

**UNDERSTANDING THE INFORMATION PRIVACY-RELATED
PERCEPTIONS AND BEHAVIORS OF AN ONLINE SOCIAL NETWORK USER**

by

Burcu Bulgurcu

B.Sc., Middle East Technical University, 2003

M.Sc., Middle East Technical University, 2006

M.Sc., University of British Columbia, 2008

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF**

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate Studies

(Business Administration)

**THE UNIVERSITY OF BRITISH COLUMBIA
(Vancouver)**

October 2012

© Burcu Bulgurcu, 2012

Abstract

The popularity of Online Social Networks (OSNs) has posed substantial challenges to users in protection of their information privacy. Academic research in this area is still limited in scope and depth. Given the paucity of research in this domain, the following research aims to further our understanding of information privacy in OSNs by focusing on users' information privacy-related perceptions and behavioral responses. To fulfill this objective, one conceptual and two empirical studies have been conducted in this thesis.

The objective of *Study #1* is to develop a theoretical foundation for users' privacy-related perceptions and behavioral responses by integrating two major literatures on *coping* and *information privacy*. This study forms the foundation for the theory and methodology of the subsequent two empirical studies.

The objective of *Study #2* is to develop an empirical understanding of the factors that affect a user's motivation to cope with a privacy threat associated with using a social application.

Drawing on the data collected from 197 Facebook users, the study shows that factors such as a user's benefit, privacy threat, and threat avoidability perceptions are influential on his privacy threat coping motivations.

The objective of *Study #3* is to empirically investigate the factors that shape a user's privacy threat perception, and in turn, his intention to use a social application. Drawing on the data collected from 747 Facebook users, the study reveals that while *permission request* (i.e., the extent of permissions requested by an application to access, process, and utilize a user's personal information) can increase a user's privacy threat perceptions, this effect can be reduced by

privacy control (i.e., the extent of privacy safeguards provided by an application to enable a user to customize the requested permissions according to his privacy preferences).

Overall, this research contributes to the literature by furthering our understanding of (1) an OSN user's perceptions and behaviors that can increase his vulnerability to privacy invasions, (2) the processes by which a user copes with a privacy threat associated with his use of an OSN feature, (3) the factors that affect his privacy threat perceptions and intentions to use an OSN feature.

Preface

This work has not been published yet. The research described in this thesis has been conducted by the student in consultation with members of the supervisory committee. The student has had the full responsibility in identifying and designing the research program, analyzing the research data, and preparing this manuscript.

This research was conducted in accordance with the suggested ethics guidelines of the Human Ethics of the UBC Research Ethics Board. UBC Behavioral Research Ethics Board approved this research via certificate number H10-02810 on June 14, 2011. Completion of the research has been approved via certificate number H10-02810-A001 on June 14, 2012.

Table of Contents

Abstract.....	i
Preface.....	iii
Table of Contents	iv
List of Tables	vii
List of Figures.....	viii
List of Abbreviations	ix
Acknowledgements	x
1 Introduction	1
1.1 Research Motivation	1
1.2 Online Social Networks: A Novel Technology.....	5
1.3 Privacy-Related Challenges in Online Social Networks.....	6
1.5 Structure of the Thesis.....	9
2 An Integrative View on Coping: Online Social Network Users' Identification Of and Coping with Privacy Threats (Study #1)	15
2.1 Overview	15
2.2 Literature Review and Study Contributions.....	17
2.2.1 A User's Threat Avoidance and Coping Behaviors under Privacy Threat.....	17
2.2.2 Coping Theory	19
2.2.3 A User's Opportunity Seeking Behaviors under Privacy Threat.....	21
2.3 Theoretical Framework	23
2.3.1 Primary Appraisal	24
2.3.2 Secondary (Coping) Appraisal.....	27
2.3.3 Behavioral Responses	28
2.3.4 Selection of a Coping Strategy	32
2.3.5 Impact on Outcomes and Reassessment	34
2.4 Different Cases of Information Disclosure	36
2.5 Detailed Frameworks for Intended and Unintended Disclosure	42
2.5.1 Intended Disclosure	44
2.5.2 Unintended Disclosure (initiated by the user or others)	46
2.6 Concluding Remarks and Connections to the Empirical Studies.....	49
3 The Role of Primary and Secondary Appraisal in a User's Coping Motivations: An Empirical Study on Facebook Applications (Study #2)	51
3.2 Theoretical Framework	53

3.3	Research Model and Hypotheses	54
3.3.1	Primary Appraisal	56
3.3.2	Secondary (Coping) Appraisal.....	58
3.3.3	Coping Behaviors.....	59
3.4	Research Method.....	61
3.4.1	Development and Design of Hypothetical Scenarios	61
3.4.2	Development and Design of the Survey Items	64
3.4.3	Data Collection: Selection of Participants and Procedure	66
3.5	Data Analysis and Results.....	69
3.5.1	Assessment of Measurement Validation.....	69
3.5.2	Results of the Structural Model Testing	74
3.6	Discussions and Conclusions	78
3.6.1	Discussion of Findings and Implications.....	78
3.6.2	Limitations and Future Research	80
4	The Roles of Permission Requests and Privacy Controls in Shaping a User's Primary Appraisal and Use Intentions: An Empirical Study on Facebook Applications (Study #3)	83
4.1	Overview	83
4.2	Theoretical Framework and Hypotheses.....	86
4.2.1	Definitions of Variables.....	87
4.2.2	Development of Hypotheses	89
4.3	Research Method.....	94
4.3.1	Study Design and Operationalization of Variables.....	94
4.3.2	Sample and Data Collection.....	100
4.4	Analysis and Results	101
4.4.1	Control and Manipulation Checks	101
4.4.2	The Results of Hierarchical Linear Modeling	104
4.4.3	The Results of ANOVA Tests	109
4.5	Discussions and Conclusions	114
4.5.1	Discussion of Findings.....	114
4.5.2	Limitations and Future Research	117
5	Conclusions	120
5.1	Summary of the Thesis.....	120
5.2	Contributions of the Thesis	123
5.3	Limitations and Suggestions for Future Research.....	125
	Bibliography	128
	Appendices.....	137
	Appendix A: Supporting Material for Chapter 3	137
	Appendix A1: Hypothetical Scenarios and Graphical Interfaces	137

Appendix A2: Scenarios with Different Types of Benefits.....	146
Appendix A3: Sample Demographics	147
Appendix A4: Validity Analysis	150
Appendix B: Supporting Material for Chapter 4	153
Appendix B1: Graphical Interfaces for Healthy Living.....	153

List of Tables

Table 1: Summary of Privacy Research that focus on OSN	3
Table 2: Research Designs for the Proposed Studies.....	13
Table 3: The Threat Avoidance and Coping Behaviors Proposed in the Privacy Literature.....	18
Table 4: Opportunity Seeking Behaviors in the Privacy Literature.....	22
Table 5: Different Forms of Disclosure	38
Table 6: Summary of a User's Opportunity Seeking and Threat Avoidance Behaviors	43
Table 7: Definitions and Sources of Key Constructs.....	56
Table 8: Sources of Measurement Items.....	65
Table 9: Measurement Items and Item Loadings.....	71
Table 10: Studies in the IS literature that focus on control.....	85
Table 11: Operationalization and Sources of Constructs.....	87
Table 12: Comparison of Low vs. High Permission Request Interfaces	95
Table 13: Comparison of Low vs. High Privacy Control	96
Table 14: Measurement Items and Item Loadings.....	97
Table 15: Experimental Conditions, Scenarios, and Survey Links	99
Table 16: Manipulation Check Questions.....	103
Table 17: ANOVA Results for Manipulation Checks	103
Table 18: The Effect of Control Variables on Intention (Independently)	105
Table 19: The Results of Hierarchical Linear Regression	106
Table 20: Results of Mediation Analysis.....	109
Table 21: ANCOVA Table for Perceived Benefit.....	110
Table 22: ANOVA Table for Perceived Privacy Threat.....	110
Table 23: Post-Host Test Multiple Comparisons for Benefit Privacy Threat.....	112
Table 24: Exclusion Criteria	147
Table 25: Profiles of Responding Participants.....	147
Table 26: Composite Reliability, AVE, and Latent Variable Correlations	150
Table 27: Cross Loadings	151
Table 28: Sample Demographics for Study 3	157

List of Figures

Figure 1: A Brief Summary of Thesis Research	10
Figure 2: A Process View on Theories on Coping and Information Privacy	24
Figure 3: Intended Disclosure (Proactive Coping – Avoiding a Threat)	42
Figure 4: Unintended Disclosure (Reactive Coping – Coping with Existing Threat)	42
Figure 5: A Framework for Privacy Threat Avoidance and Coping (Study #2)	55
Figure 6: The Results of the Structural Model Testing (Study #2).....	75
Figure 7: Interaction Graph for Threat Avoidability and Privacy Threat	77
Figure 8: A Theoretical Framework for Study 3	86
Figure 9: Age on Intention.....	105
Figure 10: IT Knowledge on Intention	105
Figure 11: The Effect on Privacy Threat & Benefit Interaction on Intention.....	108
Figure 12: Permission Request * Privacy Control Interaction on Privacy Threat.....	111
Figure 13: Post-Hoc Analysis for Privacy Threat.....	113
Figure 14: Post-Hoc Analysis for Benefit.....	114
Figure 15: Application Interface for Scenario 1: City Spot.....	142
Figure 16: Application Interface for Scenario 2: Whole Ancestry	143
Figure 17: Application Interface for Scenario 3: Site Share.....	144
Figure 18: Application Interface for Scenario 4: Healthy Living.....	145
Figure 19: Mean Value of Different Types of Benefit Perceived in Each Scenario.....	146
Figure 20: Interface for Low Request and High Privacy Control (Group 1).....	153
Figure 21: Interface for High Request and High Privacy Control (Group 2)	154
Figure 22: Interface for Low Requests and Low Privacy Control (Group 3).....	155
Figure 23: Interface for High Requests and Low Privacy Control (Group 4)	156

List of Abbreviations

EFC	Emotion-Focused Coping
HC	High Control
IS	Information Systems
IT	Information Technology
LC	Low Control
PFC	Problem-Focused Coping
OSN	Online Social Network
PA	Primary Appraisal
SA	Secondary (Coping) Appraisal

Acknowledgements

I am very happy about reaching this milestone in my academic career, and hereby would like to express my deepest gratitude to those who have touched upon my life.

I foremost would like to thank and express my heartfelt gratitude to my advisors, Prof. Izak Benbasat and Prof. Hasan Cavusoglu. I am mostly grateful to them for challenging me to achieve my highest potential and helping me to live through those challenges by providing their fullest guidance and support. I am fairly confident that without those challenges, I would not be where I am today. I sincerely appreciate that both my advisors have always found the time to devote to our long research meetings, answer all my questions, and provide the most insightful and prompt feedback despite their busy schedules. I also would like to express my appreciation to my committee member, Prof. Olga Volkoff, who took time out of her busy schedule to be part of my thesis committee and provided her insights to improve this work. Her support over the course of this work and my subsequent job search endeavor was very important to me.

I am grateful to the Social Sciences and Humanities Research Council of Canada (SSHRC) for valuable funding to support this research and to the Sauder School of Business, SSHRC, UGF, and Affiliated Awards of UBC for scholarships they granted to support my doctoral education.

I am thrilled that I will start my academic career at Boston College (BC). I would like to thank to the entire faculty in the IS Department of BC for being so welcoming during my campus visit. My particular thanks to Andy Boynton, Gene McMahon, Rob Fichman, Jerry Kane, and Sam Ransbotham, who have been extremely helpful, informative, and considerate during the process of recruitment. I feel truly privileged about being offered the job I have dreamed about and given the opportunity to be colleagues with the wonderful group of academics at BC.

I feel very fortunate that I have completed my graduate education at one of the greatest institutions and would like to thank the entire faculty at the MIS division of UBC. Yair Wand, Carson Woo, Ron Cenfetelli, and Mingdi Xin: thank you for inspiring me with your research agenda, offering the amazing courses that taught me the basics of conducting good research, and supporting me during my education. I owe particular thanks to Prof. Andrew Burton-Jones, who has always been willing to contribute to my work and provided me with the fullest emotional support. I have learnt so much from him, especially the ethics of being a good professor everyone would aspire to be and a wonderful colleague everyone would wish to work with.

The discussions I had with the other graduate students in and out of the classroom were instrumental in developing my research and teaching portfolio and passion for academia. I particularly would like to thank to my peers and friends who are or have once been graduate students in the MIS division: Eruani, Camille, David, Lior, Michael, Usman, Niran, Tae, Hongki, Shan, Cheng, Kafui, Sameh, Daniel, Wei, Arash, Landon, Chee-Wee, Cagri, Ali, and Bo – I will always remember the times we shared together with joy. Eruani, I can't think of my first two years without you. You were so helpful and patient with my endless questions about our class work and research. Sameh, thank you so much for never rejecting any of my help requests; Kafui, for sharing your passion in teaching and helping me out with my first time teaching preparations; Cheng and Shan, for being great hosts when we were in Shanghai; and Usman, for your detailed feedback on my research – it was very helpful to have another student who is

embedded in the privacy literature. Camille, David, Lior, and Michael – I am delighted to have shared most of the classes with you. Our research discussions have been real eye-openers to me.

I would like to thank the professors and colleagues in the IS community that I have met in person at conferences or through reading their research work; the inspiration I got from them was instrumental in my decision to pursue this fascinating path of academics. I am deeply indebted to Henri Barki, Merrill Warkentin, and Geneviève Bassellier for their tremendous support and mentorship. I am also grateful to the faculty and fellow doctoral students that I have met at the Doctoral Consortiums (AMCIS 2011, MCIS 2011, ICIS 2011)—Ritu Agarwal, Anne Massey, Rob Kauffman, Jae Kyu Lee, Gal Oestreicher, Bruce Weber, Harrison McKnight, and Hope Koch—thank you for your contributions to the Consortiums and to my work. Thanks also to the anonymous reviewers and editors of our papers—I have learnt a lot from your advice. I owe a big thanks to Bengisu Tulu; she has been a great friend, role model, and mentor whom I asked for advice every time I felt in trouble. Talking to her has always had the power to lighten up my day! My friend, Wietske Van Osch—thanks for making conferences so much fun!

I would like to thank my very special professors at the Organizational Behavior and Human Resources department of UBC, where I took all my elective courses from. Special thanks are to Prof. Sally Maitlis, Prof. Sandra Robinson, Prof. Karl Aquino, and Prof. Martin Schultz for the wonderful courses they had offered. What I have learnt in their classes has greatly influenced the direction and quality of the work I have produced. I also would like to thank Ms. Elaine Cho, our graduate studies assistant, without whom I would not be able to navigate through the administrative issues of the PhD program. She is one the most reliable, detailed oriented and hard working people I have ever met, and her assistance was phenomenal.

I am thankful to my professors at the Informatics Institute, Middle East Technical University (METU) – Prof. Semih Bilgen, Prof. Onur Demirors, and Prof. Kursat Cagiltay – who encouraged and supported me to take on this academic journey. I certainly would not have built my interest in the IS field without the Institute at METU. I still so much miss the times and friends from those days. My special thanks to my old time friends Evrim Baran and Burcu Akkan for sharing the wonderful times. Evrim, also thanks for sharing the overseas dreams.

I am blessed with a wonderful family. I would like thank my father, Zuher Bulgurcu, my mother, Celile Bulgurcu, and my dear sister and best friend, Buke Bulgurcu, for their eternal love and support that I have felt at every stage of my life. There is no doubt that I would not feel as happy and strong without their presence in my life. My grandfather Munir—rest in peace – it is thanks to his genes in me that I love to read and write, and made the decision to pursue an academic career. Thanks to my beautiful extended family: my grandmother, aunts, uncles, and cousins for their attention, care, and love. I love and miss you all.

Most of all, I would like to thank to my partner, Tolga Canatan, who held my hand throughout this tough journey and had to endure the insanity of a graduate student life with me. Thank you for making life much more pleasant with your beautiful heart, love, tenderness, and friendship; and much more fun with your *joie de vivre* and great sense of humor... Thank you for making such a faraway place home for me; teaching me your amazing skills in simplifying and planning everything; sharing your wisdom and helping me develop my very own perspective about pursuing an academic career; and looking out for my health and sleep when they were not my priorities. You make my life meaningful!

1 Introduction

1.1 Research Motivation

Prior research on information privacy has focused on several important questions to date. Privacy literature has primarily focused on the antecedents and outcomes of technology users' privacy concerns (Smith et al. 2011) by focusing on various technology settings, such as; *electronic commerce* (e.g., Dinev and Hart 2006; Hui et al. 2007; Malhotra et al. 2004; Van Slyke et al. 2006), *direct marketing* (e.g., Culnan 1993; Culnan and Armstrong 1999; Hine and Eve 1998; Milne 2000; Nowak and Phelps 1992; Sheehan and Hoy 1999; Smith et al. 1996), *Internet use* (e.g., Dinev and Hart 2004; Korzaan et al. 2009; Malhotra et al. 2004; Son and Kim 2008), *data mining and profiling* (Awad and Krishnan 2006; Chellappa and Sin 2005; Cranor et al. 2000), *electronic health* (Angst and Agarwal 2009); *financial portals* (Hann et al. 2007), *online and mobile advertising* (Lwin et al. 2007; Okazaki et al. 2009), and *ubiquitous computing* (Xu et al. 2009; Xue et al. 2010).

A burgeoning stream of research is investigating information privacy in *Online Social Networks (OSNs)*—a novel and fast-advancing technology, which has emerged in recent years and quickly become an indispensable tool for hundreds of millions of Internet users. OSNs are one of the defining elements of the contemporary Internet generation. A recent report indicates that the number of active OSN users surpassed one billion in 2012 (ITU 2012). Four-fifths of Internet users were reported to visit OSNs (Nielsen 2011). Two-thirds of Internet users worldwide were reported to use at least one OSN service (Madden and Zickuhr 2011). A single OSN platform (i.e., Facebook) was reported to hosts over 69 billion friendship connections (Facebook Statistics 2011). Another platform (Twitter) hosts over 175 million tweets everyday (Twitter Statistics

2012). The profile of users is also becoming diverse, with a growing number of organizations, public entities, telecom/ICT regulators and government agencies joining the individual and business users in using OSNs (ITU 2012).

The popularity of OSNs has introduced substantial new challenges (Awareness 2012), one of which is related to information privacy. Privacy issues associated with OSN use can be widespread, ranging from technical to legal issues. The consequences of these issues can be highly critical in regards to personal lives (Justice 2007), career liabilities (Jones and Soltren 2005; Rosenblum 2007), and damages to reputations (Survey 2009), and can affect users both materially (e.g., identity theft, physical stalking) and psychologically (e.g., embarrassment, shame).

Despite the inherent problems, use of OSNs can offer a range of opportunities for their users. Individuals can develop personal and business relationships; businesses can establish their brands and bring attention to their products or services; government agencies can inform and interact with the public. These opportunities, however, entirely depend on active user involvement and participation in OSNs (Ellison et al. 2007; Krasnova et al. 2009). When users are reluctant to participate as a result of their privacy concerns, not only OSN developers and individual users but also businesses and public entities that function on these platforms suffer the consequences. It is, therefore, essential to develop a deeper understanding of the OSN landscape. By doing so, the importance of this new platform can be acknowledged and the privacy-related issues associated with its use can be properly addressed.

Despite the recent attention in the academic community, research that focuses on privacy issues in OSNs is still limited in scope and depth. A few empirical studies conducted in this domain

represent important but limited research efforts (Acquisti and Gross 2006; Boyd 2008; Bulgurcu et al. 2010b; Debatin et al. 2009; Dinev et al. 2009; Dwyer et al. 2007; Govani and Pashley 2005; Hoadley et al. 2010; Hoy and Milne 2010; Jones and Soltren 2005; Krasnova et al. 2009; Krasnova and Veltri 2010). These studies depict potential privacy risks that emerge with the use of OSN systems (Boyd 2008; Jones and Soltren 2005) and show the factors that may trigger users' privacy concerns regarding their use of these systems (Bulgurcu et al. 2010b; Hoadley et al. 2010). The literature also showed that despite their concerns for privacy (or their awareness on privacy risks), users may continue revealing their personal information on OSN platforms (Acquisti and Gross 2006; Debatin et al. 2009; Govani and Pashley 2005; Krasnova and Veltri 2010). The studies are summarized in Table 1.

Table 1: Summary of Privacy Research that focus on OSN

Study	Brief Summary
Acquisti and Gross 2006	The impact of Facebook users' privacy concerns were examined on their behaviors. It was found that privacy concerns are a weak predictor of behavior, as concerned users still join the network and reveal personal information.
Boyd 2008	Facebook users' privacy concerns associated with the "News Feed" feature are examined.
Bulgurcu et al. 2010b	Drawing on content analysis of user responses to the revisions in the Facebook Privacy Policy, a process model was developed to explain the processes by which privacy concerns emerge.
Debatin et al. 2009	Facebook users' awareness of privacy issues was investigated. Users who reported a prior privacy invasion were found to be more likely to change privacy settings than those merely hearing about others' privacy invasions.
Dwyer et al. 2007	A qualitative study was conducted to develop a framework that models how OSN users' attitudes towards privacy and impression management influence development and maintenance of relationships through technology features.
Govani and Pashley 2005	Students' awareness of privacy issues and privacy protection tools were investigated with a survey study. It was found that most students

Study	Brief Summary
	were aware of possible consequences of providing personally identifiable information but were still comfortable with disclosing. Despite their awareness of protection tools, they did not take the initiative to protect their information.
Hoadley et al. 2010	A survey was conducted with Facebook users to examine their feelings about the changes in the “News Feed” feature, explore the reasons that make them upset about the changes, and show how the changes affect their behaviors. The results showed the specific factors that triggered users’ privacy concerns about this feature.
Hoy and Milne 2010	Gender differences were investigated in young adults' privacy beliefs, their reactions to behavioral advertising, personal information-sharing behaviors, and privacy protection behaviors on social networks. Results of the survey reveal gender differences in these areas.
Jones and Soltren 2005	Based on the analysis of Facebook, specific privacy risks of the system were discussed and recommendations were made to address these issues.
Krasnova and Veltri 2010	The differences in privacy perceptions of Facebook users were examined between respondents from Germany and USA. Respondents from USA were found to have higher level of intention to disclose personal information than the ones from Germany. Although respondents from Germany were found to attribute higher probability to privacy-related violations, respondents from USA indicated higher level of privacy concern, benefits, trust, and control.

In order to expand our knowledge in this domain, this research focuses on understanding OSN users’ privacy-related behaviors. In the remainder of this chapter, the concept of the OSN is briefly defined. Then, the characteristics of OSNs which make potential invasions of information privacy easier are discussed. Next, research questions and a brief summary of each study are presented. Finally, the overall structure and method of the thesis are briefly described.

1.2 Online Social Networks: A Novel Technology

An OSN refers to “a web-based network which is designed for a user to (1) construct public or semi-public profiles for self-expression and social interactions, (2) articulate a list of other users to share connections, (3) view or traverse a list of connections and those made by others within a bounded system” (Boyd and Ellison 2008, p. 211). OSNs help develop a social structure which connects its users by one or more specific types of interdependencies (e.g., friendship, professional relationships, financial exchange etc.) and facilitate interaction between members through their self-published personal profiles (Acquisti and Gross 2006).

A variety of OSN platforms are available to serve Internet users today. These platforms range from massive networks that serve general purposes (e.g., Facebook) to subject-specific networks that serve a particular user interest (e.g., LinkedIn as a professional network). Regardless of their purposes, all OSNs share some common technical features. An *OSN feature* refers to a small functional unit that enables a user to disclose information about himself and to interact with other network users. Each of these features serves a specific purpose and carries different benefits to platform users. For example, a “*photo upload*” feature enables a user to share his pictures with his friends. A “*like*” feature enables a user to give positive feedback regarding the online material shared on the platform (e.g., comments, status messages, links, and pictures). “Liking” company pages or adverts also enables the user to connect with the things he cares about as updated content from those liked pages will be visible on his “news feed”. A “*group*” feature enables a user to create a group for those who share common interests or are associated with certain affiliations. This feature allows group members to share online materials and hold discussions within the group which can be open or closed to other platform users.

1.3 Privacy-Related Challenges in Online Social Networks

Altman (1975) defines privacy as “selective control of access to the self”. Privacy represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability (Margulis 1977, p. 10). New technologies often create novel grounds for potential information privacy invasions. OSNs are no exception. The challenges to information privacy posed by the use of an OSN may in fact closely resemble those posed by the use of other online technologies. Shared concerns are usually related to a set of well-known information practices that threaten a user’s information privacy, such as: access to, disclosure of, or secondary use of his personal information. However, OSNs with their inherent characteristics are more conducive to privacy invasions as their mere existence relies on a heavy dissemination of personal information.

Firstly, real life relationships are often too complex and difficult to be properly represented on a technology platform. While individuals might have intricate and diverse ties with others in their offline (real-life) relationships, the representation of these ties are often overly simplified in OSNs (Boyd and Ellison 2008; Ellison et al. 2007). Ramifications of privacy violations depend heavily on whom the information is being disclosed to, because the type and the sensitivity of information an individual shares with a strong tie (e.g., a family member or a close friend) can differ greatly from what he would share with his weak ties (e.g., colleagues, distant friends, acquaintances, or strangers). As a result of not being able to properly represent real-life ties in an OSN platform, information can be visible to a variety of network members, possibly including unwanted ones. For example, Facebook users add each new connection as a “friend”. To represent offline ties accurately (e.g., friend, family, acquaintance etc.), a Facebook user has to assign these online ties to pre-defined “groups” provided by Facebook or groups created by the

user. He also has to manage privacy settings of these groups and identify the groups to which he would disclose each time he shares a piece of information on Facebook. This is obviously a costly process in terms of time and effort, not undertaken by most of the Facebook users.

Secondly, the number of online ties a user has in an OSN platform can be much larger than that of his offline connections. As the number of strong (intimate) relationships hardly increases in the offline world, the increase in the number of online ties can be attributed to the increase in the number of weak ties (Donath and Boyd 2004). In fact, most OSN users may have a dozen of intimate ties (i.e., close friends and family), but hundreds of additional weak ties (i.e., acquaintances and distant friends). As a result, when a user thinks that the personal information he discloses is shared only among a group of intimate friends, he may end up sharing it with a large number of “friends”, potentially including people he may not even know (Boyd and Ellison 2008; Donath and Boyd 2004). As reported in Facebook Statistics (2009), a Facebook user on average is involved in a direct or reciprocal communication with only 33 of his online friends among the 500 he may have. In such an environment, where the proportion of weak ties to strong ties is significantly high, potential for privacy invasions can be tremendous (Gerstein 1978; Gerstein 1984).

Thirdly, OSN users, who are expected to play an active role in protecting their personal information, are in fact provided with the essential privacy controls and given the ability to manage the outflow of their personal information. As stated by Pincus (2004), “OSNs have the potential to create an intelligent order in the current chaos by letting users manage how public they make themselves and why and who can contact them”. Yet, protection of personal information can still be a substantial challenge for most users for a number of reasons. First, users can be poor detectors of technology-related threats (Xiao 2010). Detection of privacy

threats can be especially challenging for OSN users as they disclose their personal lives voluntarily to enhance their social interactions with others. In such settings, it can be difficult for users to anticipate potential negative implications of their actions. Second, privacy controls can be extremely complex for most users (Ackerman and Mainwaring 2012; Gates 2010), and their adoption can be costly. There is hardly any evidence showing whether users understand and effectively use given privacy controls in an OSN platform.

Lastly, interactions in an OSN platform can be complex to keep track of for most users, as the actors involved in the network are usually highly diverse, ranging from friends to site owners, friends of friends to third-parties in the network (e.g., hackers, governments, advertisers, and application developers). In such a complex setting, it can be difficult for an OSN user to anticipate which of these actors would have access to his personal information.

