dr. Muliati binti Sedek for the continuous support of my Ph.D study and related research, for their patience, motivation, and immense knowledge. Their guidances helped me in all the time of the research and writing this thesis. Not forgotten, my ex co-supervisor, late Dr Mariana binti Yusoff. May Allah blessed her soul and grant her the highest level of jannah. Besides them, I would like to thank my fellow colleagues who shared their technical knowledge, stimulating discussions, insightful comments and encouragement.

Also, this thesis would not be realized without the continuous loves, prayers and supports from my husband, Mohd Ridzuan bin Jopri, my beloved daughter, Amna Nur Medina, my great parents, my brothers and my sister.

Last but not least, thank you to FTMK, all the administration staffs for their friendly helps and supports throughout this journey in Universiti Teknikal Malaysia Melaka. Besides (UTeM), this research would not be accomplished without the funding UTeM and Ministry of Higher Education Malaysia under the UTeM Fellowship Scheme. Thank you to all of you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF SYMBOLS

Z	-	Standardised score
p	-	Sample proportion
e	-	Estimation error
N	-	Population size
n	-	Sample size
p	-	Level of significant
β	-	Regression coefficient
$\chi 2$	-	Chi-Square Statistic
R^2	-	Squared Multiple Correlations

LIST OF ABBREVIATIONS

AIC	-	Akaike Information Correction
AMOS	-	Analysis of Moment Structures
AVE	-	Average Variance Extracted
CFA	-	Confirmatory Factor Analysis
CFI	-	Comparative Fit Indices
CMIN	-	Minimum Value of the Discrepancy
CMIN/DF	-	Minimum Value of the Discrepancy by its Degrees of freedom
C.R.	-	Critical Ratio for Regression Weight
CR	-	Construct Reliability
CSA	-	Cyber Security Agency of Singapore
CSM	-	Cyber Security Malaysia
DV	-	Dependent Variable
EFA	-	Exploratory Factor Analysis
GFI	-	Goodness-of-Fit Index
HCT	-	Hyperpersonal Communication Theory
IS	-	Information System
IT	-	Information Technology
IV	-	Independent Variable

MI	-	Modification Indices
MCMC	-	Malaysian Communication and Multimedia Commission
MOHE		Ministry of Higher Education
MOSTI	-	Ministry of Science, Technology and Innovation
MyCERT		MyComputerResponseTeam
MYREN		Malaysian Research and Education Network
IPC	-	Information Privacy Concern
PAO	-	Perceived Anonymity of Others
PAOS	-	Perceived Anonymity of Self
PI	-	Perceived Intrusiveness
PMT	-	Protection Motivation Theory
PV	-	Perceived Vulnerability
R	-	Rewards
RE	-	Response Efficacy
RMSEA	-	Root mean Square Error of Approximation
S.E	-	Standard Error of Regression Weight
SE	-	Self-efficacy
SEM	-	Structural Equation Modelling
SNSs	-	Social Networking Sites
SPSS	-	Statistical Package for the Social Science

LIST OF PUBLICATIONS

Othman, N.F., Ahmad, R. & Yusoff, M., 2013. Information Security and Privacy Awareness in Online Social Networks Among UTem Students. *Journal of Human Capital Development*, 6(1), pp.101–110.

Othman, N.F., Ahmad, R. & Sedek, M., 2016c. Factors of Concerning Privacy-Protection Behaviour. In 5th*International Conference on Technology Management, Business and Entrepreneurship (ICTMBE2016).*

Othman, N.F., Ahmad, R. & Sedek, M., 2016a. Determinants of Information Privacy Concern and Privacy Protection Behaviour Strategies in Social Networking Sites among Undergraduates in Malaysia. *5th International Cryptology and Information Security Conference 2016 (Cryptology2016)*, 2016.

Othman, N.F., Ahmad, R. & Sedek, M., 2016b. Factor Motivating Privacy Protcetion Behaviour Strategies and Information Privacy Concern in Social Networking Sites. *Asian Journal of Information Technology*, 15(16), pp.2992–2998.

Othman, N.F., Ahmad, R. & Sedek, M., 2016c. Factors of Concerning Privacy-Protection Behaviour. *International Business Management*, 10(16), pp.3682-3691.

CHAPTER 1

INTRODUCTION

1.1 Introduction

The growth of Social Networking Sites (SNSs) has been phenomenal, with Facebook, Instagram, and Twitter in the lead and others following by example. During the month of September 2015, an estimated total of 1.55 billion monthly active users was reported, with 1.01 billion people using Facebook every day (Facebook, 2015). Meanwhile, in Malaysia, the statistics demonstrated that a total of 13.3 million users or 45.5% of the population were registered as Facebook users (MCMC, 2014b). The increased emergence of users can be attributed to the various tools offered by SNSs that intrinsically encourages and facilitates information sharing and communication between users. SNSs are a growing medium that gathers people with shared interest and thoughts and enables people to stay in touch with their contacts, reconnect with old friends, and establish new relationships with other people. With some of the many applications including communicating with friends, knowledge sharing. updating others on their activities and whereabouts, sharing photos, videos, and archiving events, getting updates on activities by friends, sending messages privately and posting public testimonials (Vithessonthi, 2010; Boyd, 2008; Dwyer & Hiltz, 2007), SNSs offer an attractive way of online social interaction and communication that encourages users to make the most of them. Consequently, concerns regarding the exposure to privacy risks emerge. As supported by Kassim (2008), technology which is capable of storing and sorting huge

quantities of data and is easily accessed by a large number of people may unnecessarily expose it to various threats of individual privacy.

1.1.1 Privacy Protection Behaviour

In general, privacy protection behaviour is an action that individuals perform to keep their information safe. According to Rogers (1983), motivation towards privacy protection behaviour occurs when individuals adopt coping behaviours to control danger, risk or threat. Two coping strategies when facing risky situations is approach and avoidance (Amirkhan, 1990; Endler & Parker, 1990; Piko, 2001). Approach strategies cover fabricating personal information and seeking social support or information, whereas avoidance strategies encompass withholding personal information by self-refraining. Government authorities have prepared a list of best practices while browsing SNSs. One example includes Cyber Security Malaysia (CSM) preparing a list of Best Practices on Social Networking Sites while the Cyber Security Agency of Singapore (CSA) prepared Social Networking Safety Tips. These documents include information regarding possible impacts of using SNSs and suggests relevant guidance and tips to protect the user when making friends online. Unfortunately, apart from the importance of privacy protection behaviour in SNSs, it is also important to investigate the factors that drive users to use and adopt these strategies. Hence, the study of appropriate behaviour that can motivate and encourage users to maximize using privacy protection behaviour may be value added towards information privacy research in SNSs.

1.1.2 Information Privacy Research in Social Networking Sites (SNSs)

Information privacy in SNSs have slowly become an increased attraction among researchers. Several issues have been highlighted through various research. Profiling, data