



## **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 questionnaires 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 R<sup>2</sup>) 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, tanggapan 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 sah 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

	PAGE
<b>DECLARATION</b>	
<b>APPROVAL</b>	
<b>DEDICATION</b>	
<b>ABSTRACT</b>	i
<b>ABSTRAK</b>	ii
<b>ACKNOWLEDGEMENTS</b>	iii
<b>TABLE OF CONTENTS</b>	iv
<b>LIST OF TABLES</b>	viii
<b>LIST OF FIGURES</b>	xi
<b>LIST OF APPENDICES</b>	xiii
<b>LIST OF SYMBOLS</b>	xiv
<b>LIST OF ABBREVIATIONS</b>	xv
<b>LIST OF PUBLICATIONS</b>	xvii
<b>CHAPTER</b>	
<b>1. INTRODUCTION</b>	<b>1</b>
1.1 Introduction	1
1.1.1 Privacy Protection Behaviour	2
1.1.2 Information Privacy Research in Social Networking Sites (SNSs)	2
1.2 Problem Background	4
1.3 Problem Statement	6
1.4 Research Questions	8
1.5 Research Objectives	8
1.6 Hypotheses	8
1.7 Scope and Limitation of Study	10
1.8 Organisation of Thesis	11
<b>2. LITERATURE REVIEW</b>	<b>14</b>
2.1 Introduction	14
2.2 Information Privacy Definition	14
2.2.1 History and Research Related to Information Privacy	17
2.3 Social Networking Sites (SNSs)	21
2.3.1 Definition and Elements	21
2.3.2 Brief History and Typology	24
2.3.3 Privacy Features	28
2.4 SNSs Privacy Issues in Malaysia	31
2.5 Privacy Protection Behaviour	33
2.6 Guidance and Best Practices on SNSs	35
2.7 Behavioural Theory in Privacy Protection Behaviour	37
2.8 Motivational Factors of Privacy Protection Behaviour	39
2.8.1 Perceived Severity	40
2.8.2 Perceived Vulnerability	41
2.8.3 Response Efficacy	43
2.8.4 Self-efficacy	44
2.8.5 Rewards	46

2.8.6	Perceived Anonymity of Self	47
2.8.7	Perceived Anonymity of Others	48
2.8.8	Perceived Intrusiveness	50
2.8.9	Information Privacy Concern	51
2.9	Theoretical Framework	54
2.9.1	Protection Motivation Theory (PMT)	54
2.9.2	Hyperpersonal Communication technology (HCT)	57
2.10	Conceptual Framework	59
2.11	Chapter Summary	64
<b>3.</b>	<b>METHODOLOGY</b>	<b>66</b>
3.1	Introduction	66
3.2	Research Design	66
3.3	Location of the Study	68
3.4	Population	69
3.5	Sample Size	71
3.6	Sampling	74
3.7	Instrumentation	77
3.7.1	Operationalisation of the Constructs	81
3.8	Data Transformation	81
3.8.1	Step One	82
3.8.2	Step Two	82
3.8.3	Step Three	82
3.8.4	Step Four	83
3.9	Scoring and Interpretation	84
3.10	Translation Process	85
3.11	Validity and Reliability Instrument	85
3.11.1	Validity	86
3.11.2	Reliability	90
3.11.2.1	Pilot Study	90
3.12	Data Collection	93
3.13	Data Analysis Procedure	94
3.13.1	Descriptive Statistic	94
3.13.2	Inferential Statistic	95
3.14	Structural Equation Modelling (SEM)	96
3.15	Goodness-of-Fit Criteria	100
3.15.1	Absolute Fit Indices	100
3.15.1.1	Chi-Squares	100
3.15.1.2	Root Mean Square Error of Approximation	101
3.15.2	Incremental or Comparative Fit Indices	101
3.15.2.1	Comparatives Fit Index	102
3.16	Data Preparation in Structural Equation Modelling	102
3.16.1	Exploratory Factor Analysis (EFA)	102
3.16.1.1	Demographic Characteristic	103
3.16.1.2	Construct Validity	103
3.16.2	Confirmatory Factor Analysis (CFA)	116
3.16.2.1	Demographic characteristics	118
3.16.2.2	CFA for Privacy Protection Behaviour	118
3.16.2.3	CFA for Privacy Protection Behaviour Factor	120