1.4 Research Questions

The goal of this thesis is to further our understanding of information privacy in the domain of OSNs—an understudied context in the privacy literature. As a high level objective, this research aims to shed light on OSN users' privacy-related perceptions, behaviors, and vulnerabilities to privacy invasions. By focusing on OSN setting, this research also aims to ascertain the extent to which results in this context converge or diverge with previously studied technology settings, and to highlight the outcomes that are more or less salient in this particular context (Smith et al. 2011). This research fulfills these objectives by providing answers to the following questions:

1. How does a user cope with a privacy threat in an OSN platform? (addressed in Study #1)

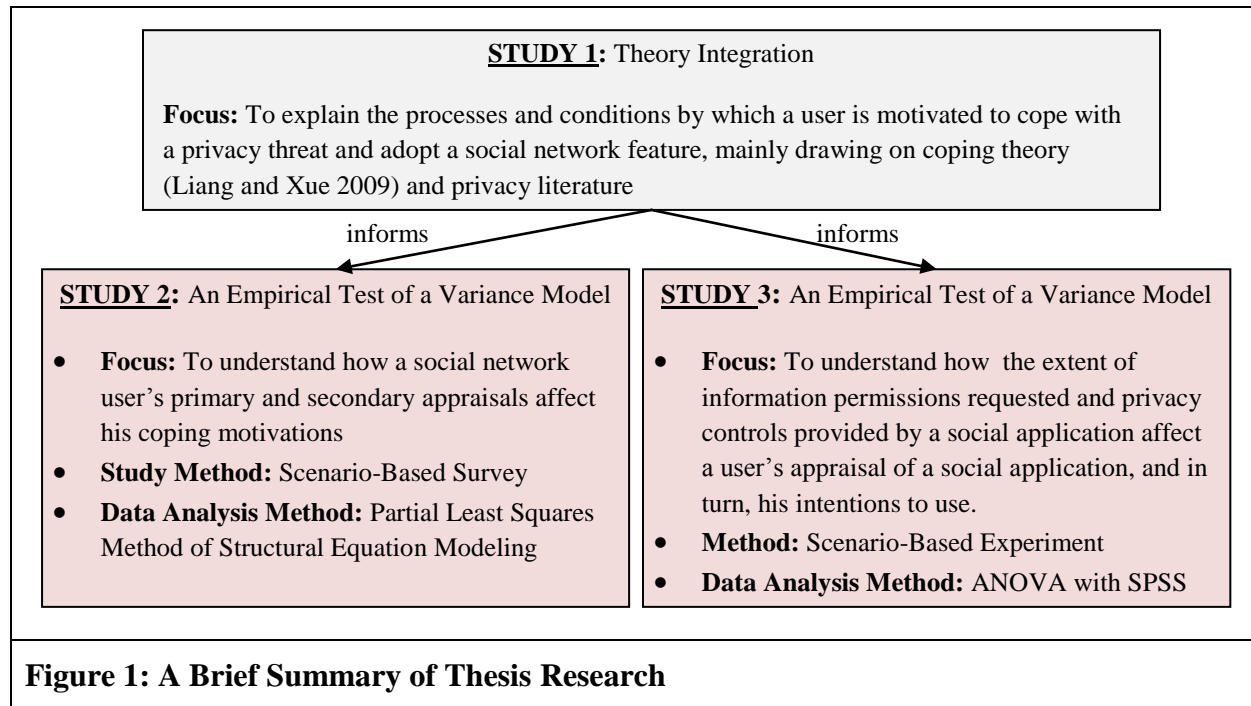
2. What are the factors that affect a user's motivation to cope with a privacy threat associated with a particular OSN feature (i.e., Facebook applications)? (addressed empirically in Study #2)
3. What are the factors that shape a user's privacy threat perceptions, and in turn, affect his intention to use a particular OSN feature (i.e., Facebook applications)? (addressed empirically in Study #3)

Answers to these questions will shed light on the factors that shape OSN users' privacy threat perceptions, the ways they cope with privacy threats, and their vulnerabilities to privacy invasions. The answers can be of interest to not only academic researchers, but also regulators, government agencies, and privacy advocacy groups. Regulators are increasingly asked to develop policies and regulatory frameworks to prevent the privacy-related challenges associated with the use of OSNs (Trends 2012). The results of this thesis can inform regulators in developing public policies for OSN privacy and designing privacy awareness programs, as the results show whether users are vulnerable to privacy invasions. The results can also inform developers of OSN platforms and applications that run on these platforms in designing and promoting their technologies, as the results show the situations that inhibit use of these technologies.

1.5 Structure of the Thesis

To fully answer the proposed research questions, three separate but complementary studies are conducted in this thesis. A brief summary of the research program is presented in Figure 1. A

detailed summary of the studies, including the research designs, key constructs, target participants, and data analysis methods, are presented in Table 2.



The objective of *Study #1* is to develop a theoretical foundation for users' privacy-related perceptions and behavioral responses by integrating two major literatures on *coping* and *information privacy*. The former describes the processes by which an individual copes with a harmful event; and the latter explains the factors that affect a technology user's behavioral reactions in the presence of his privacy concerns. Drawing on Coping Theory (Lazarus 1966), Threat Avoidance Theory (Liang and Xue 2009), Coping Model of User Adaptation (Beaudry and Pinsonneault 2005), and the information privacy literature, this study proposes that an OSN user's *primary appraisal* (i.e. a user's assessment of the consequences of using an OSN feature) and *secondary (coping) appraisal* (i.e., a user's assessment of his control over using the feature) are instrumental in determining his motivations to cope with a privacy threat and his intentions to adopt an OSN feature. The study also differentiates between different types of OSN features and

discusses how these differences can affect a user's coping and use motivations. As a main contribution, this study forms the foundation for the theory and methodology of the subsequent two empirical studies in this thesis.

The objective of *Study #2* is to develop an empirical understanding of the factors that affect a user's motivation to cope with a privacy threat associated with using a social application (i.e., Facebook applications). This study is conducted as a *scenario-based survey*. Scenarios in the survey are designed to set a challenging situation for respondents (i.e., in which they are likely to perceive both high benefits and high privacy threats associated with the given scenario). Drawing on the data collected from 197 Facebook users, the study shows that a user's benefit, privacy threat, and control perceptions are influential on his privacy threat coping motivations. As a main contribution, this study shows that the effect of a user's benefit perception on his privacy threat coping motivations can be as influential as that of his privacy threat perception.

The objective of *Study #3* is to empirically investigate the factors that shape a user's privacy threat perceptions, and in turn, his intention to use a social application (i.e., Facebook applications). This study focuses on explaining the effects of two factors: *permission request* (i.e., the extent of information related permissions requested by an application to access, process, and utilize a user's personal information) and *privacy control* (i.e., the level of privacy safeguards provided by an application to enable a user to customize the permissions according to his privacy preferences). The study is conducted as a *scenario-based experiment*, using the scenarios adopted from Study #2. Drawing on the data collected from 747 Facebook users, the study reveals that while the extent of permission requests can increase a user's privacy threat perceptions, this effect can be reduced by the given privacy controls. The study also shows the dominant effect of a user's benefit perception on his intention to use an application.

The remainder of this thesis is organized as follows. Chapter 2 presents a theory integration work (Study #1). Chapter 3 and Chapter 4 present two empirical studies (Study#2 and Study #3) that build upon the proposed theoretical foundation and test the relationships through scenario-based empirical methods. The specific objectives, research questions, theoretical foundations, research methods, and results of these empirical studies are presented in those chapters. Chapter 5 briefly summarizes the key findings and contributions of this research and suggests further research directions.

Table 2: Research Designs for the Proposed Studies

	Study 1	Study 2	Study 3
Study Scope	A Theoretical Review	Empirical Test of a Model	Empirical Test of a Model
Context	Social Networks	An instance of a social network (i.e., Facebook Applications)	An instance of a social network (i.e., Facebook Applications)
Method	N/A	Scenario-based Online Survey	Scenario-based Online Experiment
Study Design	N/A	Random assignment of developed hypothetical scenarios to study respondents.	<ul style="list-style-type: none"> Four scenarios are adopted from Study 2. A 2 (high vs. low permissions requested) by 2 (limited vs. full controls provided) experimental design is employed for each scenario. Random assignment of one of 16 hypothetical scenarios (4x2x2) to study respondents.
Explanations	N/A	The survey starts with exclusion questions and ends with demographics questions. Respondents are provided with scenario descriptions and application interfaces to answer the survey questions. While the scenario descriptions are the same in Study 2 and Study 3, application interfaces are different. The interfaces used in Study 2 are manipulated for the treatment groups in Study 3.	
Dependent Variables	Intention to Use Privacy Threat Avoidance	Problem-Focused Coping Emotion-Focused Coping	Intention to Use
Independent Variables	Perceived Benefit Perceived Privacy Threat Perceived Control	Perceived Benefit Perceived Privacy Threat Perceived Threat Avoidability	Perceived Benefit (Mediator) Perceived Privacy Risk (Mediator) Cost of Using Privacy Controls (Mediator) The extent of Permissions Requested

Study 1		Study 2		Study 3	
			The extent of Privacy Controls Provided		
Controls	N/A	Age, gender, education, experience with use of Facebook and social applications, perceived trust of applications, benefit and scenario type			
Target Participants	N/A	Active Facebook users from the United States		Active Facebook users from the United States	
Exclusion Questions	N/A	I am a Facebook user. (End survey if not a user) I login to Facebook at least once a week. (End survey if less than once a week)			
Sampling Method		Stratified Random Sampling		Stratified Random Sampling	
Sample Size	N/A	200 Subjects (50 for each scenario x 4)		800 Subjects (50 for each scenario x 4 x 2 x 2)	
Data Analysis	N/A	PLS approach to Structural Equation Modeling with a focus of explaining of the theoretical model and dependent variables with high R ²		Hierarchical Linear regression with a focus of explaining of the dependent variables with high R ² . ANOVA with a focus of explaining the impact experimental constructs on dependent variables with F-tests	

2 An Integrative View on Coping: Online Social Network Users' Identification Of and Coping with Privacy Threats (Study #1)

2.1 Overview

A burgeoning stream of research in the area of information security and privacy indicates a growing interest in understanding technology users' threat avoidance, compliance, and information protection behaviors for safe computing (Anderson and Agarwal 2010; Bulgurcu et al. 2010a; Herath and Rao 2009; Johnston and Warkentin 2010; Liang and Xue 2009; Liang and Xue 2010; Marett et al. 2011). Yet, little is known about the process by which a technology user copes with a privacy threat associated with the use of Online Social Networks (OSNs) and seeks opportunities in this platform. The objective of this study is, therefore, to further our understanding in this area by proposing a theoretical framework based on the integration of two major literatures on coping and information privacy. The former describes the processes by which an individual copes with a harmful event; the latter investigates the factors that affect a technology user's behavioral reactions in the presence of his privacy concerns. The proposed framework aims to answer the following research questions:

1. How does a user cope with a privacy threat in an OSN platform?
2. What are the different situations that may cause privacy threats in an OSN platform?
3. How do these situations shape a user's behavioral responses (i.e., opportunity seeking and coping) in an OSN platform?

To address these questions, a theoretical framework is proposed by integrating two distinct but related streams of literatures—*coping and information privacy*. Drawing on Coping Theory (Lazarus 1966; Lazarus and Folkman 1984; Lazarus and Launier 1978), Threat Avoidance Theory (Liang and Xue 2009), Protection Motivation Theory (Rogers 1975), Coping Theory of User Adaptation (Beaudry and Pinsonneault 2005), *the first part of the framework* postulates that a user's privacy threat avoidance and coping behaviors are instigated by two key processes that constantly influence each other: **Primary Appraisal** (i.e. a user's assessment of the expected consequences of disclosing personal information) and **Secondary (Coping) Appraisal** (i.e. a user's assessment of his control over the situation). Drawing on the information privacy literature, especially the notion of privacy calculus (i.e., a user's costs-benefit analysis regarding the consequences of disclosing personal information), *the second part of the framework* explains the roles of these processes (i.e., primary and secondary appraisal) in determining a user's opportunity seeking behaviors (i.e., adoption and use).

Overall, the framework aims develop a deeper and more comprehensive understanding of the factors that affect a user's information protection behaviors, with a particular focus on OSNs.

This chapter is structured as follows. The next section presents a brief review of the relevant literature, discusses the scope of the investigation, and highlights the unique contributions of the proposed framework. Section 2.3 presents a high level framework to describe how the two literatures on coping and information privacy are integrated. Section 2.4 builds upon this framework to extend it to two different situations (i.e., where information disclosure through an OSN feature is initiated by the user or by others). Section 2.5 briefly summarizes the chapter and describes how the proposed framework informs the two subsequent empirical studies that are carried out in this thesis.

2.2 Literature Review and Study Contributions

2.2.1 A User's Threat Avoidance and Coping Behaviors under Privacy Threat

An emerging research stream on information privacy has focused on a user's threat avoidance and prevention strategies (Debatin et al. 2009; Egelman et al. 2009; Korzaan et al. 2009; Stewart and Segars 2002 Kim and Hsieh 2003; Lwin et al. 2007; Sheehan 2002; Sheehan and Hoy 1999; Stone et al. 1983; Wirtz et al. 2007). These studies have provided some theoretical and empirical evidence of the relationship between users' threat perceptions and their preventive responses.

A recent study by Debatin et al. (2009) has focused on the context of an OSN (i.e., Facebook) to explore the factors that affect a user's privacy attitude about information disclosure, and in turn his behavioral reactions (i.e. changing privacy settings). The results, based on quantitative and qualitative analysis, showed that users who reported that their privacy had been invaded before were more likely to change their privacy settings compared to those who merely heard about others' privacy invasions. They also found that decreasing one's profile visibility through restricting access to friends was the most preferred strategy for privacy protection; however, in extreme cases (e.g., having a personal profile hacked) users also deleted their accounts.

Some of the other coping behaviors reported in the literature for online and offline contexts include *fabrication of information* (i.e. misrepresentation of information), *withholding information* (i.e. refusal to take action), *using privacy controls or searching for alternatives* (i.e. changing privacy settings, willingness to pay more or search more for better protection), and *private and public actions* (i.e. taking action to remove information, flaming, complaining to third parties) (Debatin et al. 2009; Korzaan et al. 2009; Lwin et al. 2007; Sheehan and Hoy 1999;

Son and Kim 2008; Stone et al. 1983; Wirtz et al. 2007). A list of these behaviors, including their references, study contexts, and research methods are provided in Table 3.

Table 3: The Threat Avoidance and Coping Behaviors Proposed in the Privacy Literature

Behavioral Responses	References	Method	Context
• Changing privacy settings	Debatin et al. 2009	Survey Interview	Social Networks
• Willingness to pay for privacy • Willingness to examine multiple websites for a better privacy protective option	Egelman et al. 2009	Experiment	Online Shopping
• Fabricate: Misrepresentation of personal information • Protect: Adoption of privacy protection technologies • Withhold: Refusal to purchase from (or register to) a web site	Lwin et al. 2007	Experiment	Online Shopping
	Wirtz et al. 2007	Survey	Online Shopping
• Problem-focused coping • Emotion-focused coping	Liang and Xue 2009	Theory Development	IT Threat Avoidance
• Avoidance motivation	Liang and Xue 2010	Survey	Personal Computer Users
• Adaptive response: Intention to remove (or do not post) information • Maladaptive (affective) response	Marett et al. 2011	Survey	Social Networks
• Refuse to give information • Take action to have the name removed • Refuse to purchase	Stone et al. 1983	Field Experiment	Organization
	Korzaan et al. 2009	Survey	Internet Use
	Stewart and Segars 2002	Survey	Online Shopping

Behavioral Responses	References	Method	Context
<ul style="list-style-type: none"> • Notifying ISP about unsolicited e-mail • Requesting removal from maligning list • Flaming senders of unsolicited e-mail • Providing incomplete data during registration • Providing inaccurate data during registration 	Sheehan and Hoy 1999; Sheehan 2002	Survey	Online Shopping
<ul style="list-style-type: none"> • Refusal (information provision) • Removal (private action) • Negative word-of-mouth (private action) • Complaining directly to online companies (Public action) • Complaining directly to third party organizations (Public action) 	Son and Kim 2008	Survey	Internet Use

Although these studies expand our understanding of a user's information protection and coping responses, the literature still lacks a systematic understanding of the processes by which a user copes with privacy threats in the domain of OSNs. To develop such an understanding, this study will mainly be drawing from coping theory (Folkman et al. 1986; Lazarus 1993; Lazarus 1966; Lazarus and Folkman 1984; Lazarus and Launier 1978).

2.2.2 Coping Theory

Coping theory postulates that individuals cope with disruptive situations through two key processes that constantly influence each other: *Primary Appraisal* (i.e. an individual's assessment of the expected consequences of a situation) and *Secondary (Coping) Appraisal* (i.e. a user's assessment of the options to have control over the situation). This theory has been developed and widely applied to the disruptive contexts where the expected consequences can be

detrimental. One of the focal application areas of this theory has been health-related domains, including coping with death (Park 1993), sexually transmitted diseases (Rosenthal et al. 1995), cancer (Kyngäs et al. 2001), and pain (Reid et al. 1998).

The theory has also been applied to the context of information systems. Threat avoidance theory (Liang and Xue 2009), which has been mainly derived from coping theory (Lazarus and Folkman 1984), protection motivation theory (Rogers 1975), and health belief model (Janz and Becker 1984) suggested a variance model to explicate a technology user's protection behaviors against being attacked by malicious IT. Drawing on this theory, Liang and Xue (2010) empirically investigated security protection behaviors of personal computer users. At the core of these prior studies is the argument that in case of a disruptive (or potentially risky) situation, an individual's threat appraisal triggers his coping appraisal, and in turn, his coping behaviors. The literature is, however, less clear about situations where the consequences are multifaceted, containing both types of consequences (i.e., beneficial and harmful).

While the expected consequences of an event in a security context (e.g., being attacked by a malicious IT, such as a virus) are often purely negative (e.g., data loss), the expected consequences of an event in a privacy context (e.g., disclosing information) are likely to be not only negative (e.g., privacy loss caused by disclosure), but also positive (e.g. benefits derived from/opportunities caused by disclosure). Although security studies that built upon coping theory focus on *only* technology users' avoidance behaviors (e.g., coping with malicious IT using anti-spy software), privacy studies should not ignore the multifaceted nature of privacy-related events and investigate *both* avoidance (coping) and opportunity seeking (adoption and use) behaviors. A similar perspective in the context of a significant IT event was adopted by Beaudry and Pinsonneault (2005). Coping as well as opportunity seeking behaviors by employees were

explicitly considered when a new IT system is introduced in the workplace which provides benefits but also pose challenges. This study defined coping as an employee's cognitive and behavioral efforts to adapt to a new system and suggested that an employee can categorize consequences of adoption of a new IT system as either threats or opportunities, and his behavioral responses (i.e., using the system to gain benefits vs. coping with the perceived threats caused by the new system) will be influenced by both perceptions.

2.2.3 A User's Opportunity Seeking Behaviors under Privacy Threat

A large body of research in the information privacy literature has focused on understanding a technology user's behavioral responses under privacy concerns (Li 2012; Smith et al. 2011). These behaviors have been investigated from two perspectives.

The first perspective explores the negative impact of a user's concern for privacy that emerges as a result of his information disclosure (or adoption and use of an information system) on his behavioral response. This stream of research has proposed that a user's intention to disclose personal information can be mitigated by his concern for information privacy.

Another stream of research has adopted the notion of privacy calculus suggesting a user's subjective cost-benefit assessment is the major antecedent of his behavioral responses. Such a privacy calculus perspective suggests that a user's overall assessment of the consequences he would face in return for disclosing his personal information would be salient in determining his behavioral responses. Studying the trade-off between a user's benefit (e.g., future convenience and personalization, enjoyment, socialization, monetary compensation, self-representation, and relationship maintenance) and cost (e.g., concern for privacy) perceptions, these studies suggest that if a user's expected net outcome is towards benefit (i.e., the value of positive outcomes are

larger than that of negative outcomes), he is likely to disclose his personal information and/or adopt the system. A summary of these two perspectives is provided in Table 4.

Table 4: Opportunity Seeking Behaviors in the Privacy Literature

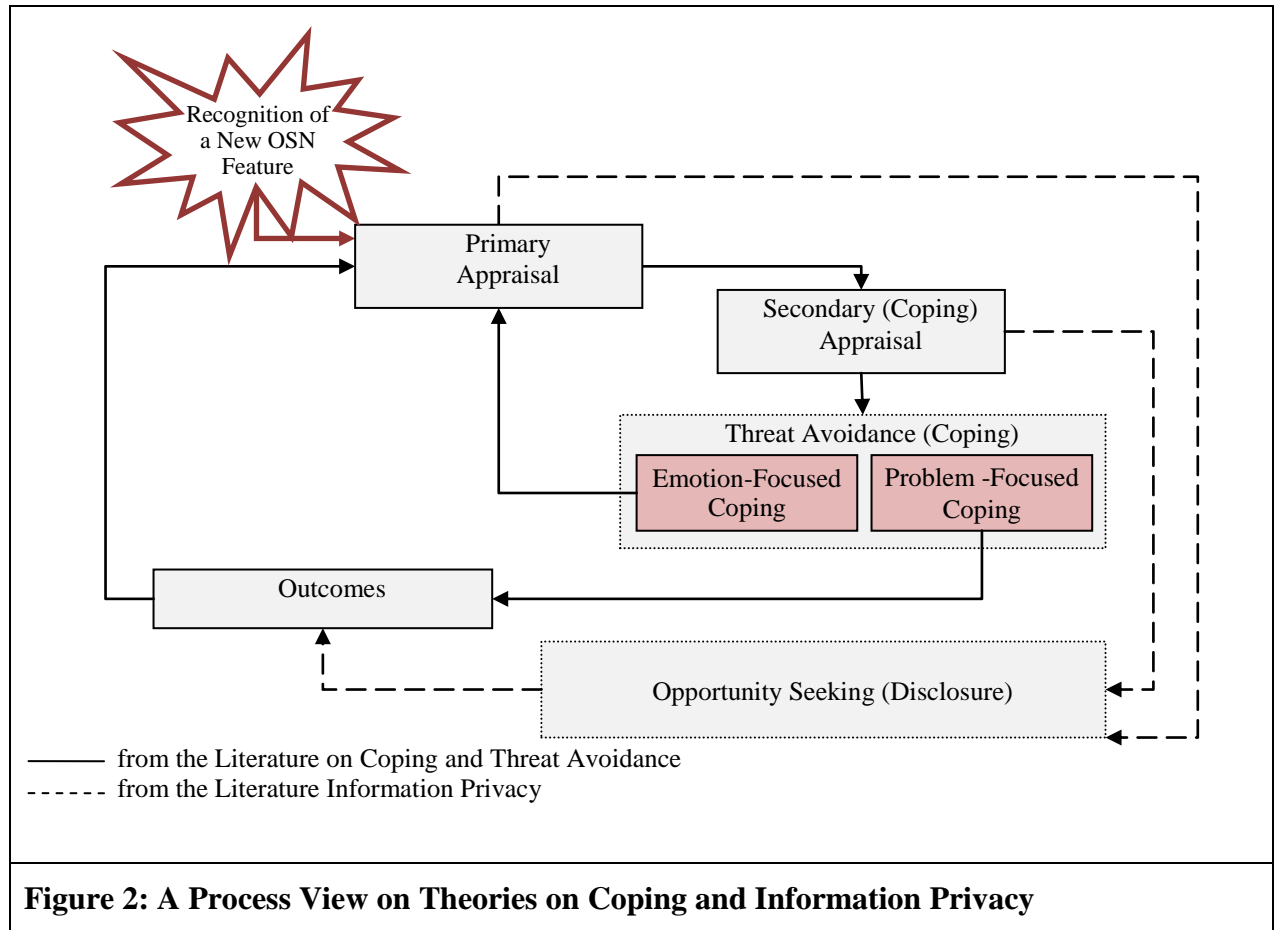
The Purpose of Disclosure	References	Perspective
To use personalized services	Awad and Krishnan 2006; Chellappa and Sin 2005	Concern for Privacy → Behavioral Response
To register for a web site	Hann et al. 2007; Sheehan and Hoy 1999	
To purchase a product	Dinev and Hart 2005; Hine and Eve 1998; Miyazaki and Fernandez 2000; Miyazaki and Fernandez 2001; Pavlou et al. 2007; Phelps et al. 2001; Van Slyke et al. 2006	
To adopt electronic health records or use web based health services	Angst and Agarwal 2009; Bansal et al. 2010	
To receive monetary rewards	Malhotra et al. 2004	
To use personalized services <i>the trade-off is between the value for online personalization and concern for privacy</i>	Chellappa and Sin 2005	Expected net outcome (Cost-Benefit Assessment) → Behavioral Response
To receive personalized services <i>the trade-off is between the monetary compensations and future convenience and concern for privacy</i>	Hann et al. 2007; Hann et al. 2002; Hui et al. 2007	
To use social networks <i>the trade-off is between the benefits of using an OSN feature (enjoyment, self-representation, relationship maintenance) and concern for privacy (perceived likelihood and damage of privacy violations)</i>	Krasnova et al. 2009; Krasnova and Veltri 2010	

The Purpose of Disclosure	References	Perspective
To use location based services <i>the trade-off is between the benefits of using a location-based service (greater connectivity, personalization, and monetary compensations) and concern for privacy</i>	Xu et al. 2009	

2.3 Theoretical Framework

This framework draws on two bodies of literatures: *1) Coping and Threat Avoidance*—research that explores how individuals cope with a broad range of threats, *2) Information Privacy*—research that explores the antecedents and behavioral outcomes of technology users’ concerns for information privacy.

Figure 2 broadly describes the proposed theory. The theory represents *a process view* of a user’s coping with privacy threats and technology use intentions. A process theory is usually probabilistic and represents the sequences among events that may affect an entity (i.e., how an event unfolds) (Abbott 1988). The solid lines in the figure depict the relationships amongst the constructs that have been adopted from the coping and threat avoidance literatures. The dashed lines in the figure represent the relationships amongst the constructs that have been adopted from the information privacy literature.



Drawing on coping theory (Lazarus 1966), technology threat avoidance theory (Liang and Xue 2009), and a coping model of user adaptation (Beaudry and Pinsonneault 2005), the framework suggests that a user's threat avoidance behaviors occur by following two key cognitive processes: (1) *Threat (Primary) Appraisal* and (2) *Coping (Secondary) Appraisal*. These processes will be explained in detail in the following sections.

2.3.1 Primary Appraisal

Primary appraisal starts with a user's recognition of a new OSN feature (or awareness of the outcomes of an OSN feature as explained in Section 2.4). In primary appraisal, a user evaluates

“*whether he has anything at stake*” in using the feature (Lazarus and Folkman 1984). Primary appraisal, thus, involves a user’s evaluation of the potential beneficial and harmful consequences of using an OSN feature and his likelihood of being affected by these outcomes. As suggested by coping theory (Lazarus and Folkman 1984), primary appraisal has to occur before coping appraisal, as a user can only be motivated to search for coping resources if he can identify and understand the significance of the benefits and privacy threats that occur as a result of his disclosure.

A disruptive event can be construed as a threat or a challenge (Lazarus and Launier 1978; Beaudry and Pinsonneault 2005; McCrae 1984), and it is the user's interpretation of the event that triggers his coping reactions. While a threat refers to expected damage that may or may not be inevitable, a challenge refers to usually positive and voluntarily selected stresses, such as having a child, starting a new job, starting a fitness program, changing religious affiliation, or embracing a new technology at workplace. Although challenges require some coping effort from the individual, they differ from threats because they are more positive in tone, are more controllable, and are often voluntarily selected.

Similarly, an OSN feature is likely to be assessed as containing both positive and negative types of consequences (Beaudry and Pinsonneault 2005; Cartwright and Cooper 1996; McCrae 1984). An OSN feature, however, is also likely to be assessed as a pure benefit: an additional category to a threat and a challenge, which are proposed by coping theory. Thus, an OSN user can appraise an OSN feature in three different ways—benefit, challenge, and privacy threat. ***Benefit*** refers to a user’s overall expectation of positive outcomes without any significant privacy threats perceived, while ***Challenge*** refers to his expectation of a positive outcome with a significant but

acceptable level of risk accompanying the benefits. ***Privacy threat*** refers to a user's expectation of negative outcomes without much significant benefits.

The relative importance of positive and negative consequences determine a user's appraisal of an OSN feature, and his motivation to search for coping resources (Lazarus and Folkman 1984).

For example, primary appraisal may start when an OSN user receives an invitation from a friend to use a social application on the platform. If the user feels that the potential negative consequences (e.g., loss of privacy) of using the feature are more significant than that of the positive ones (e.g., enjoyment of playing a social game with a friend), he would appraise the feature as a *privacy threat (i.e., significant threat without any significant benefits)*. In contrast, when perceived benefits are more significant than threats, the user would appraise the feature as a *benefit (i.e., significant benefits without any significant threats)*. When the user's perceived benefits and threats are comparable, but he still perceives the feature in a positive tone and has the intention to utilize it, then his appraisal will be a *challenge (i.e., significant benefits with significant threats)*. In such situation, the user will have to consider and cope with perceived privacy threats while utilizing the feature.

The assessment of the consequences is subjective in nature. While a user may appraise an OSN feature as a challenge, another one may appraise the same feature as a privacy threat. For example, a user who suffers from health issues may perceive significant benefits in using a medical application in an OSN, if he thinks that using the application (e.g., receiving daily reminders and suggestions from the application, interacting with other network members) can support him emotionally and help him cope with the symptoms of his illness. While the user may acknowledge the privacy threats associated with using the application — as he would have to disclose sensitive health information to gain these benefits — his overall assessment may be still

positive. Another user, in contrast, may appraise the same application as a threat if he thinks that disclosing health information would only result in harm (e.g., loss of privacy, damage to reputation, profiling and discrimination) without bringing him many benefits.

2.3.2 Secondary (Coping) Appraisal

Primary appraisal is followed by secondary appraisal (Lazarus 1966; Lazarus and Folkman 1984), as the identification of a threat would motivate the user to cope with it and minimize the anticipated harmful consequences of using an OSN feature (Lazarus 1966; Liang and Xue 2009). In secondary appraisal, a user evaluates what can be done to prevent harm and improve the prospects for benefits (Folkman et al. 1986). To do so, in this stage, the user evaluates his control over the situation considering the resources (i.e., privacy safeguards) that are available to him to cope with a privacy threat (Lazarus 1966). In the context of information privacy, *control refers to a user's ability to manage the outflow of his personal information* (Altman 1975; Dinev and Hart 2004; Hann et al. 2007), especially against the undesired consequences of disclosure, such as: secondary use of information, profiling, stalking, and embarrassment. So, while *copied resources* (i.e., privacy safeguards) are *objective* entities, a user's *secondary appraisal* (i.e., assessment of his control over the situation) is *subjective* in nature. Even when all essential privacy safeguards are provided by an OSN platform, a user's coping appraisal may still be low for a number of reasons—for example, if he is not aware of the given safeguards, or he believes that the given controls cannot effectively protect his personal information, or they are too complicated to use, or he lacks the efficacy to use them (Liang and Xue 2009).

2.3.3 Behavioral Responses

The framework posits that a user's primary and secondary appraisal affect two types of behavioral responses: *opportunity seeking (disclosure)* and *threat avoidance (coping)*.

Opportunity seeking behaviors involve an approach behavior that is triggered by a motivation to reach a positive and desirable end-state that would offer a specific advantage to the user (Liang and Xue 2009), such as: self-expression and social interactions (Ellison et al. 2007). Opportunity seeking behaviors require an *information exchange* between a user and other actors that are involved in the OSN platform—that is, *the user has to disclose* some sort of personal information to gain the advantages an OSN feature can offer. The actors can range from a user's friends to friends of friends, from groups to applications that are available on the network. For example, a user may update his profile page regularly by posting new photos and status messages to enhance his social presence and interactions with others. Similarly, a user may give access rights to a social game application, and in return, he enjoys playing a social game with other network members. Note that information disclosure can happen in different forms and can be initiated by different actors (explained in Section 2.4 in detail).

Several theories—utility maximization (Ajzen and Fishbein 1980; Awad and Krishnan 2006; Fishbein 1975), expectancy-value theory (Culnan 1993; Laufer and Wolfe 1977), expectancy theory of motivation (Stone and Stone 1990; Vroom 1964)—have explained the cognitive processes that occur before a behavioral decision is made (e.g., undertaking a behavior, choosing among alternative forms of behavior). These theories are built on the premise that an individual processes information about his behavior and its outcomes. As a result, the individual tends to

behave in ways that are expected to result in the most favorable outcomes by attempting to maximize the positively valued consequences and minimize the negatively valued ones.

Expectancy theory, for example, suggests that an individual forms expectations about the consequences of a behavior and likelihood of achieving these outcomes, and chooses between alternative behaviors according to his assessment (Vroom 1964). Exchange theories explain the nature of an exchange between two or more parties over the course of interactions and propose that an individual seeks to maximize his net gains in a given exchange and therefore tends to be involved in an exchange relationship to the extent that he expects a net gain from this relationship (Bagozzi 1982; Culnan and Bies 2003; Laufer and Wolfe 1977).

Based on the exchange and utility perspectives, prior research in the privacy literature has developed the notion of privacy calculus to explain how a user discloses his personal information in return for a higher value (Culnan 1993; Culnan and Armstrong 1999; Dinev et al. 2006; Dinev and Hart 2006; Hann et al. 2007; Hui et al. 2007; Laufer and Wolfe 1977; Milne and Gordon 1993; Xu et al. 2009). These studies have suggested that subjective cost-benefit assessment determines a user's disclosure behavior.

Similarly, the consequences of disclosure can be favorable and unfavorable in an OSN context. A recent study by Krasnova and Veltri (2010) empirically validated that a user's self-disclosure depends on his perceived net gains in an OSN platform. Based on the insight gained from the literature, it is suggested that a user's relative assessment of the expected consequences of disclosure (i.e. primary appraisal) affect his disclosure (i.e., opportunity seeking) behavior.

Privacy literature also provides insight into the relationship between a user's secondary appraisal (i.e. assessment of control over the situation) and opportunity seeking behavior. Control refers to

a user's ability to manage the outflow of his personal information and the subsequent disclosure of that information to third parties (Hann et al. 2007) and to protect himself against expected negative consequences (Altman 1975; Dinev and Hart 2004). Note that it is a user's subjective assessment of his ability to control his personal information that affects his behavioral responses. Studies in online and offline marketing literature report that a consumer's privacy concerns increase when he is not granted sufficient controls on his personal information (Culnan 1993; Dinev and Hart 2004; Malhotra et al. 2004; Phelps et al. 2000), which in turn, decreases his disclosure intentions (Milne and Rohm 2000; Phelps et al. 2001; Stewart and Segars 2002). Based on the insight gained from the literature, it is suggested that a user's subjective assessment of his control over a feature (i.e. secondary appraisal) affects his disclosure and use (i.e., opportunity seeking) behavior.

Threat avoidance (Coping) behaviors refer to a user's cognitive and behavioral efforts to protect his information privacy against specific external threats that may occur as a result of system use or disclosure. A coping behavior is triggered by an end state that is undesirable (Liang and Xue 2009), which could be taxing or exceeding the user's resources (Lazarus and Folkman 1984; Liang and Xue 2009). The emotional and psychological harm that a user may incur as a result of privacy loss can be a good example of undesirable end states that trigger a user's coping efforts. Coping theory proposes two focal types of coping strategies to deal with a privacy threat:

Problem-Focused Coping (PFC) and Emotion-Focused Coping (EFC).

Problem Focused Coping (PFC) refers to a user's deliberate cognitive and behavioral efforts which take a problem-solving approach to alter the objective reality. PFC targets the sources of the threat itself, so adoption of these strategies can effectively eliminate or reduce the threat in objective terms.

In the privacy context, a threat can be avoided through *direct* and/or *indirect* measures. *Direct measures* refer to privacy safeguards that are provided to the user. Some of the examples include opting-out from risky applications, revising privacy settings, disabling cookies on the computer, updating password regularly, adopting third party software to check privacy settings, using private browsing, and turning off location information of a mobile device. In a threat situation where direct coping measures are available to a user, he is expected to adopt them first, especially if he feels that they are sufficient and effective to eliminate a privacy threat and if he believes that he is capable of adopting these controls.

Indirect measures refer to alternative methods of coping that a user may employ when privacy safeguards are not provided to him. Prior literature suggests that *data fabrication* (i.e., misrepresentation of data by providing inaccurate or incomplete information) (Lwin et al. 2007; Son and Kim 2008; Wirtz et al. 2007) or *withholding* (i.e., limited disclosure or removal of data) (Smith et al. 1996; Son and Kim 2008) can be used as a strategy to eliminate privacy threats. Examples of withholding include terminating connections on a social network site (e.g., “unfriending” friends, unsubscribing from Fan Pages or Groups), limiting social interactions and sharing on a social network site (e.g., not using social applications on the platform, not posting pictures or status updates, removing the wall feature to prevent friends’ post on a profile page), creating fake social accounts, and so on.

Other indirect strategies include interacting with an online company (i.e., voting for Facebook’s privacy policy, posting a message on the official Facebook page) or third party organizations (i.e. TRUSTe, Privacy Commissioner of Canada) to complain or raise one’s voice (Son and Kim 2008). Employing these strategies, a user takes a problem solving approach and attempts to target the source of the threat. While these actions may not be as effective as the PFC strategies

with direct measures in eliminating a privacy threat in the short term, they can be quite influential in the long term.

Emotion-Focused Coping (EFC) refers to a user's cognitive and behavioral efforts toward creating a false perception of the environment to regulate emotional distress associated with the threat without changing the objective reality (Lazarus 1966). EFC strategies aim to adjust one's desires or importance of desires so that negative emotions related to threat (e.g., fear and stress) are mitigated (Beaudry and Pinsonneault 2005; Folkman et al. 1986; Liang and Xue 2009). Most of the EFC strategies only require cognitive efforts and are oriented towards the self. Common examples are wishful thinking (i.e., predicting a less negative outcome of a privacy risk than the actual possibilities), positive comparison (i.e., positive self-assessment compared to others), diverting attention (i.e., thinking of positive things can distract one away from the stress), denial (i.e., refusing to acknowledge the potential harmful consequences or their significance), and passive acceptance (i.e., accepting the IT event as a fact of life by changing beliefs and attitudes) (Tyre and Orlikowski 1994). A user can also be involved in behavioral acts to manage his negative emotions. For example, a user can share his negative experiences and feelings with friends or online communities (e.g., negative word of mouth; Son and Kim 2008)

2.3.4 Selection of a Coping Strategy

Based on the theories of expectancy (Vroom 1964) and rational choice (Paternoster and Pogarsky 2009), an individual evaluates different coping options that are available to him and tends to choose the one that can bring him the most valued outcome. In privacy contexts, similarly, a user is expected to value the option that is most likely to reduce the threat and

promote beneficial outcomes, and least likely to reduce the benefits that the feature can offer. When the coping option is identified, the user employs his coping strategy.

PFC mainly occurs when a user feels that the threat is avoidable (through adoption of privacy safeguards) and he has control over the situation (Folkman et al. 1986; Lazarus and Folkman 1984) with an objective to eliminate or alleviate the threat. A user may feel that adopting a PFC strategy (e.g., a direct coping strategy such as changing privacy settings) *sufficiently* eliminates the threat. In this situation, as the user would not need to deal with his emotions, he would be less likely to involve himself in an EFC strategy (to complement his PFC strategy). However, social technologies, as well as their affordances, procedures, and policies, are constantly in a state of flux, producing novel privacy issues. Users often do not feel that adopting a safeguard completely eliminates the privacy threat. As a result, they mutually employ both types of strategies (Beaudry and Pinsonneault 2005; Liang and Xue 2009).

EFC mainly occurs when a user feels that the privacy threat is not avoidable (due to insufficient, ineffective, or lack of safeguards) or he does not have control over the situation (Folkman et al. 1986; Lazarus and Folkman 1984). The objective is to reduce a user's negative emotions (e.g., fear of privacy loss, worry about consequences) and maintain his psychological well-being (Beaudry and Pinsonneault 2005; Folkman et al. 1986; Lazarus and Folkman 1984). Compared to a situation where PFC is insufficient or ineffective, or does not exist, EFC would be activated less in a situation where privacy safeguards are available and EFC is mutually used to serve with PFC.

In summary, it is suggested that a high threat situation elicits both PFC and EFC (Lazarus and Folkman 1984; McCrae 1984; Rippetoe and Rogers 1987). A user's motivation to be involved in

one (or both) of these coping strategies, as well as the extent of his motivation, depends on the environmental conditions the user perceives. In a situation where a user perceives that a privacy threat is avoidable by taking safeguarding measures, he will be more likely to employ PFC strategies, whereas when he perceives that the threat is not avoidable, he will be more likely to employ EFC strategies (Folkman et al. 1986; Lazarus and Folkman 1984).

2.3.5 Impact on Outcomes and Reassessment

At this final stage, the user evaluates how his behaviors impacted the overall situation and whether the consequences he observed are aligned with the ones that he anticipated in the initial primary appraisal stage. During reassessment (i.e., subsequent primary appraisal stages), the user subjectively evaluates the extent to which his decisions regarding disclosure and coping were satisfactory or not. Note that, while a user's PFC and opportunity seeking behaviors affect outcomes (i.e., change objective reality), EFC behavior cannot. For PFC and opportunity seeking behaviors, it is a user's observation of the changes in outcomes that triggers his reassessment. Thus, the links from PFC and opportunity seeking to primary appraisal are indirect, connected via outcomes, as depicted in Figure 2. However, the link from EFC to primary appraisal is a direct one, as changes in a user's beliefs, values, emotions, and goals may directly trigger his reassessment, without affecting the outcomes.

Coping theory (Lazarus and Folkman 1984) suggests that the relationship between a user's cognitive appraisal (i.e., primary and secondary) and his behavioral responses (i.e., use and coping) are highly dynamic and iterative. As depicted in Figure 2, these processes constantly influence each other and evolve over time. Although a user's expectations and behaviors can reach equilibrium after a few iterations at one point in time, shifts in the process are still

expected. The shift in a user's judgment may be based on various aspects of his experience with the system being used. Most common causes are the changes in the individual (e.g., changes in a person's goals, values, and expectations), social context (i.e., changes in the expectations of and pressures from the social environment), and technology (e.g., changes in technology affordances) (Beaudry and Pinsonneault 2005; Lazarus 1966; Liang and Xue 2009).

For example, a user may eliminate a privacy threat associated with using an OSN feature by revising his privacy settings. Nevertheless, he can still evaluate the outcomes of a feature used unfavorably if he realizes that his coping strategy also eliminated or reduced the favorable outcomes he had thought to achieve, or that it created conflicts with his social context or his primary values and goals (Folkman et al. 1986). Alternatively, although a user cannot find a way to eliminate a privacy threat caused by using an OSN feature, he can still evaluate the outcome favorably after his user experience if, for example, the user observes unanticipated positive outcomes, which compensate for his privacy concerns.

As another example, a user may opt in to fabricate his profile information (e.g., name and picture) on Facebook to prevent disclosure of his private information to other network members through the "friend suggestions" feature that is available on Facebook. He may initially think that the privacy threat has been resolved by fabricating his personal information and thereby appraise his action as successful. However, after a while, he may realize that while he prevented the threat (e.g., disclosure of his information to unwanted people), as a result of his coping act, he also prevented some favorable outcomes of using the network he enjoyed (e.g., real friends cannot search and friend him because of the fabricated information). As a result of this observation of the actual outcomes, he then reconsiders what is at stake for him in the given situation.

2.4 Different Cases of Information Disclosure

Information disclosure can happen in different forms and can be initiated by different actors in an OSN platform. As depicted in Table 5, information disclosure can be initiated by two different actors: *an OSN user* and *other actors* who are involved in the OSN platform.

Information disclosure that is initiated by the user may be either *intended* or *unintended*.

The term “*intended*” is used to refer to whether the actor who initiated information disclosure is aware (conscious) of his action or not. So, when disclosure is intended, the actor who initiated the disclosure is fully aware of his action. A user’s disclose of a piece of personal information on his profile page can be an example of *intended disclosure initiated by the user*. While the initial information disclosure may be intended by the user, this act may have unintended consequences, resulting in further information disclosure, which the user may not foresee at the time of initial disclosure. In other words, the user may be fully conscious of his initial action (intended), but not so of the subsequent disclosure that he initiated (unintended disclosure initiated by the user). It is important to highlight that both intended and unintended disclosures may result in positive and negative outcomes. An unintended disclosure does not have to refer to an undesirable event. A user’s observation of the consequences of an unintended disclosure initiates his primary appraisal, and in the primary stage, the user decides whether it is beneficial or harmful to him. For example, a user’s friend can post and tag a photo of the user on his profile page and disclose it not only to his friends but friends of the user. This type of disclosure is not intended by the user (i.e., unintended disclosure initiated by others). Depending on his primary appraisal, the user may perceive this disclosure as a benefit or a threat to his privacy. The similarities and differences among different disclosure situations are compared and described in-depth with several examples in Table 5.

Whether the disclosure is intentional or unintentional may also cause differences in a user's behavioral responses (i.e., opportunity seeking and coping). Section 2.5 describes the processes that shape a user's behavioral responses when disclosure is intended or unintended by the user. While Figure 3 and Figure 4 depict the processes for intended and unintended disclosure respectively, Table 6 presents a brief summary.

Table 5: Different Forms of Disclosure

	Intended Disclosure Initiated by A User	Unintended Disclosure Initiated by A User	Unintended Disclosure Initiated by Others
Initiation of Disclosure	Disclosure is initiated <u>by the user</u> .	Disclosure is initiated <u>by the user</u> .	Disclosure is initiated <u>by an actor that is different from the user</u> .
Intention of disclosure	<ul style="list-style-type: none"> • Disclosure is <u>intended</u> by the user. 	<ul style="list-style-type: none"> • Disclosure is <u>not intended</u> by the user. 	<ul style="list-style-type: none"> • Disclosure is <u>not intended</u> by the user. • Disclosure is often <u>intended</u> by the actor who discloses the information.
Goal of Disclosure	<ul style="list-style-type: none"> • The user discloses with a specific purpose or to gain a specific benefit. 	<ul style="list-style-type: none"> • The user does not have a specific purpose as it is unintended. The user may not aware of the disclosure until he observes the consequences. 	<ul style="list-style-type: none"> • The other actor discloses with a specific purpose or to gain a specific benefit. • The user does not have a specific purpose as it is unintended. The user may not be aware of the disclosure until he observes the consequences.
Method of disclosure	<p><u>Direct Disclosure:</u></p> <ul style="list-style-type: none"> • <u>By using</u> an OSN feature, the user intentionally discloses <i>new personal information</i> to others. • Information is given to those who already have access to the user's profile (e.g., friends, followers who are already authorized). (See <i>Example 1 below</i>) <p><u>Indirect Disclosure:</u></p> <ul style="list-style-type: none"> • <u>To use an OSN feature</u>, the user 	<ul style="list-style-type: none"> • <u>As a result of using</u> an OSN feature, the user ends up giving new permissions to others to access or use his personal information that is already available on the network. • The user initially uses the OSN feature with a specific purpose in mind. However, this intentional act results in unintended consequences. • Permissions are given to those <i>who do not already have access</i> to his 	<ul style="list-style-type: none"> • <u>By using</u> an OSN feature, an actor, other than the user (e.g., friends, platform owners), who has access to the user's personal information (i.e., new or already available) discloses it on the network. (See <i>Examples 5, 6, and 7</i>)

	Intended Disclosure Initiated by A User	Unintended Disclosure Initiated by A User	Unintended Disclosure Initiated by Others
	<p>intentionally gives <i>new permissions</i> to others to access and use his personal information that is already available on the network.</p> <ul style="list-style-type: none"> •Permissions are given to those <i>who do not already have access</i> to the user's profile (e.g., friends of friends, applications, groups who are not already authorized). <p>(See <i>Example 2</i>)</p>	<p>information (e.g., friends of friends, applications, groups who are not already authorized).</p> <p>(See <i>Examples 3 and 4</i>)</p>	
Primary Appraisal	<p>Primary appraisal starts with the user's recognition of the OSN feature. The user can only assess the <i>expected consequences</i> of using the feature.</p>	<p>Primary appraisal starts with the user's awareness of the unintended disclosure or its consequences. At the time the user gains awareness of the disclosure, it has already occurred. So the user can assess both the <i>actual and expected (future) consequences</i> of disclosure.</p>	<p>Primary appraisal starts with the user's awareness of the unintended disclosure or its consequences. At the time the user gains awareness of the disclosure, it has already occurred. So the user can assess the <i>actual and expected (future) consequences</i> of disclosure.</p>
Coping	<ul style="list-style-type: none"> •Primary appraisal starts with <u>a user's recognition of an OSN feature</u>. •The user is at the locus of the decision process. He has the option not to use the OSN feature. So, privacy threat may never occur. •Thus, <i>coping is proactive</i>. The user can avoid a threat without it even occurring. 	<ul style="list-style-type: none"> •Primary appraisal starts with <u>a user's observation of the consequences of an OSN feature</u> that is previously initiated by him. Initial adoption of the feature is intended by the user, but the subsequent outcomes are unintended. •The user already faces the consequences of his unintentional disclosure (i.e., can be either positive or negative for him). If 	<ul style="list-style-type: none"> •Primary appraisal starts with <u>a user's observation of the consequences of an OSN feature</u> that is already <u>initiated by others</u>. Others' action is often intended (by them), but the subsequent outcomes are unintended for the user. •The user already faces the consequences of his unintentional disclosure (i.e., can be either positive or negative for him). If

	Intended Disclosure Initiated by A User	Unintended Disclosure Initiated by A User	Unintended Disclosure Initiated by Others
		<p>consequences are appraised as a threat, then the user has to cope with it.</p> <ul style="list-style-type: none"> • Thus, <i>coping is reactive</i>. The user has to cope with a threat that has already occurred. 	<p>consequences are appraised as a threat, then the user has to cope with it.</p> <ul style="list-style-type: none"> • Thus, <i>coping is reactive</i>. The user has to cope with a threat that has already occurred.
Examples	<p><u>Example 1:</u> The user posts his photos on his profile page by using the “photo upload” feature. This information is disclosed to his friends on the network. The user is fully aware of his action and disclosure is fully intended. In return for his disclosure, the user expects to enhance his social presence on the network and interactions with his friends. His friends can now see the new pictures and post comments on the pictures.</p> <p><u>Example 2:</u> The user allows an application the permission it requests to access and utilize his personal information. The user is fully aware of his action and disclosure is fully intended. In return for his permission, the user expects to gain advantages of using the application and interact with the other network members who use</p>	<p><u>Example 3:</u> The user joins a group page to read the comments posted by the group members. After receiving a few “friendship” requests from the group members, the user realizes that group members can add him as a “friend” even though his profile is normally secured for new friendship requests (i.e., no one can add him by searching his name). He understands that his act of joining a group gave all group members the right to add him as a friend.</p> <p><u>Example 4:</u> The user posts a comment on a friend’s profile page. He thinks that his comment is only visible on his friend’s profile page, and only his friend and his friend’s friends can see his comment. However, after a while, he realizes that his friend’s profile page is open to everyone, so the comment he posted is also visible to</p>	<p><u>Example 5:</u> A friend shares a photo of the user on his profile page by using the “photo upload” feature. He also “tags” the name of the user on the photo so that the user can see the posted photo. In this case, the purpose of the user’s friend may be to share the photo with the user on the platform, so his action is intentional. The user may or may not like that his information has been disclosed on the platform and seen by his other friends.</p> <p><u>Example 6:</u> An OSN platform (e.g., Facebook) discloses its users’ public information (e.g., name, profile picture, gender, networks) to other Facebook users through “people you may know” application. In return for this disclosure, Facebook expects to increase the number of friendship connections on the network and enhance overall use and popularity of</p>

	Intended Disclosure Initiated by A User	Unintended Disclosure Initiated by A User	Unintended Disclosure Initiated by Others
	the same application.	everyone.	<p>the platform. The user is never directly informed about this disclosure. However, the user may realize that Facebook discloses other users' information (e.g., his distant friends from college) to him as his potential friends and suggest him to "friend" these people. Deducing from this information, he can conclude that his information should also be disclosed to them.</p> <p><u>Example 7:</u> The user posts a photo on his profile page. Then, a friend of him posts a comment on the photo and the photo becomes available on the friend's profile page. The purpose of the user's friend may be sharing his opinion about the photo and increasing his social interactions with others on the platform. His action is intentional. However, as a result of this action, the friends of the user's friend also gain access to the photo. The user may or may not be aware of that. If he is aware, he may or may not like that his information has been disclosed to friends of his friend.</p>

2.5 Detailed Frameworks for Intended and Unintended Disclosure

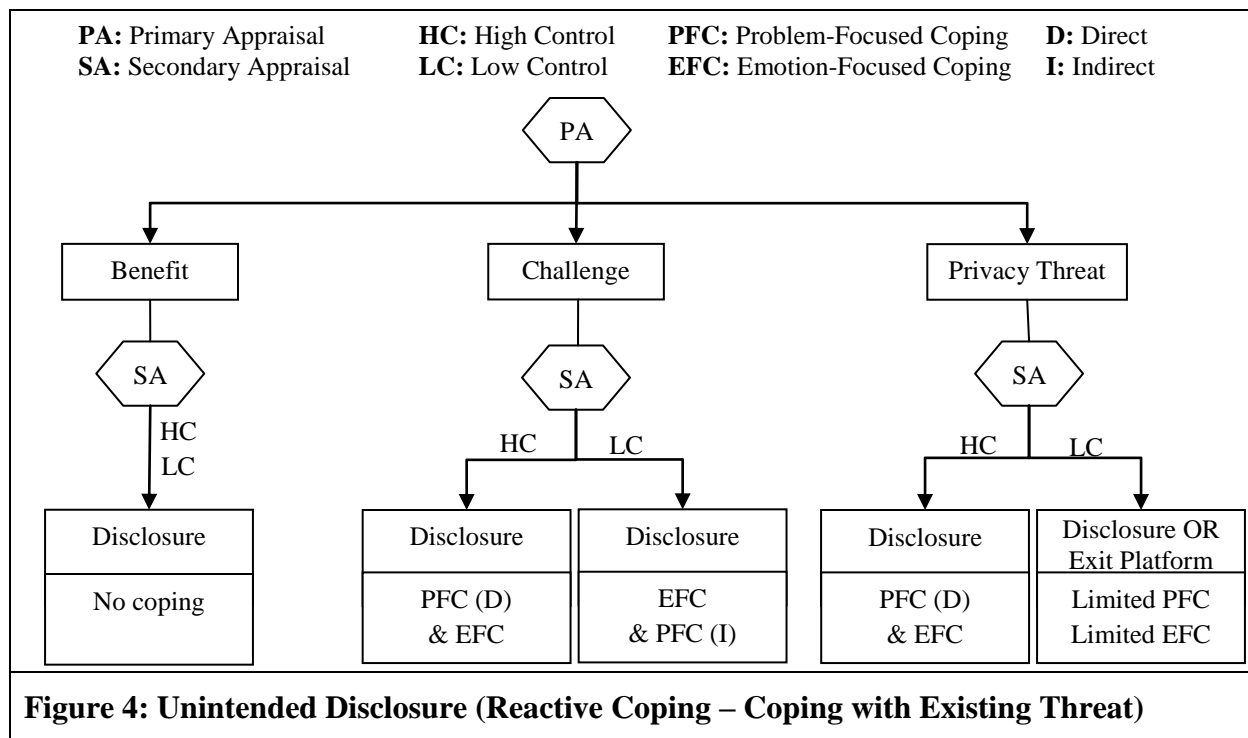
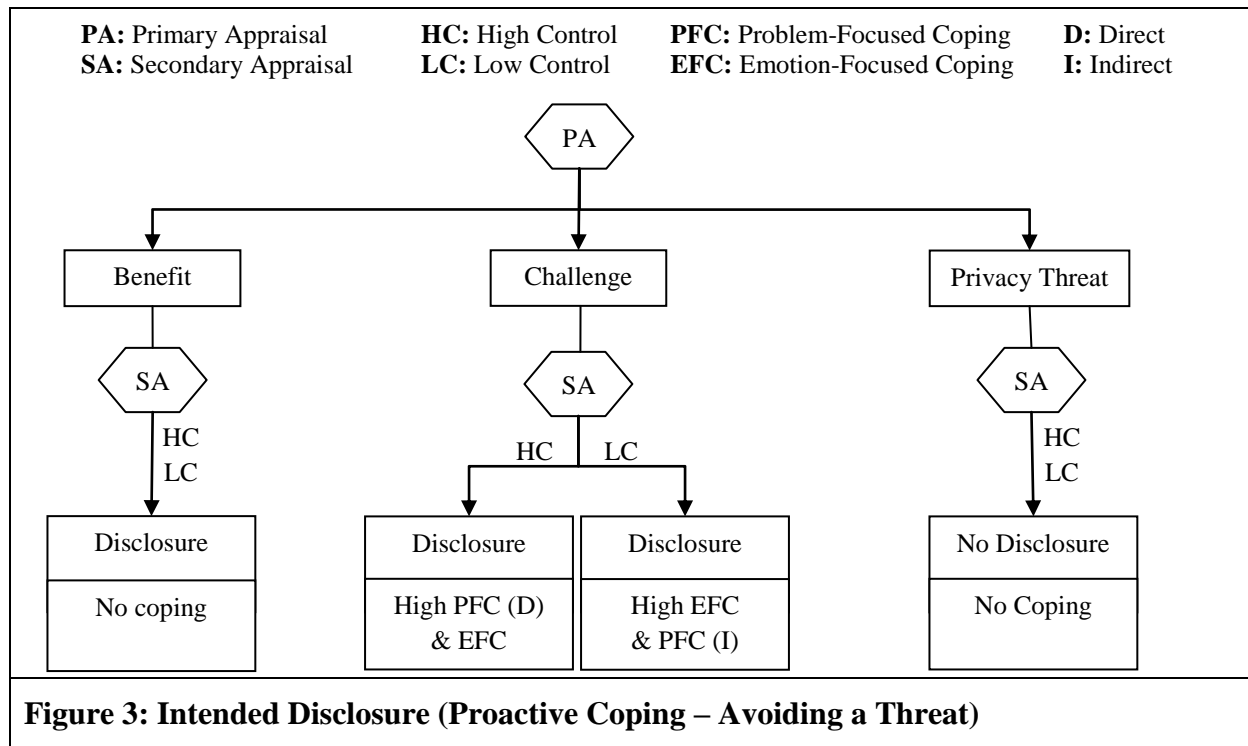


Table 6: Summary of a User's Opportunity Seeking and Threat Avoidance Behaviors

		Secondary (Coping) Appraisal			
		Intended Disclosure		Unintended Disclosure	
		High Control	Low Control	High Control	Low Control
Primary Appraisal	Benefit <i>(benefit with no significant privacy threats)</i>	<ul style="list-style-type: none"> • Intended Disclosure • No Coping 	<ul style="list-style-type: none"> • Intended Disclosure • No Coping 	<ul style="list-style-type: none"> • Unintended Disclosure • No Coping 	<ul style="list-style-type: none"> • Unintended Disclosure • No Coping
	Challenge <i>(benefit with significant privacy threat, Benefit > Threat)</i>	<ul style="list-style-type: none"> • Intended Disclosure • High PFC (direct) • EFC 	<ul style="list-style-type: none"> • Intended Disclosure • PFC (indirect) • High EFC 	<ul style="list-style-type: none"> • Unintended Disclosure • PFC (direct) • EFC 	<ul style="list-style-type: none"> • Unintended Disclosure • PFC (indirect) • EFC
	Privacy Threat <i>(Privacy threat with no significant benefits)</i>	<ul style="list-style-type: none"> • No Disclosure, thus: • No Coping 	<ul style="list-style-type: none"> • No Disclosure, thus: • No Coping 	<ul style="list-style-type: none"> • Unintended Disclosure • PFC (direct) • EFC 	<ul style="list-style-type: none"> • Unintended Disclosure • Limited PFC (indirect) • Limited EFC • OR Exit Platform

2.5.1 Intended Disclosure

Figure 3 depicts the processes for an OSN user's opportunity seeking and coping behaviors in an intended disclosure situation. An intended disclosure is initiated by a user with a specific purpose (i.e., gaining a specific benefit). The user has the option to not use the OSN feature, so a privacy threat may never occur. In such a case, coping would be proactive and the user can avoid the privacy threat by simply not using the feature.

In an intended disclosure situation, primary appraisal starts with the user's recognition of an OSN feature. As the user cannot experience the actual consequences of using the feature before he initiates the process, he can only assess the *expected consequences* of using the feature. A user may appraise the expected consequences of an intended disclosure in three different ways: benefit, challenge, and threat.

In an instance where a user appraises an OSN feature as a *benefit* (i.e., *expected consequences of using the feature are associated with significant benefits without significant privacy threats*), he would adopt the feature (i.e., disclose his personal information by using the feature) without considering his control over the situation. As the user would not feel any significant privacy threats in disclosing his personal information, he would not have any coping motivations. Rather, he would orient his efforts towards utilizing the feature to the fullest extent. As indicated in the information privacy literature (i.e., privacy calculus), the extent of a user's expected net benefits would directly determine the strength of his intention to use the feature.