3.16.2.4	CFA for Information Privacy Concern	128
3.16.2.5	Summary of CFA analysis	129
3.16.3	Measurement Model Test	129
3.16.3.1	Test of Normality	130
3.16.3.2	Test for Outliers	132
3.16.3.3	Test for Model Fit	133
3.16.3.4	Test for Discriminant Validity	135
3.17	Structural Model	136
3.18	Expert Validation	136
3.19	Chapter Summary	137
<b>4.</b>	<b>FINDINGS</b>	<b>139</b>
4.1	Introduction	139
4.2	Background of Undergraduates	139
4.2.1	General Information about the Use of Social Networking Sites	141
4.3	Privacy Protection Behaviour	142
4.4	Association of Perceived Severity, Perceive Vulnerability, Self-efficacy, Response Efficacy, Rewards, Perceived Anonymity of Self, Perceived Anonymity of Others, Perceived Intrusiveness Towards Privacy Protection Behaviour	145
4.4.1	Assessing Structural Model Validity	145
4.5	Mediator Factor of Motivational Factors of Privacy Protection Behaviour	151
4.5.1	Establish the Presence of Mediator	151
4.5.2	Test for Mediating Effect	152
4.5.3	Results of Hypotheses Testing (Mediation Effect)	154
4.6	Development of Motivational Factors in Privacy Protection Behaviour Model for Social Networking Sites	162
4.7	Expert Validation	166
4.7.1	Information Privacy Concern and Privacy Protection Behaviour	168
4.7.2	Motivational Factors of Privacy Protection Behaviour and Information Privacy Concern	170
4.8	Chapter Summary	173
<b>5.</b>	<b>DISCUSSION</b>	<b>175</b>
5.1	Introduction	175
5.2	Discussion of Research Findings	175
5.2.1	Privacy Protection Behaviour Level	175
5.2.2	Association of Perceived Severity, Perceived Vulnerability, Self-efficacy, Response Efficacy, Rewards, Perceived Anonymity of Self, Perceived Anonymity of Others and Perceived Intrusiveness Towards Privacy Protection Behaviour	177
5.2.3	Role of Information Privacy Concern (Mediator)	180
5.2.4	Motivational Factors in Privacy Protection Behaviour Model For Social networking Sites (SNSs)	185
5.3	Implications	190
5.3.1	Theoretical Implications	190
5.3.2	Practical Implications	191
5.4	Chapter Summary	192

<b>6.</b>	<b>CONCLUSION AND RECOMMENDATION FOR FUTURE RESEARCH</b>	<b>193</b>
6.1	Introduction	193
6.2	Concluding Remarks	193
6.3	Contribution of Research	194
6.3.1	Theoretical Contribution	194
6.3.2	Practical Contribution	195
6.4	Recommendation for Future Research	196
	<b>REFERENCES</b>	<b>198</b>
	<b>APPENDICES</b>	<b>231</b>

## LIST OF TABLES

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	Evolution of the Information Privacy Concept Following the Evolution of IT	19
3.1	The research process flow chart	68
3.2	Total number of undergraduates	71
3.3	Minimum sample size according to formula used	73
3.4	Summary of the proportionate sample size	75
3.5	Components of the questionnaire	78
3.6	Minimum and maximum score	82
3.7	Range calculation	82
3.8	Interval width	83
3.9	Level indication by score categorisation	83
3.10	Scoring for adoption level	84
3.11	Scoring and interpretation of adoption level	84
3.12	Excerpts of feedback from panel of experts	87
3.13	Recommended alpha range	91
3.14	Cronbach's alpha coefficient for each construct	92
3.15	Objectives, research questions, hypotheses and statistical analysis.	94
3.16	Objectives, research questions, hypotheses and statistical analysis.	98