In an instance where a user appraises an OSN feature as a *challenge* (i.e., *expected consequences of using the feature are associated with significant benefits and significant privacy threats*), he would consider adopting the feature, but at the same time, he would search for the resources (i.e.,

privacy safeguards) that he could use to alleviate the privacy threat associated with using the feature and maximizing his net benefits. Depending on his secondary appraisal, the user may adopt different strategies to cope with the privacy threat.

If the user feels that his *control over the situation is high*, he would take full advantage of the opportunity by fully using the feature, while minimizing risks objectively with direct PFC strategies (e.g., adoption of privacy safeguards) and maximizing emotional stability with EFC strategies (e.g. wishful thinking). In such a situation, PFC is employed as the main coping strategy and EFC is used as a complementary strategy.

If, however, the user feels that his *control over the situation is limited*, he would still try to maximize his net benefits to the greatest extent, while maximizing his emotional stability with EFC strategies (e.g., denial of risks) and minimizing risks objectively with indirect PFC coping strategies (e.g. withholding or fabricating personal information). In such a situation, EFC may be employed as the main coping strategy, especially if indirect PFC strategies are insufficient in alleviating the privacy threat.

When high control and low control situations are compared in terms of a user's intentions to adopt an OSN feature and motivations to cope with a threat, it is posited that a user would have stronger intentions to use the feature and higher motivations to employ PFC when *his control over the situation is high*. In contrast, he would have weaker intentions to use the feature and higher motivations to employ EFC when his *control over the situation is limited*.

In the instance where a user appraises an OSN feature as a ***privacy threat*** (i.e., *expected consequences of using the feature are associated with significant privacy threats without significant benefits*), he would not adopt the feature and therefore, would not need to cope. Note

that by employing coping strategies (e.g., revising privacy settings) that can effectively eliminate the privacy threats associated with using the feature, a user can eventually categorize it as a benefit. This framework, however, only describes time that the user's thought process reaches equilibrium.

2.5.2 Unintended Disclosure (initiated by the user or others)

Figure 4 depicts the processes for an OSN user's opportunity seeking and coping behaviors in an unintended disclosure situation. An unintended disclosure may be initiated by the user or others who have access to the network. At the time the user gains awareness of the disclosure, it has already been initiated, so a user's primary and secondary appraisals only affect his coping behaviors (no effect on his opportunity seeking behaviors). As a result of an unintended disclosure situation, the user faces the actual consequences of information disclosure. These consequences can be appraised as a benefit or a privacy threat. If the consequences are appraised as a threat, then the user has to cope with it. Thus, the user's coping would be reactive.

In an unintended disclosure case, primary appraisal starts with a user's observation of the unintended disclosure and its consequences. As disclosure has already occurred, he can assess both the *actual and expected (future) consequences* of it. As a result, he may appraise the consequences in three different ways: benefit, challenge, and privacy threat.

In an instance where a user appraises the consequences of disclosure as a benefit, he would enjoy the benefits of disclosure without searching for coping resources. In an instance where a user appraises an OSN feature as a challenge, he would enjoy the benefits of disclosure, but at the same time search for coping resources. Similar to an intended disclosure situation, if the user feels that his *control over the situation is high*, he would be motivated to employ direct PFC

strategies to minimize risks objectively and EFC strategies to maximize his emotional stability. If the user feels that his *control over the situation is limited*, he would maximize his emotional stability with EFC strategies and minimize risks with indirect PFC strategies. Note that a user would have less control over the situation in an unintended disclosure situation compared to an intended disclosure situation. Thus, his options to cope with a privacy threat would be more limited. As an example of a PFC strategy, the user may “untag” his name from a photo that has been posted by his friend (see example 5 in Table 5). While the user may like to have access to the photo himself, he may be concerned that his friends gained access to the photo. Untagging his name from the photo would remove his friends’ access to the photo. However, since the photo has been posted without his consent and has already been published on his profile page before he untagged his name, his friends could have already seen the photo. Considering that, the user would also engage in EFC strategies (e.g., *wishful thinking* – “I immediately untagged my name so I do not think that anyone could have seen this photo in such a short time”, *positive light* – “At least I managed to untag my name quickly. Worse things could have happened.”) Also note that, even if the user untags his name and makes the photo unavailable to his friends, the photo is still available in his friends’ profile page, so it is still available to friends of his friend. If the user is concerned about it, he could ask his friend to remove the photo (e.g., withholding). As an example of a PFC strategy that can be employed in such situations, the user may “fabricate” his profile information (e.g., post an unreal profile picture, put a fake surname etc.) so that incorrect information is disclosed to his potential friends (see example 6 in Table 5). To complement this strategy, he may also employ some EFC strategies (e.g., wishful thinking – “I don’t think anyone could understand that this account belongs to me.”)

In the instance where a user appraises an unintended disclosure as a threat, the user is likely to feel that his control over the situation is rather low. If the user feels that the consequences of disclosure are not too threatening because he has some level of control in order to alter the situation, employing limited PFC strategies and/or limited EFC strategies would be helpful. However, if the user feels that the consequences of disclosure are threatening because he does not have any control to change the situation, his coping motivations would drop because fear of threat drives a user's coping motivations to a certain level. However, after reaching a certain level, the user may become insensitive to the threat (Liang and Xue 2009). Over-relying on coping in such situations may lead to frustration and stress (Beaudry and Pinsonneault 2005; Begley 1998; Folkman et al. 1986).

Coping theory also indicates that, in extreme cases where an individual appraises a threat that is too significant or overwhelming, he may totally withdraw from the situation (Beaudry and Pinsonneault 2005; Begley 1998; Lazarus and Folkman 1984). In an extreme case of an unintended disclosure situation where a user feels that the consequences of disclosure is too threatening, that he lacks any resources to alter the situation, and that his adjustments (i.e., coping) are insufficient to restore his emotional stability, he may emotionally disengage himself from the situation and exit the social network platform altogether (Beaudry and Pinsonneault 2005; Begley 1998). A recent study that investigates an OSN context, for example, found that in extreme cases (e.g., having a personal profile hacked) users preferred to delete their accounts. Similarly, a survey indicates that sixty percent of respondents considered quitting Facebook (i.e., deleting or inactivating an account) due to their privacy fears (Poll 2010). Note that, while this strategy would be successful in eliminating a particular privacy threat, it would also require significant efforts to emotionally disengage a user from the situation due to other significant

benefits of using the service. In fact, there are services that help technology users with this disengagement. For example, an online site (i.e., quitfacebookday.com) has been developed to inform users about Facebook's lack of respect for private information, enhance community support, and encourage site visitors to quit the platform.

2.6 Concluding Remarks and Connections to the Empirical Studies

In this chapter, a theoretical framework was proposed to explain how an OSN user copes with a privacy threat in different disclosure situations. The proposed framework draws upon two major literatures on coping (Lazarus 1966; Lazarus and Folkman 1984) and information privacy. The framework contributes to the literature by: 1) proposing a comprehensive framework integrating two distinct literatures on coping and information privacy and, 2) discussing how the multifaceted consequences (i.e., benefits and harms) of using an OSN feature affects a user's behavioral responses, and 3) explaining how the differences in use and information disclosure situations affect a user's behavioral responses.

The discussions presented in this chapter provide a theoretical base for the empirical studies conducted in this thesis (Study #2 and Study #3). Study #2 investigates how a user's primary appraisal and secondary appraisal affect his coping motivations. Study #3 investigates how the two conditions (i.e., the extent of permissions requested and privacy controls provided by an application) affect a user's privacy threat perception, and in turn, his intention to use an application.

Drawing on coping theory, the framework proposed in this chapter was process oriented, focusing on an unfolding process of events. However, the theoretical frameworks proposed in

Study#2 and Study#3 are variance theories, focusing on a user's perceptions and behavioral responses at a stable point in time. The integration of process and variance views of threat avoidance has been undertaken by Liang and Xue (2009) in technology threat avoidance theory. Their work first outlines the process view of the dynamic coping process and then suggests a variance view to identify the key factors and describe their relationships. Similarly, this thesis proposes two variance-based frameworks as the cross-sectional snapshots of the described process and tests them with quantitative research methods using cross-sectional data.

The two empirical studies in this thesis focus on understanding behavioral intentions in a situation where *use of an OSN feature (and disclosure of personal information) is intended and initiated by a user (i.e., use of OSN applications)*. In addition, these studies are designed in a way that the *given feature is likely to be categorized as a challenge* by the study respondents (i.e., likely to be perceived as highly beneficial and harmful at the same time by study respondents). Empirical investigations are conducted by utilizing scenario-based methods. The selected method provides the ability to create a situational context that would generate high benefit and privacy threat perceptions. To study the particular context of intended use, social applications that run on Facebook platform have been selected. To study the specified contexts, several hypothetical scenarios on Facebook applications are developed. After several rounds of pilot tests, four scenarios that generated the highest benefits and privacy threat perceptions on average are selected. The theoretical frameworks proposed by the empirical studies are empirically tested based on the data collected from a representative Facebook population.

The following two chapters (Chapter 3 and Chapter 4) present the empirical studies that build upon the proposed theoretical framework.

3 The Role of Primary and Secondary Appraisal in a User's Coping Motivations: An Empirical Study on Facebook Applications (Study #2)

3.1 Overview

This study focuses on understanding the factors that affect a user's motivation to cope with a privacy threat associated with *using an OSN application* (i.e. Facebook applications): a use situation where *information disclosure is intended and initiated by the user*. The study, in particular, proposes a theoretical model to explain how an OSN user's *primary appraisal* (i.e. assessment of beneficial and harmful consequences of using an OSN application) and *secondary appraisal* (i.e. assessment of his control over the use of an OSN application) affect his *problem-focused coping (PFC)* and *emotion-focused coping (EFC)* motivations, and empirically tests it with the data collected from 197 Facebook users using a scenario-based online survey.

The proposed theoretical model in this study is largely drawn from Coping Theory (Folkman et al. 1986; Lazarus 1966; Lazarus and Folkman 1984), Technology Threat Avoidance Theory (Liang and Xue 2009), and the privacy literature. Technology Threat Avoidance Theory (TTAT) was developed to explain the factors that affect an individual IT user's threat avoidance behaviors against malicious IT (Liang and Xue 2009). Drawing mainly on Coping Theory (Folkman et al. 1986; Lazarus and Folkman 1984) and Protection Motivation Theory (Rogers 1975), Liang and Xue (2009) conceptualized TTAT as both a *process theory* (to provide a dynamic view of the overall avoidance process) and a *variance theory* (to identify the key factors of this process and describe their relationships). Adopting these theories as a lens to investigate

an OSN user's coping responses, this study makes the following contributions to the existing body of research on information privacy and coping.

First, TTAT (Liang and Xue 2009) has been developed to explain security behaviors, focusing on how individual IT users avoid the threats caused by malicious IT. The theory posits that a user's threat appraisal determines his threat avoidance motivations. The context of privacy, however, is different from that of security for which TTAT was developed, as the adoption of an OSN feature may result in both beneficial and harmful consequences. Therefore, it is expected that an OSN user considers both types of consequences associated with using an OSN feature during the coping process. A study on IT adaptation in the workplace has taken a similar perspective (Beaudry and Pinsonneault 2005), suggesting that the consequences of adapting to a new IT in a workplace may be both beneficial and harmful to employees. Thus, the current study provides a more appropriate view of coping in the information privacy domain by considering the effects of both benefits and privacy threats associated with using an OSN feature on a user's coping motivations.

Second, although Liang and Xue (2009) proposed a variance model to serve as the method for an empirical analysis with quantitative methods, they have not tested it. As a novel contribution, this study operationalizes the proposed constructs, empirically validates their measurement items, and tests the proposed relationships using the data collected from a representative Facebook population via a scenario-based online survey.

This study also extends a study by Liang and Xue (2010), which adopts the TTAT framework and empirically investigates the link between personal computer users' threat perceptions and threat avoidance motivations. First, this study operationalizes two types of coping behaviors (i.e.,

PFC and EFC) rather than presenting them at a high level variable (i.e., avoidance motivations). Second, while TTAT suggests threat avoidability as a mediator variable between users' coping appraisal and coping motivations, Liang and Xue (2010) have not included it in their empirical analysis but suggested that it should be included in future works. This study includes threat avoidability as a mediator in the proposed model, develops the appropriate measures for the construct, and examines its effect on coping motivations.

Lastly, the data analysed for this study is collected from a representative sample of the Facebook population using a stratified random sampling method, which helps enhance the generalizability of the findings of this study.

3.2 Theoretical Framework

Coping theory describes how an individual copes with a disruptive event (Folkman et al. 1986; Lazarus 1966; Lazarus and Folkman 1984). It postulates that an individual's coping motivations are formed as a result of two processes, primary and secondary appraisal, that continuously influence each other (Lazarus 1966; Lazarus and Folkman 1984).

At the *primary appraisal* stage, a user evaluates the nature of the potential consequences of an event (i.e., benefit or harm) and his likelihood of facing these consequences. Most events can be multifaceted, resulting in two types of consequences (Lazarus and Folkman 1984). The user also questions the personal significance of these consequences and their likelihood of occurrence at this stage (Folkman et al. 1986).

At the *secondary appraisal* stage, a user first evaluates the resources that are available to him to cope with a threat. The key factor that influences this stage is a user's perception of how much

control he may have to alter the situation (Lazarus and Folkman 1984). The user may be given the essential coping resources (i.e., privacy safeguards); however, he may still feel that his control over the situation is low for various reasons (i.e., lack of efficacy to use the given safeguards). Therefore, it is a user's perceived control that determines his coping appraisal.

After primary and secondary appraisals, at the coping stage, a user employs different types of strategies to address the harmful consequences of the event. He may rely on two types of coping strategies – *problem-focused coping (PFC)* and *emotion-focused coping (EFC)* – to deal with the situation (Folkman et al. 1986; Lazarus and Folkman 1984). While PFC aims to solve the problematic situation directly through objective measures (i.e., safeguards), EFC aims to change one's perception of the problematic situation to manage his emotions and stress through a cognitive process, without actually altering the objective reality. While PFC can be oriented towards changing the environment (e.g., revising privacy settings, opting out from a service) or changing one's self (e.g., gaining awareness of privacy controls available on an OSN) (Beaudry and Pinsonneault 2005; Lazarus and Folkman 1984), EFC can only be oriented towards changing one's perceptions (e.g., wishful thinking, denial, positive comparison) (Lazarus and Folkman 1984 Folkman et al. 1986).

3.3 Research Model and Hypotheses

Drawing on TTAT (Liang and Xue 2009), the proposed model posits that a user's primary and secondary appraisals affect his two types of coping behaviors—PFC and EFC. Perceived effectiveness of privacy safeguards that are available to a user, cost of using these safeguards, and self-efficacy influence a user's threat avoidability perceptions, and in turn, his coping motivations. While perceived severity and perceived susceptibility of a privacy threat influence

his overall privacy threat perceptions, perceived likelihood and importance of benefits influence his overall benefit perceptions. Lastly, perceived privacy threat moderates the relationship between threat avoidability and coping motivations, in the sense that when perceived threat is high, the impact of threat avoidability on coping is not significant, whereas when perceived threat is low, its impact will be significant. Figure 5 presents the theoretical model proposed in this study, while Table 7 presents the definitions and sources of key constructs. The proposed relationships are discussed in Section 3.3.1.

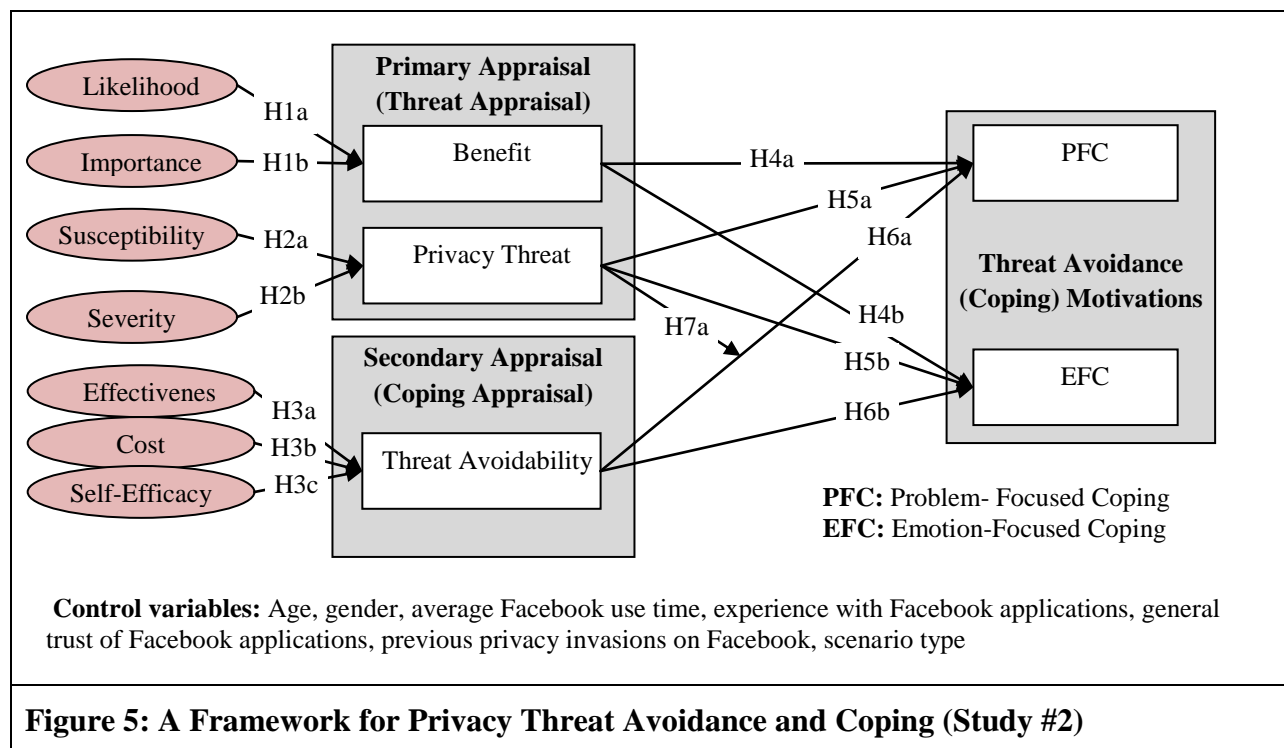


Table 7: Definitions and Sources of Key Constructs

Constructs	Definitions	Sources
Problem Focused Coping (PFC)	refers to the motivation of coping that aims to eliminate or alleviate a privacy threat in <i>objective terms</i> . PFC strategies deal directly with the source of the threat (i.e. changing privacy settings).	Coping Theory; Lazarus 1966
Emotion Focused Coping (EFC)	refers to the motivation of coping that aims to overcome negative feelings and emotions that emerge as a result of a privacy threat (Rosenstiel and Keefe 1983). While EFC behaviors do not attempt to change the objective reality, they attempt to reduce perception of a privacy threat in <i>subjective terms</i> by creating a false perception of the environment without actually changing it (e.g., denial) or adjusting one's desires or importance of desires so that negative emotions related to threat (e.g., fear and stress) are mitigated.	Coping Theory; Lazarus 1966
Threat Avoidability	refers to a user's assessment of the likelihood that he will be able to avoid a privacy threat by using a specific privacy safeguard that is available to him.	Liang and Xue 2009
Effectiveness of privacy controls that are available to a user	refers to a user's subjective judgment of the effectiveness of privacy safeguards that are available to him in managing the outflow of his personal information.	Bandura 1982; Liang and Xue 2009
Cost of adopting a privacy control	refers to physical and cognitive efforts that a user needs to adopt in order to use a privacy safeguard.	Liang and Xue 2009; Weinstein 1993
Self-Efficacy	refers to a user's subjective judgment on his personal skills, knowledge, or competency about adopting and using a privacy safeguard.	Social Cognitive Theory; Bandura 1977; Bandura 1982; Compeau and Higgins 1995

3.3.1 Primary Appraisal

Primary appraisal refers to a user's subjective assessment of an OSN feature. This appraisal may lead to two types of beliefs: benefits and privacy threats associated with using the feature.

Studies on health psychology (Janz and Becker 1984; Rogers 1975; Weinstein 2000), risk analysis (Baskerville 1991a; Baskerville 1991b) and security threat avoidance (Liang and Xue

2009; Liang and Xue 2010) propose that a user's calculation of a threat involves his assessment of the likelihood of negative consequences and the perceived severity of these consequences.

While perceived susceptibility is defined as a user's subjective judgement on the probability that a privacy threat will negatively affect him in the future, perceived severity is defined as his subjective judgement on the extent to which the negative consequences of a privacy threat will be severe for him (Liang and Xue 2009). It is hypothesized that while perceived susceptibility and perceived severity of a threat shape a user's privacy threat perception, perceived likelihood and importance of a benefit shape a user's benefit perception. Thus;

H1_a⁺: Perceived likelihood of an expected benefit associated with using a social application positively influences a user's overall benefit perception.

H1_b⁺: Perceived importance of an expected benefit associated with using a social application positively influences a user's overall benefit perception.

H2_a⁺: Perceived susceptibility of an expected privacy threat associated with using a social application positively influences a user's overall threat perception.

H2_b⁺: Perceived severity of an expected privacy threat associated with using a social application positively influences a user's overall threat perception.

3.3.2 Secondary (Coping) Appraisal

Perceived threat avoidability refers to a user's assessment of the likelihood that he will be able to avoid a privacy threat by using a specific privacy safeguard that is available to him. Drawing on prior research (Rogers 1975; Weinstein 2000; Liang and Xue 2009), perceived avoidability of a threat, driven by perceived effectiveness of a privacy control, perceived cost of using the privacy control, and a user's perceived self-efficacy, is the direct determinant of an individual's coping motivations.

Effectiveness of privacy controls refers to a user's subjective judgement that adopting and using a privacy safeguard that is available to him would effectively reduce or eliminate a privacy threat (Liang and Xue 2009). A user's perceived effectiveness of privacy controls influence his perceived threat avoidability, and in turn, his threat avoidance motivations. Thus;

H3_a⁺: Perceived effectiveness of privacy controls are positively associated with a user's perceived threat avoidability.

Cost of privacy control refers to a user's physical and cognitive efforts that are required to use a privacy safeguard (Weinstein 1993; Liang and Xue 2009). Adoption and use of a privacy safeguard requires time, comprehension and implementation efforts, and may cause inconvenience. Perceived cost can be an obstacle to a user's threat avoidance motivations, thus, negatively affecting his perceived threat avoidability. Thus;

H3_b⁻: Perceived cost of adopting privacy controls is negatively associated with a user's perceived threat avoidability.

Self-efficacy refers to a user's confidence in his personal skills, knowledge, or competency about adopting and effectively using a privacy control that would eliminate a privacy threat (Bandura 1977; 1982). A user's self-efficacy in eliminating a privacy threat requires his awareness of given privacy safeguards (i.e., privacy settings that are available to him) and his ability to adapt and utilize these controls when necessary. A user's self-efficacy positively influences his threat avoidability perception. Thus;

H3_c⁺: Perceived self-efficacy in adopting privacy controls are positively associated with a user's perceived threat avoidability.

3.3.3 Coping Behaviors

This study defines coping behaviors as a user's cognitive and emotional efforts in managing the expected negative consequences of using an OSN feature. A user's primary and secondary appraisals are proposed to influence his coping motivations (Lazarus 1966; Lazarus and Folkman 1984; Liang and Xue 2009). Note that the term "motivation" (rather than intention) is being used to assure the consistency with the current literature on coping.

Two types of coping behaviors are proposed in the theoretical framework: Problem-Focused Coping (PFC) and Emotion-Focused Coping (EFC). PFC occurs primarily when a user perceives a privacy threat and feels that he has the necessary resources to control the situation (Folkman et al. 1986; Lazarus and Folkman 1984). EFC also complements PFC so that the user can overcome his negative emotions. In general, in an intended use situation (as described in Section 2.4), a user's motivation to gain benefits from using an OSN feature and to avoid privacy threats associated with its use would motivate him to cope with a threat. Thus, the following hypotheses are suggested:

H4: Perceived benefit positively affects a user's motivations to utilize PFC (H4a⁺) and EFC (H4b⁺).

H5: Perceived privacy threat positively affects a user's motivations to utilize PFC (H5a⁺) and EFC (H5b⁺).

H6: Perceived threat avoidability positively affects a user's motivations to utilize PFC (H6a⁺) and EFC (H6b⁺).

Liang and Xue (2009) suggest that the impact of threat avoidability on avoidance motivations is negatively moderated by perceived threat in such a way that, as the threat increases, the impact of threat avoidability on avoidance motivation becomes less influential. Prior research suggests that individuals can be unresponsive to moderate to high level of privacy threats (Weinstein 2000), because when an individual's negative emotions (e.g., fear) resulting from a threat exceeds a certain level, he becomes insensitive to the changes in threat levels. Considering the context of intended use (i.e., information disclosure) that is being investigated, this study proposes a different argument. In an intended use situation, fear of a privacy threat would never exceed a critical point, since not using the feature is always an option for the user. So, when perceived threat is high, regardless of the perceived threat avoidability, a user's coping motivations would be high. However, when a user's perceived threat is low, his perceived threat avoidability would be more influential in increasing his coping motivations. Thus, the following is proposed:

H7: Perceived privacy threat moderates the relationship between a user's perceived threat avoidability and problem-focused coping motivations: when perceived privacy threat is moderate or low, perceived threat avoidability will have higher impact on problem-

focused coping, while when it is high, perceived threat avoidability will have lower or no significant impact on problem-focused coping.

3.4 Research Method

A scenario based online survey is used to test the proposed model. The initial survey instrument was developed based on the definitions of the constructs (conceptualized in section 3.3) and a comprehensive literature review. The initial survey instrument was then revised based on a card-sorting exercise and exploratory data analysis. The hypothetical scenarios were developed by adapting popular Facebook applications. The hypothetical scenarios and measurement items were then tested with two pilot tests and four applications. The scenarios which generated the highest benefit perceptions were included in the final survey. Data collection was conducted by administering the final survey online using the panel members of a market research company.

3.4.1 Development and Design of Hypothetical Scenarios

This study used a *hypothetical scenario-based survey* to address the research questions. Scenario-based approach is widely accepted in decision-making and business studies (O’Fallon and Butterfield 2005) as it incorporates the situational details that are necessary for users’ final decision making (Klepper 1989), enhances the realism of decision-making situations by providing contextual details while simultaneously ensuring that these details are uniform across respondents, and reduces measurement errors (Bachman 1992). This method is also commonly adopted in the information systems and security and privacy literatures (Darcy 2009; Malhotra et al. 2004; Siponen and Vance 2010).

The scenarios for this study were developed to investigate an *intended disclosure situation that is initiated by the user* (see Chapter 2). The participants were presented with hypothetical scenarios (Weber 1992) and asked how they would respond to the questions in a given hypothetical situation (Piquero and Tibbetts 1996; Rosenthal and Rosnow 1984). Social applications that run on the Facebook platform were selected for the purpose of this study, as they represent an intended use situation that can only be initiated by a user.

The hypothetical scenarios that have been developed consist of two parts: scenario description and application interface. Scenario descriptions were provided to explain the features of the application, and thus served to create a user's benefit perceptions. Application interfaces were provided to present the information permissions requested by an application to access, process, and utilize a user's personal information, and thus served to create a user's privacy threat perceptions. Both the scenario description and the application interface were provided simultaneously before the survey items were presented to a participant. The objective was to allow the study participants to make the cost-benefit calculations by checking both the scenario description (i.e., benefit) and the interface (i.e., threat) before they replied to the survey items.

Several pilots were conducted to develop the methodology of this study. First, an online forum was developed to stimulate a discussion with the undergraduate students who were taking a management information systems course at our institution. The discussion included the advantages and disadvantages of different OSN platforms, the features these platforms had to offer, major benefits and costs they associated with these features, and their behavioral responses. Based on these discussions, the features of various OSN platforms were listed and categorized. Then, two panel discussions were held with the MBA students in our institution to understand their threat and benefit perceptions associated with these features and behavioral

responses. As a result of these discussions, Facebook applications were selected as the focus of this investigation.

To ensure the generalizability of findings across different types of applications, various hypothetical scenarios, likely to generate different types of benefits (i.e., social, utilitarian, and mixed benefits) were developed. Based on discussions held in pre-study stages as well as the publicly available descriptions and ratings of the popular Facebook applications, nine hypothetical scenarios were developed. Next, these scenarios were reviewed in two rounds of pilot tests. The first pilot test involved 38 participants and the second 53 participants. The pilot tests included the hypothetical scenarios, the initial measurement items, and several open-ended questions regarding the realism, readability, and relevance of the developed scenarios. Each respondent was asked to review the scenarios presented in a random order, followed by the survey questions.

These pilot tests served three key purposes. *First*, they aimed to enhance the realism, readability, and relevance of the scenarios. Based on the feedback received in the first pilot test, the scenarios were revised. In the second pilot test, all participants reached a consensus that the scenarios were realistic, relevant, and easy to read, and had minor requests for improvement. After this stage, the scenario descriptions were sent to an editor to further improve the sentence structures and readability of the scenario descriptions.

Second, the pilot tests aimed to identify applications that are likely to generate the highest benefit and privacy threat perceptions among the respondents. Based on the results of the pilots, the most popular applications (i.e., the ones generating highest benefit perceptions) were selected. Perceived privacy threat was not as high as expected in the first pilot, so in the second pilot, the

application interface was revised to request additional permissions, likely to increase respondents' threat perceptions. The respondents' threat perceptions increased significantly in the second pilot test, so the designed interface was deemed appropriate to be included in the main study.

Third, the pilot tests aimed to identify a set of scenarios that could be representative of Facebook applications. It was determined that Facebook users may perceive three types of benefits in using an application: social, utilitarian, and mixed benefits. As a result, four applications generating different types of benefits (one social benefit, two mixed benefits, and one utilitarian benefit) were selected and included in the main study. The categorization of scenarios according to the benefit types, along with the questions asked for the assessment, is presented in Appendix A2.

After the final revisions, the scenarios were finalized. All the selected scenarios generated high benefit and high privacy threat perceptions. These scenarios, along with the descriptions and graphical interfaces, are presented in the Appendices (Appendix A1). When administering the survey, each participant was presented with one randomly selected scenario of the four scenarios available, followed by the survey items.

3.4.2 Development and Design of the Survey Items

Survey item development started with a comprehensive literature review to determine the existing measurement scales that have proven reliable. These items were adapted according to the purpose of this study and included in the survey instrument. For the other constructs that have not been previously operationalized and empirically tested, new measures were developed by closely following their definitions. All research constructs were measured reflectively using

multi-item Likert scales. Table 8 presents the constructs, their sources, and the number of items used to measure them, while Table 9 presents the measurement items with their anchors.

Table 8: Sources of Measurement Items

Construct	Type	Source	Items
Benefits of Use	Reflective	Bulgurcu et al. 2010a	4
Likelihood of Benefits	Reflective	Developed for this study	4
Importance of Benefits	Reflective	Developed for this study	4
Threats to Privacy	Reflective	Developed for this study	6
Susceptibility of Privacy Threat	Reflective	Developed for this study	4
Severity of Privacy Threat	Reflective	Developed for this study	4
Threat Avoidability	Reflective	Developed for this study	4
Effectiveness of Privacy Controls	Reflective	Developed for this study	3
Costs of Adopting Privacy Controls	Reflective	Developed for this study	3
Self-Efficacy	Reflective	Bulgurcu et al. 2010a	3
Problem-Focused Coping	Reflective	Developed for this study	5
Emotion-Focused Coping	Reflective	Developed for this study	5

The initial survey instrument was refined based on card-sorting exercises and exploratory data analysis. First, feedback on our initial measurement items was solicited from faculty members and graduate students who had experience with survey research methods at our institution. Early versions of the work were presented twice at our institution and feedback was obtained. Based on the feedback, the initial survey items were revised. Next, card-sorting tests (Moore and Benbasat 1991) were performed with seven graduate students who were asked to match the measurement items with predefined construct categories and definitions. The results of sorting led to satisfactory classifications.

A final test was conducted to ensure the validity and reliability of measurement items and to re-test the revised scenarios. Four survey links, each for one hypothetical scenario, were developed and a market research company (GMI: Global Market Insite) was asked to distribute the survey links to their panel members. Data was collected from 100 participants (25 participants for each

scenario) and the quality of measures tested with the partial least squares (PLS) approach to structural equation modeling. The measures had sufficient validity and reliability, so they were deemed appropriate for the study. The validated scenarios and measurement items were included in the final survey. In all pilots tests and the final survey, the questions for dependent variables were asked in the beginning of the survey, before the questions for independent variables were asked.

The survey also included demographic variables, such as age, gender, education level, and State of residence. These variables were used to execute this study's stratified sampling data collection strategy to collect from a representative sample of the Facebook population. To exclude the variance explained by confounding factors, the survey also captured participants' pre-conceptions regarding the benefits and costs associated with using Facebook and Facebook applications, as well as their prior experiences with privacy violations on social network platforms.

3.4.3 Data Collection: Selection of Participants and Procedure

Selection of Participants: Data was collected by administering the final survey instrument online. The sample was drawn from the panel of a professional market research company (i.e., GMI: Global Market Insite, Inc.). The company provided with an access to a nationwide sample of their panel members located in the United States. Since the number of Facebook users who live in the United States (approximately 157 million users that is 32% of the overall Facebook population) are larger than the number of those who live in any other country, it was deemed appropriate to collect the data from the panel members living in the United States. The subjects of this study, therefore, included the panel members who received an invitation e-mail from the

company and opted-in to complete the survey in exchange for membership points that can be redeemed for merchandise.

The sample was specifically constructed to represent the Facebook population. To reach a representative sample, a stratified random sampling strategy was utilized in this study. The most recent demographics (Facebook 2011) of the Facebook population was obtained and the research company was asked to contact a group of participants who represent the given population in terms of age, gender, education, and location based on Facebook 2011 Statistics. Participants who were less than eighteen and more than sixty-five years old were not included in the study for ethical and practical reasons. The market firm was also asked to exclude the panel members who were not active Facebook users. Based on the sampling criteria, the research company randomly selected the potential subjects from its panel and sent them e-mail invitations.

To create a diverse sample population and to reach the demographic characteristics of the sample desired, the market research firm ensured that the demographics of the drawn sample closely resembled that of the Facebook population in terms of four important attributes: age, gender, education, and location. The firm put quotas to these four attributes on the survey tool so that when a quota was reached for a given group, they continued sending invitations to the remaining groups. Several attention (trap) questions were included at different stages of the survey to prevent respondents who did not read the questions carefully from taking the survey. Wrong answers to such trap questions directly ended the survey, so the quality of the final data set was deemed to be very high. Data was collected from 200 respondents. Three respondents were removed from the final sample due to their unreliable responses, so the data analysis was conducted with 197 data points.

Of the final sample, 54 percent were female, and 27 percent were in the 36 to 45 age range. While 31 percent of the sample had an undergraduate education, 17 percent had a graduate degree. 42 percent of the people in the sample were using their social network accounts 3 to 5 times a week, while 34 percent were using Facebook for more than an hour per week. 94 percent of the respondents were aware of the social applications that run on Facebook, while 81 percent of the sample used an application on Facebook at least once. The sample was representative of the overall Facebook population in terms of gender, age, education, and location, based on Facebook 2011 Statistics. The sample demographics are presented in Appendix A3.

No significant differences were found between early versus late responders (or any other randomly selected sub-samples in the data set), reducing the concern of non-response bias (Rogelberg and Stanton 2007).

Procedure: Potential subjects were first asked to consent to participation in the study via a checkbox query. Subjects who consented to participate in the survey were then asked four main questions regarding their demographics (i.e. age, gender, education, location), followed by two questions to ensure that subjects were active Facebook users. The rest of the demographics questions were asked at the end of the survey. Subjects who did not login to the system once a week and had not spent at least half an hour on the OSN during the last six months were excluded from taking the survey. To reach the given demographics of the representative Facebook population, the market firm iteratively collected the data by sending e-mail invitations to small sub-samples. They first put quotas on each of the four demographic variables, so when one of the quotas was reached, the firm prevented those groups from taking the survey. In the next iterations, the firm continued sending e-mail invitations solely to the groups, the quotas of which had not been filled.

Following the exclusion questions, the scenario description and the application interface were presented on the same page. Subjects were asked to confirm that they had read the scenario description and carefully investigated the application interface via a checkbox query. Only the subjects who selected the check box were allowed to continue the study. The application interface was presented in all the following pages to ensure that subjects could check the permissions requested by the application. The scenario description was not included in the following pages to shorten the survey pages. However, a web link was provided on all pages to present the scenario description for those who preferred to read it again during the survey.

While scenario-based studies with few survey items often use a design of multiple scenarios per respondent (Jasso 2006), the design of one scenario per respondent was chosen because of the large number of survey items associated with each scenario (Paternoster 1982). Each respondent indicated the benefits and privacy threats they perceived in a given scenario and the strategies they would employ to cope with the perceived privacy threats. The order of questions for benefit and privacy threat constructs was randomly assigned in the survey for each survey link to control for the order effect. For the administration of the survey, each respondent was presented a randomly selected scenario and was expected to answer the same set of questions following the description and the interface of the given scenario.

3.5 Data Analysis and Results

3.5.1 Assessment of Measurement Validation

The component-based partial least squares (PLS) approach of structural equation modeling (SEM) was used to validate quality of measurement scales and to test the hypothesized

relationships in the research model. The Smart-PLS software package (version 2.0.M3) was employed to perform the analysis. The PLS was preferred over the covariance based approach because of several reasons. First, PLS is considered to be more appropriate to test exploratory models that are at the early stages of development. This study is novel in its operationalizations of several theoretical constructs (i.e. PFC, EFC, threat avoidability) and examining their effects on a user's coping intentions. Second, PLS places minimal restrictions on the sample size and residual distributions (Chin 1998). Also, PLS does not require data normality. As the collected data does not comply with the normal distribution requirement of other methods, PLS is deemed suitable for this study.

As all the measurement scales were proven to be valid and reliable, they were kept for the structural model estimation. The estimates derived from the SEM analysis were used to estimate the structural model and to test the research hypotheses. Table 9 shows the questionnaire items and their descriptive statistics.

Table 9: Measurement Items and Item Loadings

	Dimensions/Questions	Scale	Mean	STD	Load
	Perceived Benefits of Use				
	Overall, I believe that using this application would_____.				
B-1	be favorable to me	a	4.82	1.51	0.94
B-2	provide gains to me	a	4.82	1.43	0.95
B-3	be beneficial to me	a	4.93	1.43	0.97
B-4	impact me positively	a	4.82	1.45	0.94
	Perceived Likelihood of Benefits				
	It is _____ that I would enjoy the benefits of using this application.				
LB-1	likely	b	4.74	1.67	0.94
LB-2	probable	b	4.58	1.69	0.92
LB-3	expected	b	4.14	1.74	0.93
LB-4	certain	b	3.73	1.76	0.90
	Perceived Importance of Benefits				
	The benefits I would gain from using this application are _____ to me.				
IB-1	important	b	4.47	1.76	0.95
IB-2	valuable	b	4.58	1.73	0.96
IB-3	significant	b	4.31	1.71	0.96
IB-4	substantial	b	4.13	1.67	0.92
	Perceived Threats to Privacy				
	Overall, I believe that using this application would_____.				
T-1	be harmful to my privacy	A	4.28	1.62	0.91
T-2	impact my privacy negatively	A	4.22	1.64	0.91
T-3	be a threat to my privacy		4.19	1.69	0.91
T-4	result in a loss of control over my personal information		4.12	1.84	0.86
T-5	bring some uncertainty about the future use of my personal information	a	4.59	1.80	0.90
T-6	make it difficult for me to predict how my information will be accessed and used in the future	a	4.87	1.74	0.84
	Perceived Susceptibility of Privacy Threat				
	If I use this application, it is _____ that my privacy would be under threat.				
ST-1	likely	b	4.49	1.65	0.96
ST-2	probable	b	4.44	1.67	0.97
ST-3	expected	b	4.17	1.68	0.95
ST-4	certain	b	3.86	1.78	0.93

	Dimensions/Questions	Scale	Mean	STD	Load
	Perceived Severity of Privacy Threat				
	Using this application would pose a _____ threat to my privacy.				
SeT-1	severe	b	3.32	1.71	0.95
SeT-2	serious	b	3.53	1.76	0.97
SeT-3	significant	b	3.73	1.81	0.97
SeT-4	substantial	b	3.67	1.82	0.95
	Perceived Threat Avoidability				
	I feel that I can _____ the privacy threats that may result from using this application.				
TA-1	avoid	a	4.25	1.55	0.92
TA-2	ward off	a	4.16	1.53	0.93
TA-3	prevent	a	4.13	1.55	0.95
TA-4	eliminate	a	3.66	1.66	0.91
	Perceived Effectiveness of Privacy Controls				
	The privacy protection tools that I am provided with in using this application _____.				
E-1	are effective in safeguarding my privacy	a	4.13	1.45	0.98
E-2	work effectively in protecting my personal information	a	4.10	1.44	0.98
E-3	enable me to prevent potential privacy problems effectively	a	4.07	1.50	0.97
	Self-Efficacy				
	I have the necessary _____ to avoid privacy threats that may result from using this application.				
SE-1	skills	a	4.93	1.48	0.98
SE-2	knowledge	a	4.84	1.56	0.96
SE-3	competencies	a	5.01	1.52	0.97
	Perceived Costs of Adopting/Using Privacy Controls				
C-1	Modifying privacy settings to eliminate privacy threats that may result from using this application would be <u>burdensome</u> for me.	a	4.10	1.68	0.92
C -2	Adopting privacy controls to eliminate privacy threats that may result from using this application would be <u>time consuming</u> for me.	a	4.38	1.65	0.94
C -3	Changing privacy settings to avoid privacy threats that may result from using this application would be <u>difficult</u> for me.	a	3.76	1.68	0.88
	<i>Please read each item and indicate, by using the following rating scale, to what extent you would use it in the described situation.</i>				
	Problem-Focused Coping (PFC)				
	If I am to use this application, I would _____				

	Dimensions/Questions	Scale	Mean	STD	Load
	that may result from using this application.				
PFC-1	focus on what I can do to eliminate the privacy threats	c	5.27	1.46	0.90
PFC-2	work on reducing the privacy threats	c	5.43	1.46	0.94
PFC-3	try to identify solutions to get around the privacy issues	c	5.41	1.45	0.94
PFC-4	work on preventing the privacy threats	c	5.29	1.45	0.88
PFC-5	think of what I can do to avoid the privacy threats	c	5.41	1.47	0.92
	Emotion-Focused Coping (EFC)				
	If I am to use this application, I would _____ that may emerge as a result of the privacy threats posed by using this application.	c			
EFC-1	try to eliminate my worries	c			
EFC-2	try to figure out different ways to deal with my stress	c	4.66	1.48	0.80
EFC-3	work on reducing my anxieties	c	4.21	1.49	0.93
EFC-4	try to ease my frustration	c	4.21	1.49	0.94
EFC-5	think of ways to mitigate my negative feelings	c	4.36	1.47	0.93

Scales Used in the Questionnaire

a 1 Strongly Disagree; 2 Disagree; 3 Somewhat Disagree; 4 Neutral; 5 Somewhat Agree; 6 Agree; 7 Strongly Agree

b 1 Not at All — 7 = Very Much

c 1 Extremely Unlikely; 2 Quite Unlikely; 3 Somewhat Unlikely; 4 Neutral; 5 Somewhat Likely; 6 Quite Likely; 7 Extremely Likely

First, the average variance extracted (AVE) scores and the factor loadings of measurement items on respective latent variables were examined to ensure convergent validity. The AVE scores for all variables were above the minimum recommended value of 0.50 (see Table 26 in Appendix A4). The loadings for all the measurement items were also above the recommended minimum value of 0.707 (Chin 1998) (see Table 27 in Appendix A4). It was concluded that the measurement items fulfilled the required convergent validity.

Second, to ensure the discriminant validity of constructs in the research model, the square root of the average variance extracted (AVE) for each construct were compared with the other correlation scores. The square root of the AVE for each construct in the model, as reported in

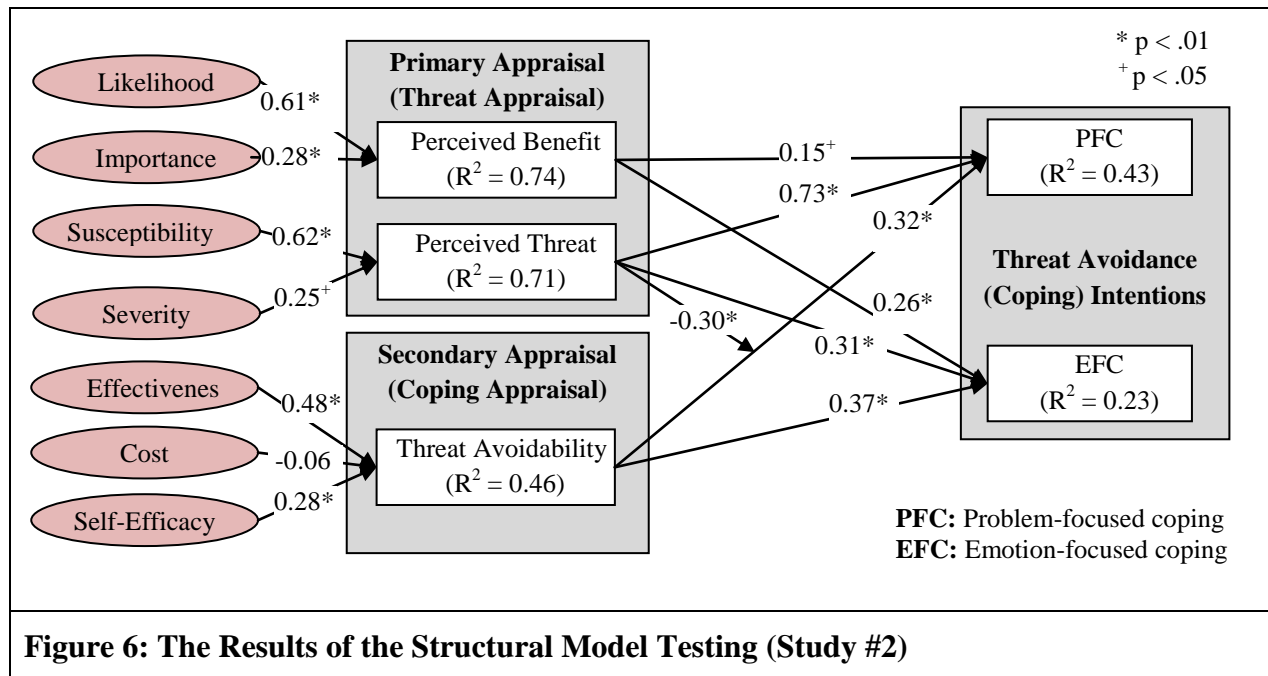
the diagonal of the correlation of constructs matrix in Appendix A4, was larger than the corresponding off-diagonal correlations of the constructs to their latent variables.

As reported in Appendix A4, the composite reliability values for all of the constructs in the research model were greater than 0.94 and Cronbach's alpha values were greater than 0.90. The scores validate that the constructs had adequate scale reliability and internal consistency (Fornell and Larcker 1981; Gefen et al. 2000; Nunnally and Bernstein 1994).

Common method bias can be a potential threat to this study, as the data were self-reported and the questions to both the dependent and independent variables were asked in the same questionnaire (Podsakoff et al. 2003). To ensure that common method bias was not a threat to this study, we applied Liang et al.'s (2007) method and created a separate factor with all items in the model (Podsakoff et al. 2003). We also conducted an exploratory factor analysis and concluded with five separate factors that were consistent with the number of main constructs in the model. The results indicated that common method bias was not a significant concern.

3.5.2 Results of the Structural Model Testing

The bootstrapping re-sampling method with 197 cases and 1,000 re-samples were used for structural model estimation. Based on the results of the model estimation, all the hypotheses, except H3b (cost → threat avoidability), were supported. The results of the structural model estimations, including R^2 values, are presented in Figure 6. The reported significance of paths is based on a two-tailed t-test.



H1a and H1b were supported at $p < 0.01$. H2a and H2b were supported at $p < 0.01$ and $p < 0.05$ respectively. Likelihood and Importance of Benefit explained 74 percent of the variance for Perceived Benefit, and Susceptibility and Severity of Threat explained 71 percent of the variance for Perceived Privacy Threat.

While the impacts of Perceived Effectiveness of Safeguards and Self-Efficacy on Threat Avoidability were statistically significant, that of Perceived Cost was not. Hence, we found significant support for H3a and H3c ($p < 0.01$), but no support for H3b. The variables explained approximately 46% of the variance for Threat Avoidability.

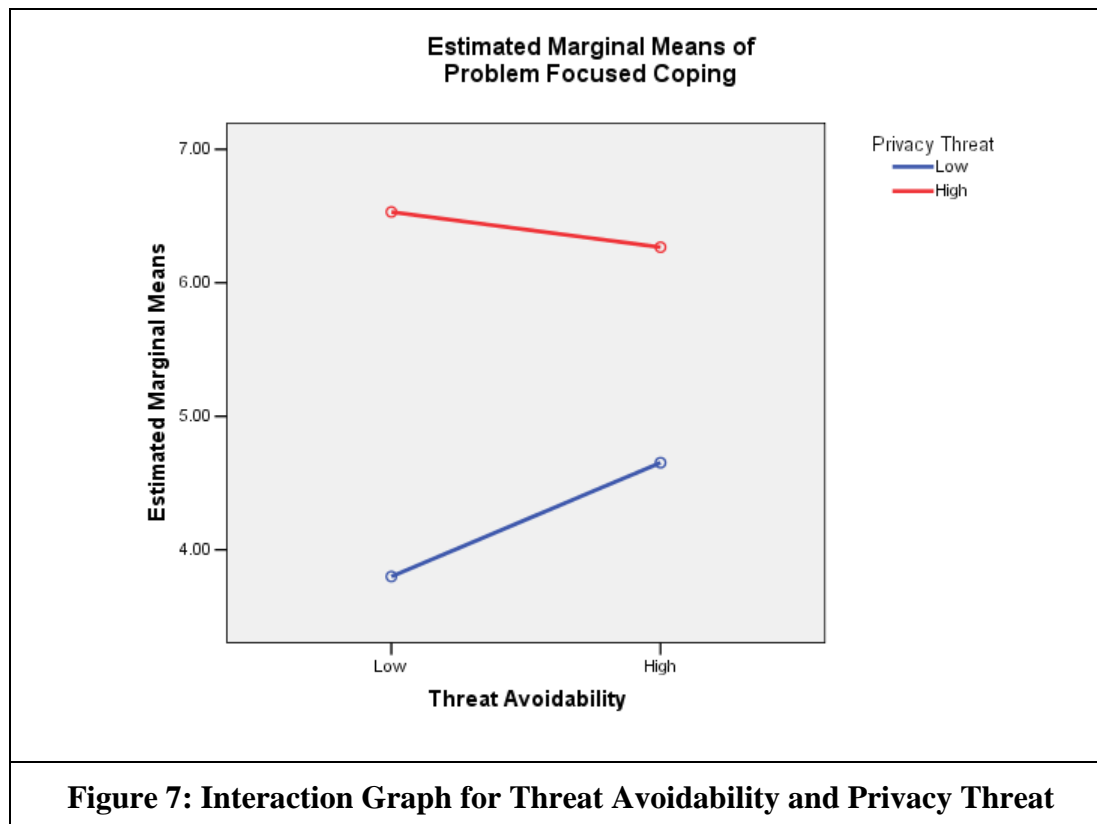
The model accounts approximately for 43 percent of the variance explained for PFC, and 23 percent of the variance explained for EFC. The effects of several variables—age, gender, average Facebook use time, experience with Facebook applications, general trust of Facebook applications, previous privacy invasions on Facebook, scenario type—were controlled on coping variables. No significant impact of control variables was found.

H4a ($p < 0.05$), H5a ($p < 0.01$), and H6a ($p < 0.01$) were supported. While Perceived Benefit, Perceived Privacy Threat, and Threat Avoidability explained 42% of the variance for PFC, the control variables explained only 1%. H4b, H4b, and H4b ($p < 0.01$) were also supported. While Perceived Benefit, Perceived Threat, and Threat Avoidability explained 21 percent of the variance for emotion-focused coping, the control variables explained only 2%.

The interaction effect of threat avoidability and privacy threat on PFC was significant, so H7 was fully supported ($p < 0.01$). In order to clarify the nature of this interaction, the participants were categorized into two groups (i.e., low and high) according to their benefit and privacy threat perceptions. Following Aiken and G. (1991), a spotlight analysis at one standard deviation above (i.e., high) and one standard deviation below (i.e., low) the mean of privacy threat was performed. The interaction graph for threat avoidability and privacy threat on PFC is presented in Figure 7: when a user's privacy threat perception is high, his PFC motivation is high regardless of his perceived threat avoidability. However, when his privacy threat perception is low, his PFC motivation increases with his perceived threat avoidability.

This result may seem to be conflicting with the proposition by Liang and Xue (2009, p. 84), which suggests that “the relationship between perceived avoidability and avoidance motivation is negatively moderated by perceived threat so that it is weaker when perceived threat increases”. According to them, when a user's perceived threat avoidability is high, the effect of high threat (caused by malicious IT) on avoidance motivation would be lower than that of low threat. As a justification, they suggest that technology users would be relatively unresponsive when they face critical threats. When fear resulting from threat reaches a certain level, it causes users to start becoming insensitive to changes in their fear level. In this study, however, we found that in a high threat situation, a user's PFC motivation would be high regardless of his perceived threat

avoidability. One explanation for this discrepancy is that, we investigated an intended disclosure situation that is initiated by the user. In such situations, privacy threat and fear caused by this threat are never expected to be critically high as the user can always decide not to use the technology. However, it may be possible that in a situation where disclosure is unintended by the user, and in particular initiated by others, his perceived privacy threat and fear caused by this threat can be critically high. In such situations, the relationship between threat avoidability and PFC motivation can be negatively moderated by perceived privacy threat.



3.6 Discussions and Conclusions

This study proposed a research model on the drivers of a social network user's coping motivations, focusing on a particular setting (i.e., voluntary; social applications). The data was collected via a scenario based online survey and the proposed model was empirically tested with the data collected from 197 active Facebook users. Data analyses revealed important research findings that provide a deeper understanding of a user's privacy threat avoidance motivations. The results indicate that a user's perceived threat is determined by perceived susceptibility and severity of the threat; while benefit is determined by perceived likelihood and importance of the benefit. Second, a user's perceived threat avoidability was found to be determined by his perceived effectiveness of safeguards that are available to him, costs of using these safeguards, and self-efficacy. As a main contribution, this study showed that a user's benefit, privacy threat, and threat avoidability perceptions significantly affect his threat avoidance motivations. Finally, this study provides empirical evidence to support the moderating effect of perceived threat on the relationship between threat avoidability and problem-focused coping.

3.6.1 Discussion of Findings and Implications

This study investigated the antecedents of two types of coping motivations: problem-focused coping and emotion-focused coping. Based on data collected from 197 Facebook users, strong support was found for the proposed theoretical model. Both types of coping motivations were found to be influenced by perceived threat avoidability, as well as the perceived benefits and privacy threats associated with using an application. It was also found that, while perceived privacy threat and threat avoidability positively influence a user's PFC motivations, their interaction have a negative impact on PFC. If a user's privacy threat perception is too high; his

PFC motivation would be high regardless of his perceived threat avoidability. However, if his privacy threat perception is moderate (or low); his PFC motivation would depend on his perceived threat avoidability.

This study makes important contributions to the coping and privacy literatures. While there is an emerging body of literature on user's privacy threat coping motivations in the privacy literature, the concept of coping as an individual response to perceived privacy threats has not been systematically explored in the literature. This study adopted coping theory as a lens to study a user's privacy threat coping motivations and proposed two focal coping dimensions as the dependent variables. As a contribution, the proposed constructs were operationalized, their measurement items were empirically validated, and the proposed relationships were tested using quantitative data analysis methods.

The results showed that a user's coping motivations are influenced by three major variables—a user's benefit, privacy threat, and threat avoidability perceptions. This study's unique contribution is in showing that not only a user's threat perceptions but also his benefit perceptions drive his coping motivations in a social network context. As an extension of Liang and Xue (2010)'s work, this study proposed two types of coping rather than amalgamating them under a general construct (i.e. avoidance motivation). Therefore, this study showed how a user's benefit and threat perceptions individually affect his coping motivations.

While threat avoidability was proposed as a mediator variable between a user's coping appraisal and coping motivations (Liang and Xue 2009), this has been excluded in the empirical analysis and suggested as a future work (Liang and Xue 2010). As a contribution, this study operationalized and tested the impact of the threat avoidability construct.

While the potential impacts of different benefit types (i.e., social, utilitarian, and mixed benefits) on a user's coping motivations were controlled by using different scenarios, no significant impact was found. This implies that while the magnitude of benefit significantly affects a user's coping motivations, the nature of benefit does not matter. It also increases the generalizability of the results to various applications which offer different types of benefits.

3.6.2 Limitations and Future Research

A major limitation of this study is related to the cross-sectional data collection method. The data collected for the dependent and independent variables of the study were collected at the same time with the same survey instrument. This precludes our ability to make causal inferences regarding the observed relationships, despite the strong theoretical base that supports them.

Another important limitation of this study is that it employs perception-based measures rather than actual behaviors. While the use of hypothetical scenarios allows all study participants to think at the same level of abstraction of details, this study could be improved by investigating the actual behavior and by collecting data across time for dependent and independent variables.

This study does not consider the interplay between a user's primary and secondary appraisal as a process, but investigates a snapshot of the process adopting a variance model (i.e., focusing on how primary appraisal affects secondary appraisal at a certain point in time). Thus, this study does not provide insight into how a user's assessment of the consequences of coping affects his reassessment of the feature (i.e., primary appraisal) and the effectiveness of coping resources. As the actual coping behavior was not captured in this study, it was not deemed appropriate to ask how a user's assessment evolved as a consequence of his coping acts. Future research is needed to extend the view presented in this study in order to thoroughly understand the entire process.

Research, in particular, should focus on ascertaining the links among a user's coping acts and his reappraisal of the consequences of using a social feature (i.e., reappraisal of threat and benefit) and effectiveness coping resources (i.e., reappraisal of coping), and eventually on determining how the results of the process affect his decision to use a social feature.

Also, further research is essential to understand the different types and dimensions of a user's coping behaviors. This study investigated problem and emotion focused coping as broad concepts. However, the various specific strategies that can be employed by the user to eliminate the privacy threat (e.g., safeguarding, fabrication etc.) or deal with emotions (e.g., wishful thinking, denial etc.) should be investigated in future research.

This study focused on a voluntary setting in which an OSN feature is likely to be categorized as a challenge (i.e., high benefit and high threat). For more comprehensive results, further research should also investigate and compare a user's threat avoidance behaviors in different contexts. A fruitful research direction would be investigating coping behaviors in a setting where information disclosure is unintended.