3.17	Demographic characteristics of participants for EFA phase	103
3.18	Factor Eigenvalues (Initial analysis).	104
3.19	Proposed items under each factor	106
3.20	Items factor loadings and communalities (Numbers of factors=8)	111
3.21	Final analysis.	114
3.22	Fit indices and recommended value for CFA	116
3.23	Demographic characteristics of participants for CFA phase.	118
3.24	Fit indices and recommended value for measurement model	130
3.25	Assesment of normality	131
4.1	Demographic data of undergraduates	139
4.2	Types of SNSs used	141
4.3	Duration of using SNSs per day	141
4.4	Privacy protection behaviour adoption	142
4.5	Scoring and interpretation of adoption level of privacy protection behaviour	144
4.6	Level of privacy protection behaviour adoption	145
4.7	Code for each variable	146
4.8	Criteria for fit indices	149
4.9	Standardised regression weights	151
4.10	Hypotheses testing results	152
4.11	Decision criteria for mediation test	152
4.12	Comparison of $\chi^2$ (CMIN), Sig- $\chi^2$ (CMIN/DF), PNFI and AIC values	152
4.13	Decision criteria for mediation effect	154
4.14	Regression weights: Full mediation	154

4.15	Decision Criteria for Perceived Severity	156
4.16	Decision Criteria for Perceived Vulnerability	156
4.17	Decision Criteria for Self-efficacy	157
4.18	Decision Criteria for Response Efficacy	158
4.19	Decision Criteria for Reward	158
4.20	Decision criteria for Perceived anonymity of Self	159
4.21	Decision criteria for Perceived Anonymity of Others	160
4.22	Decision Criteria for Perceived Intrusiveness	160
4.23	Regression weight for the mediation test	161
4.24	Hypotheses testing results (Mediation)	161
4.25	Regression weights (Full mediation)	162
4.26	Potential Interviewees for Follow-Up Qualitative Analysis	167

## LIST OF FIGURES

<b>FIGURE</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	WorldCat non-fiction books and articles with 'privacy' in the title	20
2.2	A typological of SNSs	27
2.3	Protection Motivation Theory	56
2.4	Conceptual framework of the study	63
3.1	Location of Study	69
3.2	Recommendation sample size according to Raosoft software	72
3.3	Chronology of the data collection	89
3.4	Factor Eigenvalues (Initial analysis).	105
3.5	CFA for Privacy Protection Behaviour	119
3.6	CFA for Perceived Severity	120
3.7	CFA for Perceived Vulnerability	121
3.8	CFA for Self-efficacy	122
3.9	CFA for Response Efficacy	123
3.10	CFA for Reward	124
3.11	CFA for Perceived Anonymity of Self	125
3.12	CFA for Perceived Anonymity of Others	126
3.13	CFA for Perceived Intrusiveness	127
3.14	CFA for Information Privacy Concern	128
3.15	Measurement model	134



4.1	Structural Mode	148
4.2	Illustration of a Mediation Design, X Affects Y Indirectly Through M	153
4.3	Proposed predictive model (The Malaysian Students Motivational Factors of Privacy Protection Behaviour)	165
5.1	The Malaysian Students Motivational Factor of Privacy Protection Behaviour	187

## LIST OF APPENDICES

<b>APPENDIX</b>	<b>TITLE</b>	<b>PAGE</b>
A	Questionnaire Distributed to Respondents (Before EFA and CFA)	231
B	Permission from the Universities	244
C	Results of the Mahalanobis distance	248
D	Credential of Translators	251
E	Credential of Content Experts	252

## LIST OF SYMBOLS

$Z$	-	Standardised score
$p$	-	Sample proportion
$e$	-	Estimation error
$N$	-	Population size
$n$	-	Sample size
$p$	-	Level of significant
$\beta$	-	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 *5<sup>th</sup> 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 Protection 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