Finally, although this study provides insight into how a user's primary and secondary appraisals affect his coping behaviors, it does not explain how different environmental conditions may affect a user's employment of different coping acts. For example, in which situations does a user prefer to employ direct coping strategies (e.g., safeguards) over indirect ones (e.g., data fabrication, withholding)? Future research would strongly benefit from conducting controlled experiments to investigate the changes in a user's coping acts in different settings (i.e., intended vs. unintended) provided with sufficient or insufficient privacy controls. These studies should focus on understanding how environmental conditions which are likely to affect a user's benefit,

threat, and control perceptions, result in changes to the sequencing and strength of a user's problem and emotions focused coping efforts. Such studies would help us understand the conditions under which a user would be more likely to employ problem or emotion focused coping, and vice versa.

4 The Roles of Permission Requests and Privacy Controls in Shaping a User's Primary Appraisal and Use Intentions: An Empirical Study on Facebook Applications (Study #3)

4.1 Overview

Coping theory (Lazarus 1966; Lazarus and Folkman 1984) develops an understanding of coping by examining the stages that an individual goes through to cope with a harmful event. The theory postulates that an individual's coping efforts are shaped by a process that includes several consecutive and interrelated stages that can be cognitive or behavioral (i.e., primary appraisal, secondary appraisal, and coping). As suggested by the theory, the coping process starts with an individual's recognition of an event, followed by its appraisal (i.e., primary appraisal—assessment of whether the consequences of the event are beneficial or harmful to the individual). The theory, however, is silent on the factors that shape a user's primary appraisal.

The literature on information privacy also lacks sufficient theoretical and empirical explanations on the issue. To present a cohesive view of the extant privacy-related literature, Smith et al. (2011) proposed a macro model based on a summary of existing research. The model summarized the antecedents and outcomes of technology users' privacy concerns, proposed in the privacy literature, and depicted them in a macro view (i.e., Antecedents → Privacy Concerns → Outcomes). They argued that while a significant number of studies have investigated the relationship between a privacy concern and behavioral outcomes, limited attention has been paid to understanding the factors that serve as the antecedents of privacy concerns. A small body of prior research, which investigated the antecedents of privacy concerns, focused on a number of variables, such as: previous privacy experiences and victimization (Smith et al. 1996), privacy

awareness (Malhotra et al. 2004; Phelps et al. 2000), procedural fairness (Culnan and Armstrong 1999; Milne and Culnan 2004), seeking permission to collect and use personal information (Nowak and Phelps 1995; Nowak and Phelps 1997), role overload and conflict (Zhang et al. 2011), performance and effort expectancy (Fadel and Brown 2010), personality differences (Bansal et al. 2010; Dinev and Hart 2006; Xu 2007), demographic differences (Culnan 1993; Sheehan and Hoy 1999; Sheehan and Hoy 2000), and cross-cultural differences (Dinev et al. 2006; Johnston et al. 2009; Xu et al. 2008). These studies were conducted with only minimal replication, so further research was advised to understand those antecedents as well as the others that have not yet studied in the literature (Smith et al. 2011).

To expand our understanding of antecedents of primary appraisal, this study focuses on the context of *Online Social Networks (OSNs)* and investigates the roles of two important factors—*permission request* and *privacy control*—in shaping an OSN user's primary appraisal. The study, in particular, investigates how these factors shape a user's appraisal of a *social application* (i.e., a user's benefit and privacy threat perceptions associated with using the application), and in turn, his intention to use to it. The study first proposes a theoretical framework and empirically tests it using the data collected from 746 Facebook users via a scenario-based online experiment.

Permission request refers to the extent and sensitivity of permissions requested by a social application to access, process, disclose, and/or utilize a user's personal information that are available on a user's social network profile in return for the service it provides to the user. In general, to adopt and use a social application on a social network site, a user has to give certain permissions to the application, such as: access to some of his own or his friends' personal information (e.g., access to birthdays, photo albums), process some of his own or his friends' personal information (e.g., send SMS message), or disclose some of his personal information

(e.g., disclose purchase history on profile page). By manipulating the extent of permissions requested on an application (e.g., low vs. high permission request), this study investigates how the extent of permission requests affects a user's primary appraisal, and in turn, his intention to use the application.

Privacy control refers to the extent of privacy safeguards provided by an OSN feature to potential users in order to enable them to protect their information and/or to adapt the permissions according to his privacy preferences. Despite the importance of privacy controls (safeguards) in ensuring a safe computing environment, there are only a few theoretical and empirical attempts to study the nature and influence of controls (Margulis 2003a; Smith et al. 2011). These studies (presented in Table 10) mainly propose perceived control as an alleviator of a user's privacy concerns. By manipulating the extent of privacy controls provided on an application (i.e., low vs. high privacy control), this study investigates how the given privacy controls affect a user's primary appraisal, and in turn, his intention to use an application.

Table 10: Studies in the IS literature that focus on control

Argument/Findings	Type	References
Perceived control over personal information → Privacy concern	Empirical	Xu 2007; Malhotra et al. 2004; Xu et al. 2011
The amount of privacy control desired → Privacy concern	Empirical	Phelps et al. 2001; Phelps et al. 2000
Perceived ability to control disclosure of personal information → Privacy concern	Empirical	Dinev and Hart 2004
Perceived lack of control over personal information → Perceived privacy invasion	Theoretical	Culnan and Armstrong 1999; Nowak and Phelps 1997; Sheehan and Hoy 2000

Finally, while the privacy literature provides strong evidence of the negative effect of privacy threats (or concerns) and positive effect of benefits on a user's use and disclosure behavior, it does not provide any discussion on the relative importance of these factors in influencing a

user's behavioral responses. An exception is an empirical study which found a user's perceived benefit (i.e., convenience and monetary rewards) can be effective in mitigating his privacy concerns (Hann et al. 2007). To explore the interplay between a user's benefit and privacy threat perceptions and investigate their relative impacts on a user's intention, this research constructs a setting where both a user's benefit and privacy threat perceptions associated with using an OSN feature are expected to be high.

4.2 Theoretical Framework and Hypotheses

This section presents the proposed research model (Figure 8), the definitions of variables, and the development of hypotheses.

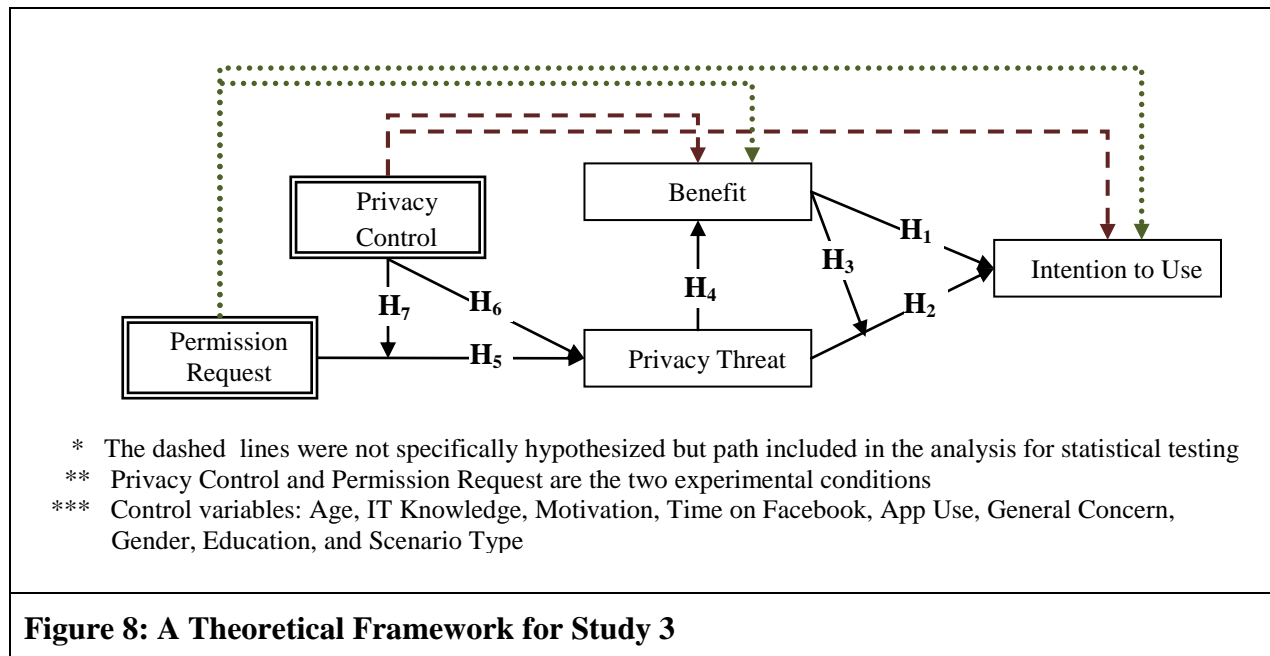


Figure 8: A Theoretical Framework for Study 3

4.2.1 Definitions of Variables

The variables proposed in the theoretical model are: intention to use, benefit, privacy threat, permission request, and privacy control. While intention to use was proposed as the dependent variable of this study, benefit and privacy threat were proposed as the mediator variables.

Permission request and privacy control were proposed as the two experimental conditions of the study. Intention to use was adopted from Theory of Planned Behavior (Ajzen 1991; Fishbein 1975), perceived benefit and perceived privacy threat were adopted from Study #2 in this thesis, and the two experimental conditions were designed and manipulated for this study.

The definitions and sources of the constructs are presented in Table 11. The operationalizations of the experimental conditions and the manipulated application interfaces are presented in *Section 4.3.1* and *Appendix B1* respectively.

Table 11: Operationalization and Sources of Constructs

Construct	Definition	Source / Condition
Intention to Use	A user's intention to use a feature (i.e., an application) on a social network platform.	Theory of Planned Behavior (Ajzen 1991; Fishbein 1975)
Perceived Benefit	A user's subjective assessment of the positive outcomes associated with using a social application.	Adopted from Study 2.
Perceived Privacy Threat	A user's subjective assessment of the negative outcomes associated with using an application.	Adopted from Study 2.
Permission Request	An experimental condition that refers to the extent and sensitivity of information related permissions requested by a social application.	Manipulation of the application interface.
Privacy Control	An experimental condition that refers to the extent of privacy safeguards that are provided by a social application.	Manipulation of the application interface.

Intention to use refers to a user's intention to use an OSN feature. This study particularly investigates a user's voluntary adoption of an application that runs on an OSN platform (i.e., a social application on Facebook).

Permission request refers to the extent and sensitivity of information related permissions requested by an OSN feature to access, process, disclose, and/or utilize a user's personal information that are available on a user's social network profile. For example, the application may request permission to access and use some of his personal information (e.g., permission to access to friends' birthdays and develop a birthday reminder calendar, access to cell phone number and send SMS messages as reminders) or disclose some of his personal information (e.g., disclose purchase history on profile page). Note that while a user has to allow the requested permissions (by clicking on the allow button available on the application interface) in order to use the application, he is not required to disclose this information on his social network profile. If the user did not provide his cell phone number on his profile page, for example, the application cannot access and use this information, even if he grants this permission to the application. By manipulating the extent of permissions requested by an application (i.e., low vs. high permission request), this study investigates how permission requests affect a user's benefit and privacy threat perceptions, and in turn, his use intention.

Privacy control refers to the extent of privacy safeguards provided by an OSN feature to increase a user's ability to protect his personal information against the undesired consequences of its information practices (Altman 1975; Dinev and Hart 2004; Hann et al. 2007). The provided controls enable a user to remove and/or adapt some of the permissions requested by the application according to his privacy preferences. By manipulating the extent of privacy controls provided by an application (i.e., low vs. high privacy control), this study investigates how

privacy controls affect a user's benefit and privacy threat perceptions, and in turn, his use intention.

4.2.2 Development of Hypotheses

Prior studies in the privacy literature have focused on understanding the antecedents of behavioral and cognitive outcomes in the presence of a user's privacy concerns (Smith et al. 2011). A group of studies proposed privacy concerns as an inhibitor of information disclosure and technology adoption. These studies have provided theoretical and empirical evidence for the negative impact of a user's privacy concern on several cognitive and behavioral responses; such as, likelihood of using personalized services (Chellappa and Sin 2005), intention to disclose information (Malhotra et al. 2004), purchase decision process and purchase behavior (Phelps et al. 2001), disclosure of health information (Bansal et al. 2010), attitude towards adopting electronic health records (Angst and Agarwal 2009).

Another stream of research focused on the concept of privacy calculus, referring to technology users' calculative risk-benefit assessments. These studies argued that a user is expected to choose the best alternative available to him by acting towards gaining benefits and refraining from costs (Culnan and Armstrong 1999). Thus, they suggested that a user's subjective assessment of the potential consequences of using a technology (i.e., benefit and risk perceptions) determines his behavioral intention to disclose or use the technology (Culnan 1993; Dinev and Hart 2006; Li et al. 2010; Malhotra et al. 2004; Xu et al. 2009). These studies provided evidence for the positive effect of perceived benefits and the negative effect of perceived privacy risk (or privacy threat) on a user's behavioral responses (i.e., adoption, use, disclosure) in various contexts, such as; online shopping (Featherman and Pavlou 2003; Malhotra et al. 2004; Norberg and Horne 2007;

Norberg et al. 2007), push-pull technologies (Xu et al. 2009), and social networks (Krasnova et al. 2009; Krasnova and Veltri 2010). Financial compensation (Hann et al. 2007; Phelps et al. 2000; Xu et al. 2009), personalization and convenience (Chellappa and Sin 2005; White 2004), social adjustment, self-presentation, and enjoyment (Krasnova and Veltri 2010; Krasnova 2010; Lu et al. 2004) were proposed as benefits that a user receives in return for his information disclosure.

Similarly, consequences of using a social application on an OSN platform are expected to be associated with costs and/or benefits. Drawing on the privacy calculus literature, it is suggested that while a user's privacy threat perception negatively affects his intention to use an application, his benefit perception positively affects it. Thus;

H₁: The higher the benefits a user perceives associated with using an application, the higher his intention to use it.

H₂: The higher the perceived privacy threats a user perceives associated with using an application, the lower his intention to use it.

This study also posits the relationship between perceived threat and intention as a function of perceived benefit, such that the higher the perceived benefit, the weaker the threat-intention relationship. It is expected that a user with high benefit perceptions will be less sensitive to privacy threats than a user with low benefit perceptions, although he may have high threat perceptions simultaneously. While the literature does not provide much insight into a potential benefit-threat interaction, a few studies provide empirical evidence for the effect of benefit in overriding a user's privacy concerns (Chellappa and Sin 2005; Hann et al. 2007). This study,

particularly designed to generate high benefit and high threat perceptions, will test the effect of proposed benefit-threat interaction on intention. Thus;

H₃: *Benefit* moderates the relationship between *privacy threat* and *intention to use*, such that for individuals who perceive *low benefits*, higher *privacy threat* will have a higher negative impact on *intention*, but for those who perceive *high benefit*, higher *privacy threat* will be less influential or have no significant impact on intention.

The study also tests the negative impact of privacy threat on benefit. While this relationship has not been studied in the privacy literature before, we argue that an increase in a user's perceived privacy threat associated with using an application can reduce his benefit perception. Fiske (1980) found that as a result of simultaneous good and bad experiences, individuals feel worse than neutral, even if they independently judge the two experiences to be of similar magnitude. Similarly, in this context, it may be possible that as a result of perceiving two types of stimulus simultaneously in the given scenario—*positive stimulus* that derives from scenario description and *negative stimulus* that derives from application interface—respondents' benefit perceptions are negatively affected by their privacy threat perceptions. Hence, we suggest;

H₄: The higher the perceived privacy threat associated with using an application, the lower the perceived benefit.

Previous research showed that a technology user's perceptions of and responses to information practices of online companies are linked (Angst and Agarwal 2009; Smith et al. 2011; Smith et al. 1996). The privacy literature proposed several information practices as the dimensions of a user's privacy concerns. For example, Solove (2006) proposed a privacy taxonomy and identified a list of potential harmful consequences a user may incur as a result of companies' data

collection, processing, dissemination, and invasion practices. Smith et al. (1996) has identified privacy concern dimensions on several information practices—collection, unauthorized internal or external secondary use, improper access, and processing of data. Based on these practices, several studies in the literature posited that a user's concerns over these practices can be the potential inhibitors of technology adoption and use (Malhotra et al. 2004; Solove 2002; Hine and Eve 1998; Malhotra et al. 2004; Okazaki et al. 2009; Phelps et al. 2000; Smith et al. 1996; Stewart and Segars 2002; Van Slyke et al. 2006).

An application requires a user to grant certain permissions (i.e., information practices) to the application. Nowak and Phelps (1997) suggested that, in the context of direct (offline) marketing, consumers tend to be less concerned about their privacy when marketing firms seek permission to collect and use their information. Permission seeking may reduce privacy concerns in offline settings; however, we suspect that it does not apply to online settings. Permission seeking can make the user more aware of the information practices of the OSN feature for which the permissions were requested. As a result of this awareness, the user starts thinking about the potential consequences of these practices; thus, threat (primary) appraisal is initiated. In this study, we suggest that the extent of those permissions requested by an application increases a user's privacy threat perceptions. Thus,

H₅: Compared to those under *high permission request* conditions, users under *low permission request* conditions will perceive *lower privacy threat* associated with using an application.

Privacy literature has linked the concept of privacy with control by either defining privacy as control (Altman 1974; Altman 1975; Margulis 2003a; Margulis 2003b; Westin 1967) or by

positioning control as a key factor in shaping privacy perceptions (Smith et al. 2011; Dinev and Hart 2004; Malhotra et al. 2004; Smith et al. 1996; Westin 1967; Xu 2007). These studies view control as an ultimate means to enhance a user's autonomy and minimize his vulnerability to privacy invasions. A few studies empirically showed that a user's perceived control (or ability to control) can reduce his privacy concerns (Dinev and Hart 2004; Xu 2007). Similarly, this study hypothesizes that the higher the privacy controls provided by an application (i.e., limited vs. full controls) the lower a user's privacy threat perception.

H₆: Compared to those under *high privacy control* condition, users under *low privacy control* condition will perceive *higher privacy threat* associated with using an application.

Because the potential privacy threats can be mitigated by adopting the privacy controls provided, this study also proposes an interaction effect of permission request and privacy control. That is, the impact of high permission request will have lower impact on privacy threat for a user in a high privacy control condition compared to one in a low control condition, as the user will have full control to deal with the threat. However, the impact of high permission request will have high impact for a user in a low privacy control condition as he will have limited control to deal with the threat,. Thus;

H₇: *Privacy control* moderates the relationship between *permission request* and *privacy threat*, such that for a user in a *low privacy control* condition, *higher permission request* will have a higher positive impact on *privacy threat*. However, for a user who is in a *high control* condition, the effect of high *permission request* on *privacy threat* will be less influential or insignificant.

4.3 Research Method

To test the proposed relationships in the theoretical model, an online experiment was administered using a hypothetical scenario method (Weber 1992). The following sub-sections present the study design, operationalization of variables, and data collection procedures.

4.3.1 Study Design and Operationalization of Variables

The two independent variables that were investigated in this study were permission request and privacy control. A **2** (permission request: low vs. high) **by 2** (privacy control: low vs. high) *between-subject factorial design* was used. The four hypothetical scenarios developed in Study #2 were used in this study. While scenario descriptions were directly adopted, the scenario interfaces were manipulated according to the four experimental conditions. To check the effectiveness of the manipulations, a pilot test was conducted with 60 participants (i.e., 15 respondents for each manipulated interface). As there were significant differences among the groups (see section 4.4.1 for the details), the manipulated interfaces were included in the main study (presented in Appendix B1).

Permissions request was operationalized as the extent and sensitivity of information related permissions requested by the application. The manipulations were performed on the application interfaces of the hypothetical scenarios. The low permission request interface was directly adopted from Study 2. For the high permission request interface, a number of other permission requests were modified and some others were included in the interface. The new permissions were particularly selected due to the sensitivity of their requests (i.e., post to Facebook as me, send me SMS message, read my check-ins and my friends' check-ins). Table 12 compares the

low and high permission request interfaces. The sample interfaces are presented in Appendix B1 (See Figures 20 and 22 for low permission request interfaces, and Figure 21 and 23 for high permission request interfaces).

Table 12: Comparison of Low vs. High Permission Request Interfaces

Permissions Requested in Both Low and High Permission Request Interfaces	
Access my basic information – includes name, profile picture, gender, networks, user ID, list of friends, and any other information I’ve made public.	
<i>Send me e-mail</i> – City Spot may e-mail me directly.	
<i>Access my data any time</i> - City Spot may access my information any time.	
Permissions Requested in Low Permission Request	Permissions Requested in High Permission Request
<i>Post to my wall</i> - City Spot may post status messages, notes, photos, and videos to my wall	<i>Post to Facebook as me</i> - City Spot may post status messages, notes, photos, and videos on my behalf.
<i>Access my profile information</i> – Includes About Me, Activities, Interests, Birthday, Hometown, Location, Education History, Relationship Status	<i>Access my profile information</i> - Includes Likes, Music, TV, Movies, Books, Quotes, About Me, Activities, Interests, Groups, Events, Notes, Birthday, Hometown, Current Cities, Work History, Photos, Videos, and Facebook Statuses
	<i>Send me SMS messages</i> - City Spot may send SMS messages to my phone
	<i>Check-ins</i> - City Spot may read my check-ins and friends’ check-ins
	<i>Access my contact information</i> - City Spot may access my current address and phone number

Privacy control was operationalized as the extent of privacy safeguards provided by an application that enables a user to remove or revise the requested permissions according to his preferences. There were no privacy controls provided on the application interface in low control condition. However, as the option is available on Facebook, respondents could consider revising general privacy settings on the OSN platform (but this was not explicitly stated in the scenario description). In contrast, a full set of privacy controls were provided on the application interface in high control condition. The given controls provided flexible options to the respondents, as

they could choose not to grant the requested permissions (e.g., never post to my wall, delete e-mail, remove permissions etc.) or customize them according to their privacy preferences (i.e., change e-mail address, customize to whom the information will be available). Note that the request for basic information is default for all applications on Facebook, so there was no control provided to remove its permission. Table 13 compares the low and high privacy control interfaces. The sample interfaces are presented in Appendix B1 (See Figures 22 and 23 for low privacy control, and Figure 20 and 21 for high privacy control interfaces).

Table 13: Comparison of Low vs. High Privacy Control

Privacy Controls in Low Privacy Control Interface	Privacy Controls in High Privacy Control Interface
<i>Access my basic information</i>	<i>Access my basic information</i>
<i>Send me e-mail</i>	<i>Send me e-mail</i> * Change e-mail * Delete e-mail
<i>Post to my wall</i>	<i>Post to Facebook as me</i> * Never post to my wall * Customize
<i>Access my data any time</i>	<i>Access my data any time</i> * Remove
<i>Access my profile information</i>	<i>Access my profile information</i> * Remove * Customize
	<i>Send me SMS messages</i> * Remove
	<i>Check-ins</i> * Remove
	<i>Access my contact information</i> * Remove

The measures for all variables were 7-point scales adapted from prior research. The measures for the dependent variable (i.e., intention to comply) were adapted from Theory of Planned Behavior (Ajzen 1991; Fishbein 1975). The measures for mediator variables (i.e., benefit and privacy threat) were adopted from Study #2. The measurement items are presented in Table 14.

Table 14: Measurement Items and Item Loadings

	Dimensions/Questions	Scale	Mean	STD	Load
	Intention to Use				
IU-1	I would consider using this application in the future.	a	4.28	1.83	0.91
IU-2	I intend to use this application in the future.	a	3.90	1.80	0.92
IU-3	I would consider using this application the next time ____.	a	4.32	1.85	0.90
	I need to search for local deals in my city. * <i>used for City Spot Scenario</i>	a			
	I need to search for a distant family member. * <i>used for Whole Ancestry Scenario</i>	a			
	I need to search for venues in my city. * <i>used for Site Share Scenario</i>	a			
	I need advice or peer support on health related matters. * <i>used for the Healthy Living Scenario</i>	a			
IU-4	I would recommend to my friends that they use this application.	a	4.10	1.69	0.81
	Perceived Benefits of Use				
	Overall, I believe that using this application would ____.				
B-1	be favorable to me	a	4.46	1.62	0.89
B-2	provide gains to me	a	4.58	1.58	0.92
B-3	be beneficial to me	a	4.63	1.61	0.94
B-4	impact me positively	a	4.54	1.60	0.90
	Perceived Threats to Privacy				
	Overall, I believe that using this application would ____.				
T-1	be harmful to my privacy	a	4.62	1.69	0.94
T-2	impact my privacy negatively	a	4.51	1.71	0.94
T-3	be a threat to my privacy	a	4.58	1.77	0.93
T-4	result in a loss of control over my personal information	a	4.39	1.81	0.84
T-5	bring some uncertainty about the future use of my personal information	a	4.89	1.75	0.92
T-6	make it difficult for me to predict how my information will be accessed and used in the future	a	5.12	1.69	0.87
	Control Variable: Age		N*		
	What is your age?				
	19–25		167		
	26–35		195		
	36–45		138		
	46–55		159		
	56–65		62		
	66–75		26		

Dimensions/Questions	Scale	Mean	STD	Load
Control Variable: Education		N*		
Please indicate the highest level of education you have attained:				
Less than high school		117		
High school degree		121		
College degree		130		
Undergraduate degree		228		
Graduate degree		137		
Other _____		14		
Control Variable: IT Knowledge				
How would you rate your knowledge of computers and information technologies?	b	5.02	1.20	
Control Variable: Motivation				
<ul style="list-style-type: none"> Receiving deals from local businesses is important to me. (<i>City Spot</i>) Learning about my ancestors and distant family members is important to me. (<i>Whole Ancestry</i>) Searching for new venues in the city and sharing the experiences I've had with local businesses are important to me. (<i>SiteShare</i>) Getting health related advice and peer support are important to me. (<i>Healthy Living</i>) 	a	4.31	1.85	
Control Variable: General Concern <i>Adapted from Dinev and Hart 2006</i>				
I am concerned that the information I disclose to Facebook applications could be misused.	a	5.09	1.48	0.95
I am concerned about providing personal information to Facebook applications, because of what others might do with it.	a	5.16	1.50	0.97
I am concerned about providing personal information to Facebook applications, because it could be used in a way I did not foresee.	a	5.26	1.49	0.96
Control Variable: Average Time on Facebook				
How much time (approximately) do you spend on Facebook?				
Up to 15 minutes per month				
Up to 15 minutes per week				
Up to 15 minutes per day		3.80	1.11	
Up to 1 hour per day				
Up to 3 hours per day				
More than 3 hours per day				
Control Variable: Use of Facebook Applications				
Do you use Facebook Applications?		2.64	1.13	

Dimensions/Questions		Scale	Mean	STD	Load
	Never				
	Rarely				
	Sometimes				
	Often				
	Always				

Scale

a 1 Strongly Disagree; 2 Disagree; 3 Somewhat Disagree; 4 Neutral; 5 Somewhat Agree; 6 Agree; 7 Strongly Agree

b 1 (Very Low) -- 7 (Very High)

N For Age and Education, counts (N) were reported for each age and education group.

* The question was slightly modified to make it relevant to the presented hypothetical scenarios. One of the four questions was included to the survey link according to the scenario it presents.

Finally, 16 application interfaces were custom designed for the study (i.e., four experimental conditions for each of the four hypothetical scenarios). Each interface was included in the beginning of one of 16 survey links followed by the questionnaire items. Each subject was randomly assigned to a single questionnaire/link. Because of the between-subject design of the study, each participant observed a single interface and was asked to answer all the subsequent questions according to the given interface. The experimental conditions, scenario names, and survey links are summarized in Table 15.

Table 15: Experimental Conditions, Scenarios, and Survey Links

Group #	1	2	3	4
<i>Exp. Condition/ Scenario Name</i>	<i>Low Request Full Control</i>	<i>High Request Full Control</i>	<i>Low Request Limited Control</i>	<i>High Request Limited Control</i>
Whole Ancestry	Survey Link #1	Survey Link #2	Survey Link #3	Survey Link #4
Site Share	Survey Link #5	Survey Link #6	Survey Link #7	Survey Link #8
Healthy Eating	Survey Link #9	Survey Link #10	Survey Link #11	Survey Link #12
City Spot	Survey Link #13	Survey Link #14	Survey Link #15	Survey Link #16

4.3.2 Sample and Data Collection

The data collection procedures in Study #2 were also followed in this study. The sample was drawn from a panel of members of a professional market research company. The company provided access to a nationwide sample of their panel members located in the United States. A stratified random sampling strategy was utilized to acquire a sample that represents the Facebook population. To reach the demographic characteristics of the sample desired, the demographics of the drawn sample closely resembled that of the Facebook population in terms of four important attributes: age, gender, education, and location.

The potential subjects were randomly directed to one of the 16 survey links developed for the study. The design of one scenario per respondent was chosen, as in Study #2, because of the large number of survey items associated with each scenario (Paternoster 1982). Similar to the survey design in Study #2, the subjects were first asked to consent to participation in the study. Then they answered the four main questions regarding their demographics (i.e. age, gender, education, location), followed by two questions to ensure that the subjects were active Facebook users. Following the exclusion questions, the scenario description and the application interface were presented on the same page. Please see the data collection procedures in Study #2 for more details.

Data was collected by administering the final survey instrument online. The final sample included data from 800 respondents (50 data points for each survey link). However, the subjects who provided unreliable responses to manipulation check questions were removed from the data set. As a result, the data analysis was conducted with 747 data points.

The sample in this study is representative of the overall Facebook population in terms of gender, age, education, and location, based on Facebook 2011 Statistics. Of the final sample, 27 percent were in the 19 to 25 and another 27 percent were in the 36 to 45 age range. 55 percent of both age groups were female. The details of the sample demographics are presented in Appendix B, Table 28.

4.4 Analysis and Results

This section first presents the results of the manipulation checks and data analysis conducted with the data collected from 747 respondents. The manipulation checks were conducted with ANOVA tests and the results are presented in Section 4.4.1. The data analysis was conducted in three stages. In the first stage, principle component analysis was used to create factor scores for each variable using SPSS. In the second stage, Hierarchical Linear Modeling (HLM) was used to test the effects of a series of independent variables on intention to use and to identify the theoretical model with the highest explanatory power (R^2). At this stage, the analyses suggested by Baron and Kenny (1986) were also conducted to test the mediating effect of perceived benefit and privacy threat on intention to use. The results of the HLM regressions are presented in Section 4.4.2. In the last stage of the analysis, ANOVA was used to understand the effects of experimental conditions on perceived benefit and privacy threat. The results of the ANOVA tests are presented in Section 4.4.3.

4.4.1 Control and Manipulation Checks

ANOVA tests were performed to confirm that the random assignment of subjects to one of the four experimental conditions was successful. To ensure that the random assignment had been

successful, four treatment groups on a variety of demographics variables were compared. Results indicate that there were no significant differences between groups.

Manipulations were measured subjectively with the questions included at the end of the questionnaire. Table 16 presents the manipulation check questions. Table 17 presents the ANOVA results for the manipulation checks.

Two questions were asked to perform a manipulation check for the permission request treatment. Analysis of variance indicates that the respondents in the high permission request group (i.e., treatment group) perceived significantly higher permission requests than respondents in the low permission request group (i.e., control group), confirming that the interfaces were reviewed and understood as desired ($M_{Low} = 3.74$, $M_{high} = 4.84$, $F(1, 745) = 80.16$, $p < 0.00$).

Three questions were asked to perform a manipulation check for the privacy controls treatment. ANOVA results indicate that the treatment for privacy control was successful. Participants in the full privacy control condition reported significantly higher privacy control than those in the low privacy control condition (Privacy Control: $M_{Low} = 3.52$, $M_{High} = 4.39$, $F(1, 745) = 67.92$, $p < 0.00$).

Table 16: Manipulation Check Questions

Treatment	Manipulation Check Questions	Statistical Test
Permission request	<ul style="list-style-type: none"> I have noticed that the extent of permissions requested by this application to collect and use my personal information is significant. <i>Scale:</i> Strongly disagree_____ Strongly agree This application asks for permissions to access and use my personal information. <i>Scale:</i> Not at all _____ Very Much 	ANOVA
Privacy control	<ul style="list-style-type: none"> I have noticed that this application provides me with the privacy controls that I need to protect my personal information. <i>Scale:</i> Strongly disagree_____ Strongly agree <p>Adapted from Reed et al. 1993</p> <ul style="list-style-type: none"> I feel that I have control over the amount of personal information collected by this application. I feel that I have control over the type of personal information that is accessed by this application. <i>Scale:</i> Strongly disagree_____ Strongly agree 	ANOVA

Table 17: ANOVA Results for Manipulation Checks

Source	Sum of Squares	df	Mean Square	F	Sig.
ANOVA Results (DV: Permissions Request)					
Permission Request	72.47	1	72.47	80.16	.00
Error	673.53	745	0.90		
ANOVA Results (DV: Privacy Control)					
Privacy Control	62.33	1	62.33	67.92	.00
Error	683.67	745	0.92		

4.4.2 The Results of Hierarchical Linear Modeling

Hierarchical Linear Modeling (HLM) is a data analysis strategy in which the independent variables are entered cumulatively according to a hierarchy determined by the purpose of a study (Cohen et al. 2003). The focus of HLM is determining the model with the highest explanatory power (R^2) while finding out the partial coefficient of each variable in the equations it is included.

The common use of HLM suggests the inclusion of independent variables according to their temporal or logical priority (Cohen et al. 2003). Thus, the control variables were first introduced in the model to test for their initial effects on intention to use (Model 1). Second, the two experimental variables were included to test the impact of permission request and that of privacy control on intention in the presence control variables (Model 2). Next, privacy threat (Model 3), and benefit (Model 4) were included respectively to test for their effects on intention. Table 19 presents the specified models, including the F-values and significance of each variable as well as changes in the R^2 values.

The effects of control variables on intention: The individual effects of several control variables were first checked on intention to use. The results are presented in Table 18. Results show that a user's age, IT knowledge, motivation, average time spent on Facebook, use of Facebook applications, and general privacy concern towards using Facebook applications affect his intention to use. The results from Figure 9 suggest that the younger the respondent, the higher his intention to use. In contrast, the results from Figure 10 indicate that the higher a user's IT knowledge, the higher his intention to use. The influences of gender, education, and scenario type on intention were also tested: however, they were not found to be significant.

Table 18: The Effect of Control Variables on Intention (Independently)

Control Variable	Sum of Squares	Residual	df	Mean Square	F-Value	β	p
Age	54.48	691.52	1	54.48	58.69	-0.27	<.00
IT Knowledge	39.69	706.31	1	39.69	41.87	0.23	<.00
Motivation	128.17	617.83	1	128.17	154.55	0.41	<.00
Time on Facebook	47.80	698.19	1	47.80	51.02	0.25	<.00
Facebook App Use	119.24	626.76	1	119.24	171.73	0.40	<.00
General Concern	121.03	624.97	1	121.03	144.28	-0.40	<.00
Gender	1.68	744.32	1	1.68	1.68	0.05	.20
Education	0.05	745.96	1	0.05	0.05	-0.01	.83
Scenario Type	0.01	745.99	1	0.01	0.01	0.00	.93

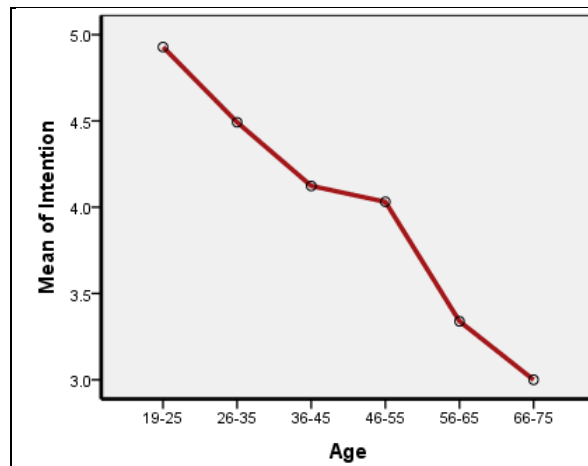


Figure 9: Age on Intention

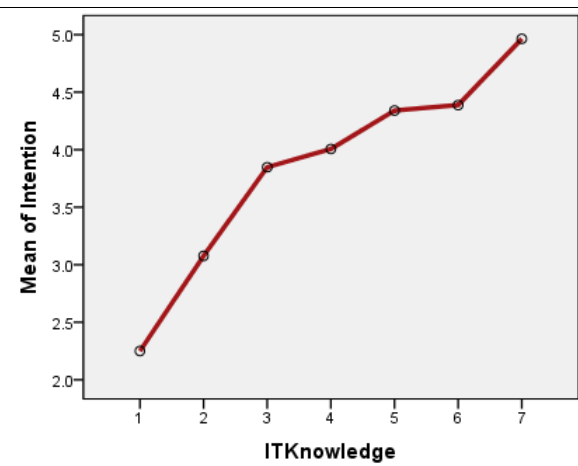


Figure 10: IT Knowledge on Intention

Table 19: The Results of Hierarchical Linear Regression

	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Intercept	(.184)	(.213)	(.218)	(.199)	(.149)	(.112)
Age	-.117** (.022)	-.125** (.022)	-.124** (.021)	-.130** (.019)	-.052* (.015)	-.052* (.014)
IT Knowledge	.077** (.025)	.066** (.025)	.057 [†] (.025)	.050 [†] (.023)	.026 (.017)	.024 (.017)
Motivation	.297** (.016)	.294** (.016)	.292** (.016)	.259** (.014)	.076** (.012)	.075** (.012)
Facebook App Use	.223** (.028)	.209** (.028)	.201** (.028)	.160** (.025)	.100** (.019)	.099** (.019)
General Concern	-.287** (.030)	-.253** (.030)	-.234** (.030)	-.002 (.033)	-.002 (.025)	-.001 (.025)
Permission Request		-.153** (.060)	-.170** (.059)	-.084** (.056)	.001 (.042)	.001 (.042)
Privacy Control			.119** (.058)	.050 [†] (.054)	.013 (.041)	.007 (.040)
Privacy Threat				-.440** (.035)	-.210** (.028)	-.178** (.029)
Benefit					.621** (.026)	.621** (.026)
Threat * Benefit						-.032 [†] (.020)
Adjusted R²	37%	40%	41%	51%	73%	73%
ΔR²=		3%	1%	10%	22%	-

Path Coefficient ^(statistical significance) (Standard Error)

** p< .01, * p<.05, p<.10[†]

As presented in Table 19, the significant control variables were introduced in **Model 1**. Control variables explained 37% of the variance in R². Next, permission request and privacy control were introduced in **Model 2** and **Model 3** respectively and they were both found to have a significant impact on intention. While permission request increased the variance in R² by 3%, privacy control increased it by another 1%.

Privacy threat was introduced in **Model 4** and found to have significant negative impact on intention. It increased the variance in R² by 10%. While the impact of general privacy concern on

intention became insignificant, the impact of privacy control and IT Knowledge became moderately significant ($p < .10$) when threat was introduced in Model 4.

Benefit was included in **Model 5**. The positive impact of benefit on intention was found to be significantly higher than those of other variables (it was almost three times more influential than privacy threat). Benefit increased the variance in R^2 by another 22%. In the presence of benefit in Model 5, both of the experimental conditions—permission request and privacy control—lost their significant effects on intention.

Finally, the threat-benefit interaction was included in **Model 6**. While the effect was found to be significant ($p < .10$), the variance in R^2 did not change. The final model explained 72% of the variance in intention to comply, with significant effects of age ($p < .05$), motivation ($p < .05$), Facebook application use ($p < .01$), privacy threat ($p < .01$), benefit ($p < .01$), and the interaction term for privacy threat and benefit ($p < .10$). The results provide empirical evidence to support Hypothesis 1, 2, and 3.

To have a deeper understanding of the effect of benefit-threat interaction on intention (H3), further analysis was conducted. Adopting a method by Escalas and Bettman (2005), the data set was split into three subsets (high, medium, and low benefit) based on plus and minus standard deviation of the mean of perceived benefit construct. Figure 11 illustrates the effect of privacy threat and benefit interaction on intention. The results indicate that privacy threat has a significant negative influence on intention when benefit is low; yet, when benefit is high or medium, privacy threat does not have any significant influence on intention ($\beta = -.05$, $\text{Err} = .02$, $p < .02$).

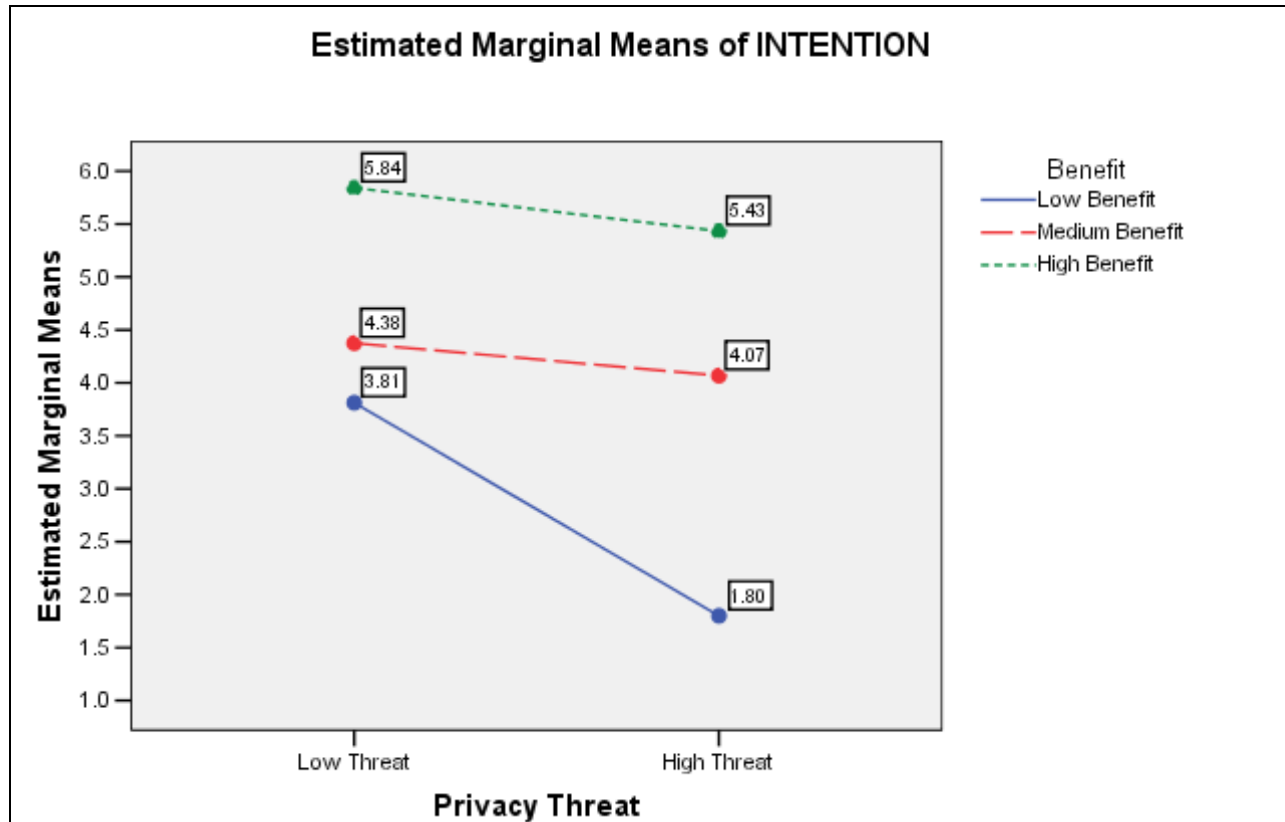


Figure 11: The Effect on Privacy Threat & Benefit Interaction on Intention

Mediation analysis: The results of the HLM analysis provided empirical support for the mediation relationship proposed in the theoretical framework. For a further investigation, the procedures suggested by Baron and Kenny (1986) were followed. The analysis procedures are presented below. The results of the mediation analysis are presented in Table 20.

- (1) The effects of IVs (i.e., requested permissions and privacy controls) on mediating variables (i.e., benefit and privacy threat) were tested independently (*Path a – Column 1*).
- (2) The effects of two mediating variables on intention were tested independently (*Path b - Column 1*).
- (3) The effects of IVs on intention were tested independently (*Path c – Column 1*).

(4) The effects of both IVs and mediating variables on intention were tested simultaneously (*Path a, b, c – Column 2*).

Table 20: Results of Mediation Analysis

Mediating Variable: Benefit					Mediating Variable: Privacy Threat			
	IV: Requested Permissions		IV: Privacy Controls		IV: Requested Permissions		IV: Privacy Controls	
	1	2	1	2	1	2	1	2
Path a	-.60**	-	.34**	-	.67**	-	-.47**	-
Path b	.82**	.81**	.82**	.81**	-.60**	-.57**	-.60**	-.58**
Path c	-.56**	-.08 [†]	.38**	.10*	-.56**	-.18**	.38**	.10 [†]
	Partial Mediation		Partial Mediation		Partial Mediation		Partial Mediation	

**p<.00, *p<.05, [†]p<.10

As presented in Table 20, all the relationships tested in procedures 1, 2, and 3 were found to be significant. Baron and Kenny (1986) suggest that if *path c* loses its significant impact when estimated simultaneously with the mediator variable for the given IV (column 1), then the proposed mediator variable fully mediates the impact of IV variables on intention. However, as presented in Table 20, if *path c* is still significant when estimated simultaneously with the mediator variable (column 2), but smaller than when it is tested independently (column 1), then the proposed mediator variable partially mediates the impact of IV variables on intention (Baron and Kenny 1986). Based on the results presented in Table 20, it is concluded that both benefit and privacy threat partially mediate the impact of IVs on intention. However, it is important to highlight that if benefit and privacy threat are introduced to the model simultaneously, both IVs lose their significant impact on intention (See Table 19).

4.4.3 The Results of ANOVA Tests

The direct effects of two experimental factors on perceived privacy threat are tested. The direct effects of these factors on benefit are also controlled (as they may also directly affect benefit in

addition to their indirect effects through privacy threat). The results of a 2X2 ANOVA test on perceived benefit and privacy threat indicate that both permission request and privacy control significantly affect these two variables. The comparisons between the groups were performed with contrast tests. The ANOVA/ANCOVA tables are presented in Table 21 and Table 22 for benefit and privacy threat.

Table 21: ANCOVA Table for Perceived Benefit

Independent Variable	Sum of Squares	Df	Mean Square	F-Value	Sig.
Permission Request	14.63	1	14.63	21.00	.00
Privacy Control	3.59	1	3.59	5.15	.02
Privacy Threat	132.30	1	132.30	189.86	.00
Error	517.76	743	0.70		

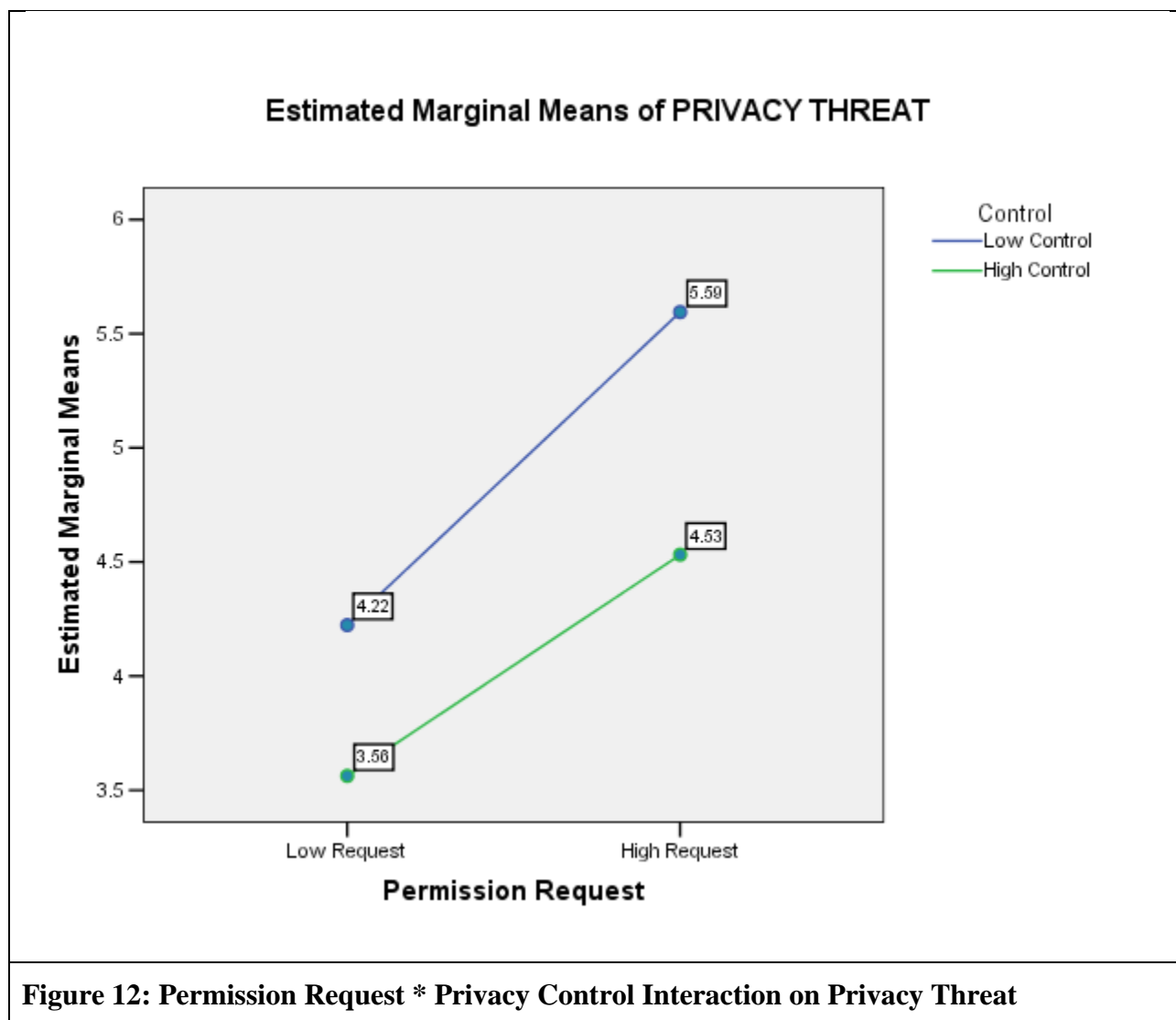
ANCOVA results (Table 21) show that, in controlling for the effects of the experimental conditions, privacy threat had a significant negative impact on benefit ($\beta = -0.47$, Std. Error = .04, $p < .00$). Thus, Hypothesis 4 was supported. While the effects of experimental conditions were not hypothesized, they were included in the analysis for statistical testing. Permission request ($\beta = -0.15$, Std. Error = .07, $p < .00$) and privacy control ($\beta = 0.07$, Std. Error = .06, $p < .05$) were both found to have significant effects on benefit.

Table 22: ANOVA Table for Perceived Privacy Threat

Independent Variable	Sum of Squares	Df	Mean Square	F-Value	Sig.
Permission Request	89.43	1	89.43	109.31	.00
Privacy Control	48.58	1	48.58	59.38	.00
Permission Request * Privacy Control	2.64	1	2.64	3.22	.07
Error	607.89	743	0.818		

ANOVA results (Table 22) indicate that respondents in the high permission request group perceived significantly higher privacy threat ($\beta = 0.35$, Std. Error = .03, $p < .00$) than those in the low permission request group, supporting Hypothesis 5. The results also showed that the

respondents in the full privacy control group perceived significantly lower privacy threat ($\beta = -0.26$, Std. Error = .03, $p < .00$) than those in the low privacy control group, so Hypothesis 6 was supported. Empirical support was also found for the impact of permission request and privacy control interaction on privacy threat. The effect of permission request on privacy threat was slightly higher for low privacy control condition than full privacy control condition ($p < .10$), so Hypothesis 7 was moderately supported. The interaction graph is presented in Figure 12.



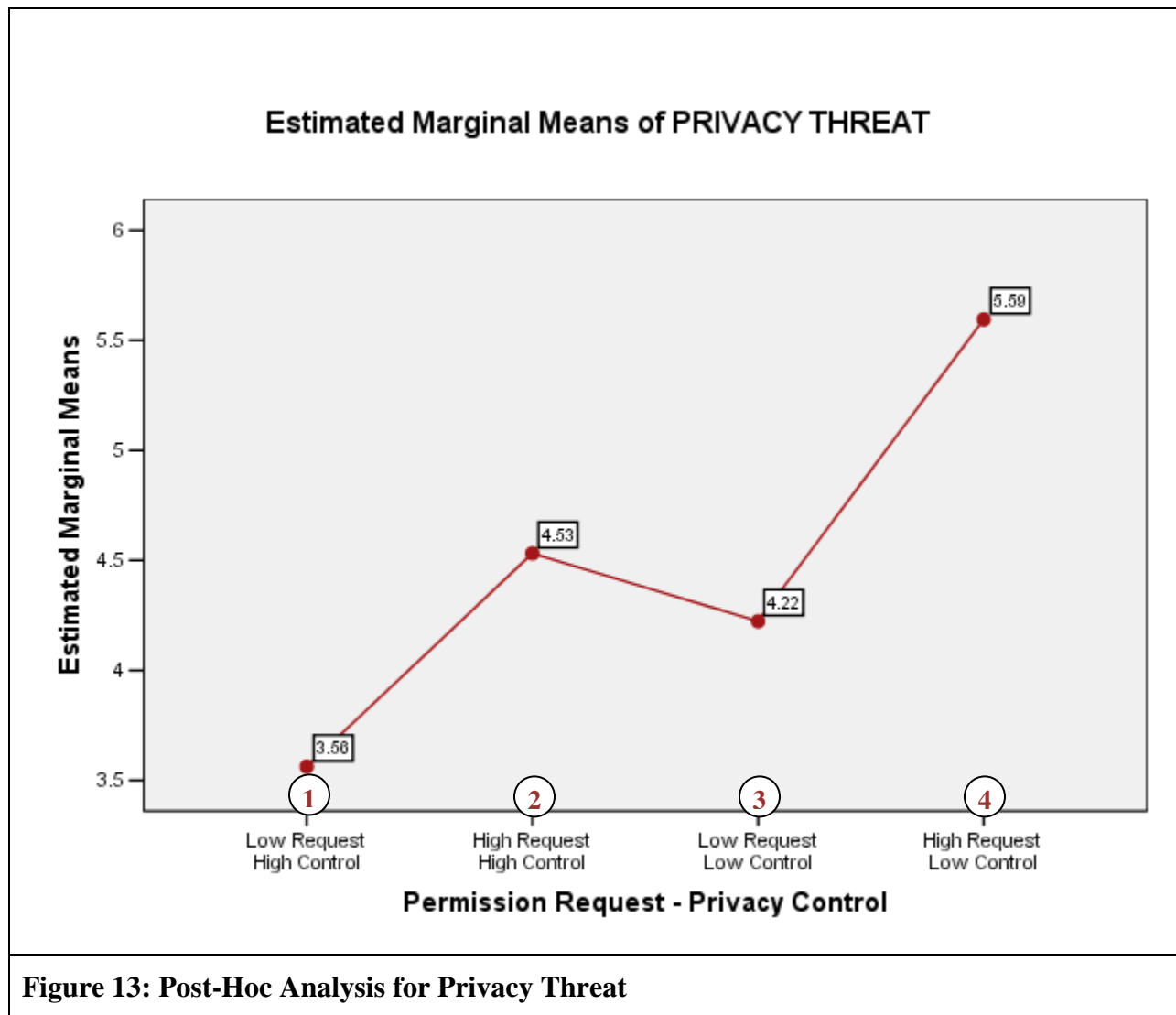
Post-Hoc Comparisons: Finally, to compare respondents' benefit and privacy threat perceptions across groups, four groups were created based on the experimental manipulations: **Group (1)** high control – low request (n = 138), **Group (2)** high control – high request (n = 200), **Group (3)** low control – low request (n = 200), **Group (4)** low control – high request (n = 209). Then, the group averages for benefit and privacy threat were compared using the ANOVA Scheffé Test. This test was preferred due to the unequal sample sizes among groups. Table 23 presents the results of the analysis. Figures 13 and Figure 14 present the mean plots for groups.

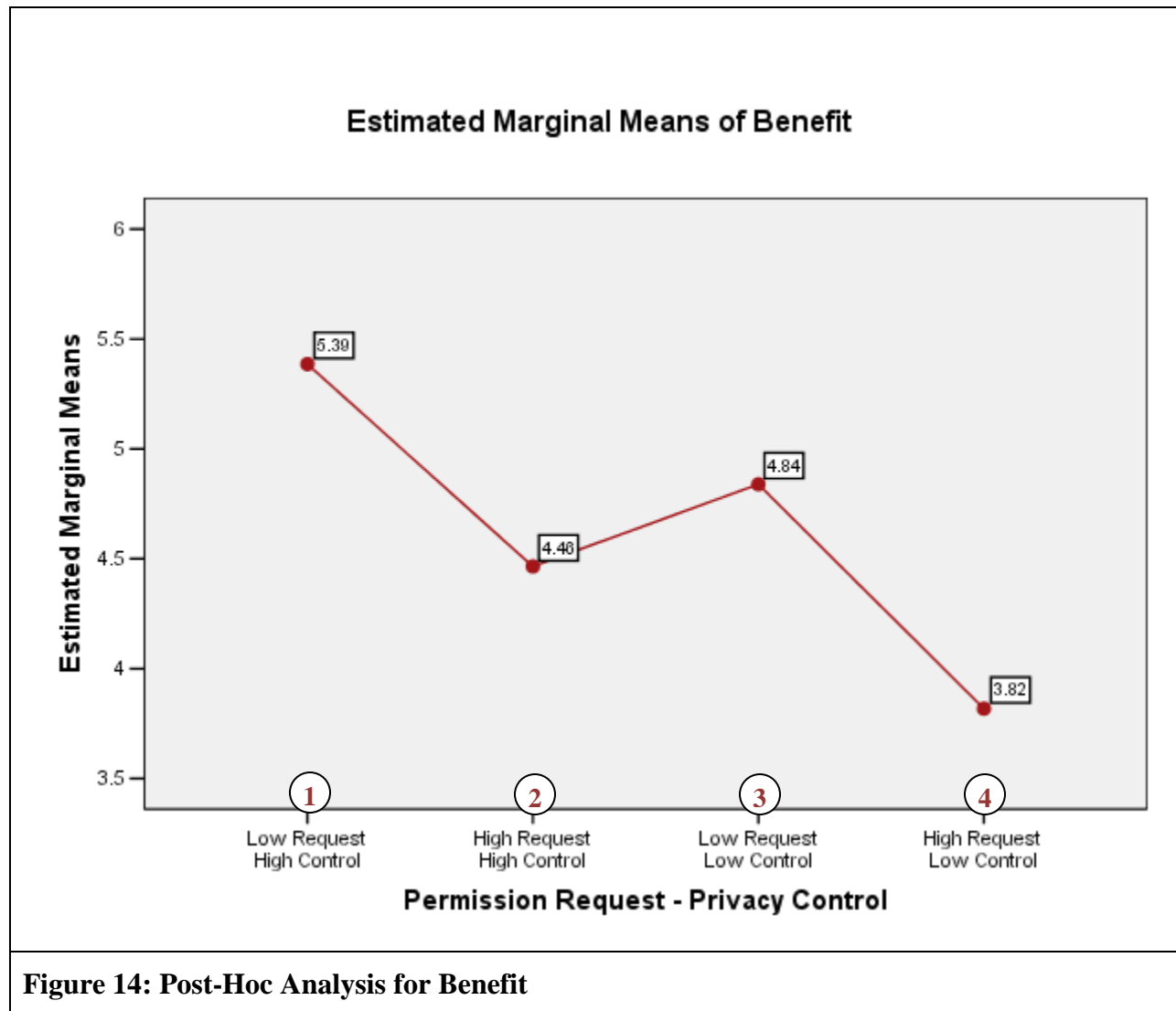
Table 23: Post-Host Test Multiple Comparisons for Benefit Privacy Threat

Comparison of Groups for Perceived Privacy Threat				
Comparison Groups		Mean Difference	Std Error	Sig.
Group 1 _{Mean = 3.56}	Group 2 _{Mean = 4.53}	-0.97	.17	.00
	Group 3 _{Mean = 4.22}	-0.66	.17	.00
	Group 4 _{Mean = 5.59}	-2.03	.17	.00
Group 2 _{Mean = 4.53}	Group 3 _{Mean = 4.22}	0.31	.15	.24
	Group 4 _{Mean = 5.59}	-1.06	.15	.00
Group 3 _{Mean = 4.22}	Group 4 _{Mean = 5.59}	-1.37	.15	.00
Comparison of Groups for Perceived Benefit				
Comparison Groups		Mean Difference	Std Error	Sig.
Group 1 _{Mean = 5.39}	Group 2 _{Mean = 4.46}	0.92	.10	.00
	Group 3 _{Mean = 3.84}	0.55	.10	.01
	Group 4 _{Mean = 3.82}	1.57	.10	.00
Group 2 _{Mean = 4.46}	Group 3 _{Mean = 4.84}	-0.37	.10	.08
	Group 4 _{Mean = 3.82}	0.65	.10	.00
Group 3 _{Mean = 4.84}	Group 4 _{Mean = 3.82}	1.02	.10	.00

Results indicate that respondents in Group 4 had the highest privacy threat perception, followed by Group 2 and Group 3. Respondents in Group 2 and Group 3 did not have significantly different privacy threat perceptions, while the rest of the group comparisons were significantly different. As expected, respondents in Group 1 had the lowest privacy threat perception.

In contrast, respondents in Group 4 had the lowest benefit perception, followed by Group 3 and Group 2. As expected, respondents in Group 1 had the highest benefit perception. Results indicate that respondents in Group 2 perceived slightly more benefit than the ones in Group 3 ($p < .10$).





4.5 Discussions and Conclusions

4.5.1 Discussion of Findings

This study examined the effects of two factors—permission request and privacy control—on a user’s benefit and privacy threat perceptions and, in turn, his intention to use a social application. Based on data collected from 746 Facebook users, all of the hypotheses were supported and strong support was found for the proposed theoretical model.

This study was particularly designed to investigate a challenge situation where a user is expected to have both high benefit and high privacy threat perceptions associated with using an application. As hypothesized, it was found that a user's benefit and privacy threat perceptions significantly influence his intention. The results particularly highlight the key effect of benefit on intention. First, it was found that benefit was almost three times more influential on intention than privacy threat. In fact, in the presence of benefit the effects of two experimental conditions—permission request and privacy control—on intention became insignificant. Second, evidence was found for the negative interaction of benefit and privacy threat on intention. The negative effect of privacy threat on intention was not significant when benefit was high.

Findings of this study offer important theoretical and practical implications. First of all, analysis of data highlighted the key effect of benefit on intention. The results imply that benefit can override the negative effect of threat on intention, so users can be extremely vulnerable to privacy threats when they perceive high benefits associated with using an OSN feature.

Consistent with the hypotheses of the proposed research model, respondents' perceived privacy threat was found to be higher in a high permission request condition than a low permission request condition, especially when they were not provided with privacy controls (i.e., a low privacy control condition). An interesting result was found when Groups 2 and 3 were compared in terms of respondents' privacy threat and benefit perceptions. In Group 2 (i.e., a low permission request and low control condition), although requested permissions were limited, users were not provided with any privacy controls to eliminate the threat. Whereas in Group 3 (i.e., a high permission request and high control condition), users were provided with a full set of privacy controls so that they could objectively eliminate perceived privacy threats. As a result,

respondents in Group 3 were *objectively* better off compared to Group 2. Nevertheless, no significant difference was found between Group 2 and Group 3 in terms of respondents' perceived privacy threat. Interestingly, we also found that respondents in Group 2 (i.e., a low permission request and low control condition) had even higher benefit perceptions compared to the ones in Group 3 (i.e., a high permission request and high control condition). These findings imply that requesting a minimum number of permissions can be the key to encouraging users to adopt an application, as providing privacy controls may not be sufficient to reduce their threat perception (or increase benefit perception) when permission request is high.

Lastly, while it was hypothesized that the manipulations on the application interface (i.e., permission request and privacy control) would only influence respondents' privacy threat perceptions, it was observed that respondents' benefit perceptions were also significantly influenced (i.e., reduced) in high permission request interfaces, especially when they were not provided with privacy controls. This is an important finding for the promotion of non-invasive applications. Requesting several permissions might in fact be fair and legitimate for some applications, as these requests can be necessary for an application to function and generate benefits (e.g., requesting cell number to send text reminders). This study, however, reports that higher permission request not only increases users' threat perceptions but also can decrease their benefit perceptions. Therefore, application designers are advised to refrain from requesting more permissions than needed as that would not only increase users' privacy threat perceptions but also decrease their benefit perceptions.

4.5.2 Limitations and Future Research

This study investigated a variance theory and has not considered the fact that a user's privacy threat and benefit perceptions would evolve over time within a process. Qualitative and/or longitudinal research is needed to provide deeper explanations of how a user's perceptions and behaviors evolve over time. The study could also be improved by investigating a user's actual behaviors and by collecting data across time for dependent and independent variables.

While it was not the focus of this study, it is expected that the studied experimental conditions—permission request and privacy control—could also affect the strategies that a user employs to cope with a privacy threat. Future research should focus on the identifying the conditions that shape a user's coping strategies and empirically study which strategies users employ in different conditions through controlled experiments.

Although this study provides insight into how the two experimental conditions—permission request and privacy control—affect a user's privacy threat perceptions, it does not explain which specific permissions are more critical in increasing privacy threat and in turn, inhibiting use intention. Further research should be conducted to understand which specific information practices (i.e., permission requests) are more influential on privacy threat. Some of the questions that can be asked are: Are all information practices the same in terms of generating privacy threats?; Would an application's access to a user's personal information (e.g., access to location information) generate more or less concern than utilization of his information (e.g., post on a user's wall regarding his location information)?; Would a user be more concerned about an application's access to his or his friends' personal information?

By simply looking at how the extent of permission requests affect a user's privacy threat and benefit perceptions, this study finds that higher permission requests increase users' threat perceptions and decrease benefit perceptions. The application in question, however, may need the requested permissions to properly function. For example, a birthday reminder application would have access to a user's friends' birthday information to develop a birthday calendar. As these permission requests can also provide significant benefits to the user, it is important to find the means to communicate the rationale of an application's requests and persuade the users that the required permissions are fair and legitimate for the functionalities provided by the application. Therefore, future research should focus on how to communicate the rationale for permission requests effectively and increase a user's benefit perceptions instead of increasing his privacy threat perceptions while asking for these permissions.

This research highlights the dominant role of a user's benefit perception over his privacy threat perception in adopting an OSN feature. The findings imply that users can be extremely vulnerable to privacy threats in an online social network setting, especially when they perceive high benefits in using an OSN feature. Future research should focus on designing new application interfaces to nudge users to be more aware and mindful about their state of vulnerability and the consequences of their actions.

While this study only manipulated the application interface to understand the factors that affect a user's privacy threat perception, further research should also find out the factors that can enhance a user's benefit perceptions. A fruitful research direction would be manipulating the important contextual information on the scenario descriptions, such as the number of friends or general social network users who already use the application and the rating of the application. The results

of such studies would guide application designers in communicating their value propositions more effectively.

5 Conclusions

5.1 Summary of the Thesis

In this thesis, first, a theory was developed to explain an OSN user's privacy threat avoidance and opportunity seeking behaviors by integrating two major literatures on coping and information privacy. Coping literature was utilized to explain processes by which an OSN user copes with a privacy threat. Privacy literature was utilized to explain factors that affect an OSN user's behavioral responses regarding information disclosure and use of an OSN feature. Also, the theory posited that information disclosure in an OSN platform may occur in three different ways: i) disclosure intended and initiated by the user, ii) disclosure unintended but initiated by the user, and iii) disclosure unintended by the user but initiated by other actors in the platform. The theory explained how disclosure situations identified would shape an OSN user's privacy threat avoidance and coping responses.

In addition, two empirical studies were conducted in this thesis. The first empirical study examined factors that influence a user's motivation to cope with privacy threats associated with using a social application. The second one examined the factors that influence a user's benefit and privacy threat perceptions associated with using a social application, and in turn, his intention to use it.

The theory and the results of the subsequent empirical studies provide answers to the research questions that initially motivated this thesis, which are as follows:

1. How does a user cope with a privacy threat in an OSN platform?

As explained by the proposed theory, an OSN user's threat avoidance (coping) behaviors—which were identified as PFC and EFC—occur as a result of two cognitive processes that constantly influence each other: ***Primary Appraisal*** and ***Secondary (Coping) Appraisal***. The theory posited that when a user perceives high control over a situation that is likely to result in a privacy threat, he will mainly employ ***PFC*** (which refers to a user's deliberate cognitive and behavioral efforts that take a problem-solving approach to alter the objective reality; e.g., changing privacy settings) whereas, when he perceives low control, he will mainly employ ***EFC*** (which refers to a user's cognitive and behavioral efforts toward creating a false perception of the environment to regulate emotional distress associated with the threat without changing the objective reality, e.g., wishful thinking). The theory also posited that information disclosure can either be intended or unintended by a user. Similarly, it can either be initiated by the user or other actors in an OSN platform. The theory discussed that different ways of disclosure would shape a user's coping and opportunity seeking behaviors differently. Most importantly, when disclosure is intended and initiated by the user, he can assess the expected consequences of using an OSN feature. If the user thinks that the negative consequences of using the feature are more critical for him compared to the positive consequences, he may decide not to use the feature. In this situation, he would not need to cope with any privacy threat. If the user decides to use the feature, depending on his perceived control over the situation, he would employ PFC or EFC behaviors. When disclosure is not intended and not initiated by the user, however, he can only be aware of the disclosure by observing the consequences of it. In such situations, the user perceives less control, and as a result, his coping motivations are expected to drop in general. He may also need to depend more on EFC.

2. *What are the factors that affect a user's motivation to cope with a privacy threat associated with a particular OSN feature (i.e., social applications)?*

Study #2 examined the effects of perceived benefit, privacy threat, and privacy threat avoidability on a user's coping motivations. The results of the study provided strong evidence that an OSN user's perceived benefit and privacy threat associated with using an OSN application, and that his perceived privacy threat avoidability positively affects his PFC and EFC motivations. It was also found that when a user's privacy threat perception is high, his PFC motivation would also be high, regardless of threat avoidability perception.

3. *What are the factors that shape a user's privacy threat perceptions, and in turn, affect his intention to use a particular OSN feature (i.e., social applications)?*

Study #3 examined the effects of permission request and privacy control on a user's privacy threat perception, and in turn, his intention to use a social application. Results revealed that while the extent of permissions requested by an application increases a user's privacy threat perception, privacy controls provided by the application decrease his privacy threat perception. Statistical analysis showed that these factors could also be influential on a user's perceived benefit associated with using an application. In return, while a user's benefit perception increases his intention to use an application, his privacy threat perception decreases it. Results also showed that the effect of perceived benefit on intention can be three times more influential than that of perceived privacy threat, and in fact, perceived benefit can override a user's perceived privacy threat associated with using a social application.

5.2 Contributions of the Thesis

The results of this thesis make several contributions to theory and practice. First, this research advances our knowledge of information privacy in the domain of OSNs. To the best of my knowledge, this thesis is the first comprehensive study in the academic literature to explain the processes that activate an OSN user's behavioral responses regarding coping and opportunity seeking (i.e., use and information disclosure). Rather than solely applying existing theories to a new setting, this research extends our knowledge by identifying different situations that may result in information disclosure in an OSN platform and explains how these differences would shape an OSN user's behavioral responses.

Second, this research provides empirical support for the significant effects of perceived benefit on an OSN user's privacy threat coping motivations. Showing that not only privacy threat but also benefit affects an OSN user's coping motivations, this research enhances our understanding of the factors that drive user behaviors in an OSN domain.

Third, this research expands the coping and information privacy literatures by examining two factors—permission request and privacy control—that affect a user's privacy threat and benefit perceptions. While a majority of the studies in the privacy literature have focused on the relationship between privacy-related concerns and behavioral outcomes, only a few studies have investigated antecedents of these concerns (Smith et. al. 2011). As a theoretical contribution to the literature, this research sheds light on two factors that drive a user's privacy threat perception.

The results of this thesis show that respondents' perceived privacy threat was found to be higher when a information related permission requests were high than low, especially when they were

not provided with privacy controls. As an important finding, when two groups of respondents—one group being asked for a low number of permissions when no privacy controls were provided and another group being asked for a high number of permissions when all privacy controls were provided—are compared, no significant difference was found in their privacy threat and benefit perceptions associated with using a social application. These findings reveal that by minimizing the number of information-related permissions requested, application developers can attract and retain more users instead of scaring them with a long list of permissions. Providing some privacy controls to their users so that they can adjust the requested permissions according to their privacy preferences would also be helpful to encourage users in adopting an application. However, requesting a minimum number of permissions can still be key to attracting more users, as providing privacy controls while requesting a large number of permissions may not be sufficient to reduce their threat perceptions. Otherwise, application developers should find means to persuade users in regards to the rationale of their permission requests.

Fifth, this research particularly highlights the key effect of benefit on intention. It was found that benefit was almost three times more influential on intention than privacy threat. In fact, when a user's benefit perception is high, it was found that privacy threat is not influential on a user's intention to use an OSN feature. The results imply that a user's benefit perception can override the negative effect of threat on intention, so users can be extremely vulnerable to privacy threats when they perceive high benefits associated with using an OSN feature. This finding can serve to inform the development of new public policies and design of privacy awareness and training programs for OSNs. Particularly, public policies that oblige technology developers to design interfaces that can inform and nudge users regarding the long term consequences of the privacy threats can be helpful to reduce users' vulnerabilities to privacy invasions.

5.3 Limitations and Suggestions for Future Research

This research has a number of limitations. First, the empirical studies in this thesis focused on understanding a use situation where disclosure is intended and initiated by a user (i.e., social applications that run on an OSN platform). However, unintended disclosure situations, especially the ones that are initiated by others, can cause larger threats to a user's information privacy.

These issues can be critical and unique, as they may only occur in social contexts. Future research should focus on developing a deeper understanding of these situations by investigating a user's privacy-related perceptions and behaviors in such situations.

Second, the proposed theoretical framework in this thesis mainly depends on well established theories on coping and information privacy. While these theories provide extensive information regarding human behavior, to better explain the novel privacy issues in unintended disclosure situations, future research should conduct qualitative research (e.g., interviews with OSN users, case studies etc.). A quantitative approach to theory testing is employed following the suggestion of Liang and Xue (2009) in this thesis, however conducting qualitative studies as future work could also be helpful in understanding the entire coping process, especially the interplay among a user's primary appraisal, secondary appraisal, and his re-appraisal of the consequences.

Third, the empirical studies which are part of this thesis examined an OSN user's behavioral intentions by using scenario-based methods rather than examining their behaviors. While measuring intentions and using scenario-based methods are well accepted in the IS literature, future research would benefit from designing field experiments to investigate actual user behaviors. Another fruitful research direction would be analysing trends in actually user behaviors using secondary data sources. For example, use patterns of a group of users of an OSN

platform, such as Facebook, can be received from the company and investigated to understand how implementation of major technology and policy changes shape users' behaviors.

Researchers can also use secondary qualitative data sources. As an example, they can analyze user comments posted on privacy policy of an OSN platform or forum discussions of a privacy advocacy group to understand their privacy-related concerns.

A few prior studies have shown that technology users' intention to use a technology and their actual behaviors can be uncorrelated (i.e., privacy paradox) (Acquisti and Grossklags 2004; Norberg et al. 2007; Sheehan and Hoy 1999), as they found that while users declare they do not intend to use a technology due to their concerns over their information privacy, in reality they do use it. In this research, however, we found that users intend to use an OSN feature although they acknowledge privacy threats associated with its use. Considering previous research on privacy paradox, it makes it even more likely that in reality, users would use an OSN feature despite their privacy concerns. This is an important finding showing that users could be extremely vulnerable to privacy-related threats. Future research should be conducted to replicate this finding with actual user behaviors.

Fourth, the data was collected in a cross-sectional fashion in both empirical studies. To make stronger causal inferences regarding the observed relationships, future studies should measure the dependent and independent variables at different points in time. For example, users' perceptions and behaviors can be measured before and after a significant event on an OSN platform, such as, major changes in privacy policies, privacy settings and controls, or technology interfaces that can affect user' privacy-related perceptions.

This research only focused on privacy at an individual level. Privacy-related behaviors in an OSN context can be shaped within different levels (e.g., group, network, organization, society). So, it can be useful to conduct multi-level research and investigate group behavior to provide a more comprehensive view of privacy (Bélanger and Crossler 2011; Smith et al. 2011).

This research does not investigate different types of behaviors that can be undertaken to cope with a privacy threat but instead frames them as a whole under PFC and EFC motivations. These motivations, however, may include various coping behaviors, such as changing privacy settings, data fabrication, withholding, etc. Future research should focus on understanding the conditions that lead to different types of coping behaviors.

Finally, this research combines several information practices in one interface and presents them as low vs. high permission requests. While this approach helps one to understand how the extent of permissions requested affects a user's privacy-related permissions in general, it cannot explain which of these practices result in more privacy concerns. An important research direction would be designing future experiments to study these permissions individually. For example, would users be more or less concerned when an application requests to access his personal information rather than his friends' information? Which of the information practices generate higher concern? For example, is information disclosure more or less problematic than information access? Does the nature of perceived privacy threat (e.g., threats with emotional, psychological, or material consequences) affect a user's behaviors? Answers to these questions would help us understand how a user's primary appraisal is shaped and thus, expand the theory proposed in Study #1. The answers would also have practical implications as they can help technology developers in understanding their users' privacy concerns and design technologies that can attract more users.

Bibliography

- Ackerman, M. S., and Mainwaring, S. D. 2012. "Privacy Issues and Human-Computer Interaction," *O'Reilly and Associates*.
- Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Lecture notes in computer science* (4258), pp: 36-58.
- Acquisti, A., and Grossklags, J. 2004. "Privacy Attitudes and Privacy Behavior," in: *Economics of Information Security*. Camp, L. J., and Lewis, S., (eds.): Kluwer Academic Publishers. pp: 165-179.
- Aiken, L. S., and G., W. S. 1991. *Multiple Regression: Testing and Interpreting Interactions*, London: Sage.
- Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50), pp: 179-211.
- Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*, Englewood Cliffs, NJ: Prentice-Hall.
- Altman, I. 1974. "Privacy: A Conceptual Analysis," in: *Man-Environment Interactions: Evaluations and Applications*. Carson, D. H., (ed.). Washington, DC: Environmental Design Research Association, pp: 3-28.
- Altman, I. 1975. *The Environment and Social Behavior*, Monterey, CA: Brooks/Cole.
- Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34: 3), pp: 613-643.
- Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33: 2), pp: 339-370.
- Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30: 1), pp: 13-28.
- Awareness. 2012. "The State of Social Media Marketing: Top Areas for Social Marketing Investment and Biggest Social Marketing Challenges in 2012," *Awareness, Inc*
- Bachman, R. P., R.; Ward, S. 1992. "The Rationality of Sexual Offending: Testing a Deterrence/ Rational Choice Conception of Sexual Assault," *Law and Society Review* (26: 2), pp: 343-372.
- Bagozzi, R. P. 1982. "A Field Investigation of Causal Relations among Cognitions, Affect, Intentions, and Behavior," *Journal of Marketing Research* (19: 4), pp: 562-583.
- Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavior Change," *Psychological Review* (84), pp: 191-215.
- Bandura, A. 1982. "Self-Efficacy Mechanism in Human Agency," *American Psychologist* (37), pp: 122-147.
- Bansal, G., Zahedi, F. M., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49: 2), pp: 138-150.

- Baron, R. M., and Kenny, D. A. 1986. "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic and Statistical Considerations," *Journal of Personality and Social Psychology* (51: 6), pp: 1173-1182.
- Baskerville, R. 1991a. "Risk Analysis as a Source of Professional Knowledge," *Computer & Security* (10: 8), pp: 749-764.
- Baskerville, R. 1991b. "Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security," *European Journal of Information Systems* (1: 2), pp: 121-130.
- Beaudry, A., and Pinsonneault, A. 2005. "Understanding User Responses to Information Technology: A Coping Model of User Adaptation," *MIS Quarterly* (29: 3), pp: 493-524.
- Begley, T. M. 1998. "Coping Strategies as Predictors of Employee Distress and Turnover after an Organizational Consolidation: A Longitudinal Analysis," *Journal of Occupational and Organizational Psychology* (71), pp: 305-329.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35: 4), pp: 1017-A1036.
- Boyd, d. 2008. "Facebook's Privacy Trainwreck," *Convergence: The International Journal of Research into New Media Technologies* (14: 1), pp: 13-20.
- Boyd, D. M., and Ellison, N. B. 2008. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13: 1), pp: 210-230.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010a. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34: 3), pp: 523-A527.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010b. "Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook," in *Proceedings of the International Conference on Information Systems*, St. Louis, USA, pp: 1-11.
- Cartwright, S., and Cooper, C. L. 1996. "Coping in Occupational Settings," in: *Handbook of Coping: Theory, Research, Applications*. Zeidner, M., and Endler, N. S., (eds.). Oxford, England: John Wiley & Sons. pp: 202-220.
- Chellappa, R., and Sin, R. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6), pp: 181-202.
- Chin, W. W. 1998. "Commentary: Issues and Opinion on Structural Equation Modeling," *MIS Quarterly* (22: 1), pp: vii-xvi.
- Cohen, P., Cohen, J., West, S. G., and Aiken, L. S. 2003. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, Mahwah, NJ: Lawrence Erlbaum Associates Publishers.
- Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19: 2), pp: 189-211.
- Cranor, L. F., Reagle, J., and Ackerman, M. S. 2000. "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," in: *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy* Vogelsang, I., and Compaine, B. M., (eds.): The MIT Press. pp: 47-70.
- Culnan, M. J. 1993. ""How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17: 3), pp: 341-363.

- Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10: 1), pp: 104-115.
- Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59: 2), pp: 323-342.
- Darcy, J. H., A.; Galletta, D. F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research in Organizational Behavior* (20: 1), pp: 79-98.
- Debatin, B., Lovejoy, J. P., Horn, A.-K., and Hughes, B. N. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* (15: 1), pp: 83-108.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy Calculus Model in E-Commerce - a Study of Italy and the United States," *European Journal of Information Systems* (15: 4), pp: 389-402.
- Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences," *Information Systems Journal* (19: 4), pp: 391-412.
- Dinev, T., and Hart, P. 2004. "Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model," *Behaviour & Information Technology* (23: 6), pp: 413-422.
- Dinev, T., and Hart, P. 2005. "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," *International Journal of Electronic Commerce* (10: 2), pp: 7-29.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17: 1), pp: 61-80.
- Donath, J., and Boyd, D. 2004. "Public Displays of Connection," *BT Technology Journal* (22: 4), pp: 71-82.
- Dwyer, C., Hiltz, S. R., and Passerini, K. 2007. "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and Myspace," in *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, Colorado.
- Egelman, S., Tsai, J., and Cranor, L. F. A., Alessandro. 2009. "Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators," in *Proceedings of the 27th international conference on human factors in computing systems*, New York, NY.
- Ellison, N. B., Steinfield, C., and Lampe, C. 2007. "The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites," *Journal of Computer-Mediated Communication* (12: 4), pp: 1143-1168.
- Fadel, K. J., and Brown, S. A. 2010. "Information Systems Appraisal and Coping: The Role of User Perceptions," *Communications of the Association for Information Systems* (26: 1), pp: 107-126.
- Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59: 4), pp: 451-474.
- Fishbein, M., and Ajzen, I. . 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, MA: Addison-Wesley.
- Fiske, S. T. 1980. "Attention and Weight in Person Perception: The Impact of Negative and Extreme Behavior," *Journal of Personality and Social Psychology* (38: 6), pp: 889-906.

- Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., and Gruen, R. J. 1986. "Dynamics of a Stressful Encounter: Cognitive Appraisal, Coping, and Encounter Outcomes.," *Journal of Personality and Social Psychology* (50: 5), pp: 992-1003.
- Gates, G. 2010. "Facebook Privacy: A Bewildering Tangle of Options." The New York Times. New York: The New York Times.
- Gerstein, R. 1978. "Intimacy and Privacy," *Ethics and Information Technology* (89: 1), pp.76-81.
- Gerstein, R. 1984. "Intimacy and Privacy," in: *Philosophical Dimensions of Privacy*. Schoeman, F., (ed.). Cambridge: Cambridge University Press. pp: 265-271.
- Govani, T., and Pashley, H. 2005. "Student Awareness of the Privacy Implications When Using Facebook." Privacy Policy, Law, and Technology Course: Carnegie Mellon University.
- Hamilton, D. L., and Huffman, L. J. 1971. "Generality of Impression Formation Processes for Evaluative and Nonevaluative Judgments," *Journal of Personality and Social Psychology* (20: 2), pp: 200-207.
- Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24: 2), pp: 13-42.
- Hann, I.-H., Hui, K.-L., Lee, T. S., and Png, I. P. L. 2002. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off," in *Proceedings of the Twenty-Third International Conference on Information Systems*, Barcelona, Spain.
- Herath, T., and Rao, H. G. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18: 2), pp: 106-125.
- Hine, C., and Eve, J. 1998. "Privacy in the Marketplace," *Information Society* (14: 4), pp: 253-262.
- Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9: 1), pp: 50-60.
- Hoy, M. G., and Milne, G. 2010. "Gender Differences in Privacy-Related Measures for Young Adult Facebook Users," *Journal of Interactive Advertising* (10: 2), pp: 28-45.
- Hui, K.-L., Hock Hai, T., and Sang-Yong Tom, L. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31: 1), pp: 19-33.
- ITU. 2012. "Trends in Telecommunication Reform 2012," *International Telecommunication Union*, Geneva, Switzerland.
- Janz, N. K., and Becker, M. H. 1984. "The Health Belief Model: A Decade Later," *Health Education Quarterly* (11: 1), pp: 1-45.
- Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods and Research* (34: 3), pp: 334-423.
- Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34: 3), pp: 549-A544.
- Johnston, A. C., Warkentin, M., and Luo, X. 2009. "National Culture and Information Privacy: The Influential Effects of Individualism and Collectivism on Privacy Concerns and Organizational Commitment," in *Proceedings of the International Federation of Information Processing (IFIP) International Workshop on Information Systems Security Research*, Cape Town, South Africa, pp: 88-104.
- Jones, H., and Soltren, J. H. 2005. "Facebook: Threats to Privacy."
- Justice, E. 2007. "Facebook Suicide: The End of a Virtual Life."

- Kim, S. K., and Hsieh, P.-H. 2003. "Interdependence and Its Consequences in Distributor-Supplier Relationships: A Distributor Perspective through Response Surface Approach," *Journal of Marketing Research* (40: 1), pp: 101-112.
- Klepper, S. N., D. 1989. "The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited," *Criminology* (27: 4), pp: 721-746.
- Korzaan, M., Brooks, N., and Greer, T. 2009. "Demystifying Personality and Privacy: An Empirical Investigation into Antecedents of Concerns for Information Privacy," *Journal of Behavioral Studies in Business* (1), pp: 1-17.
- Krasnova, H., Günther, O., Spiekermann, S., and Koroleva, K. 2009. "Privacy Concerns and Identity in Online Social Networks," *Identity in the Information Society* (2: 1), pp: 39-63.
- Krasnova, H., and Veltri, N. F. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA," in *Proceedings of the* pp: 1-10.
- Krasnova, H. Spiekermann, S., Koroleva, K., Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25: 2), pp: 109-125.
- Kyngäs, H., Mikkonen, R., Nousiainen, E. M., Ryttilähti, M., Seppänen, P., Vaattovaara, R., and Jämsä, T. 2001. "Coping with the Onset of Cancer: Coping Strategies and Resources of Young People with Cancer," *European Journal of Cancer Care* (10: 1), pp: 6-11.
- Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33: 3), pp: 22-42.
- Lazarus. 1993. "Coping Theory and Research: Past, Present, and Future," *Psychosomatic medicine* (55: 3), pp: 234.
- Lazarus, R. S. 1966. *Psychological Stress and the Coping Process*, New York: McGraw-Hill.
- Lazarus, R. S., and Folkman, S. 1984. *Stress, Appraisal, and Coping*, New York: Springer Publishing Company.
- Lazarus, R. S., and Launier, R. 1978. "Stress-Related Transactions between Person and Environment," in: *Perspectives in Interactional Psychology*. Pervin, L. A., and Lewis, M., (eds.). New York: Plenum. pp: 287-327.
- Li, H., Sarathy, R., and Xu, H. 2010. "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems* (51: 1), pp. 62-71.
- Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems*, pp.1-11.
- Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33: 1), pp: 71-90.
- Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11: 7), pp: 394-413.
- Lu, Y., Tan, B. C. Y., and Hui, K.-L. 2004. "Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits," in *Proceedings of the International Conference on Information Systems*, Washington, DC, USA, pp.
- Lwin, M., Wirtz, J., and Williams, J. D. 2007. "Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective," *Journal of the Academy of Marketing Science* (35: 4), pp: 572-585.
- Madden, M., and Zickuhr, K. 2011. "65% of Online Adults Use Social Networking Sites, and Most Describe Their Experiences in Positive Terms.," *Pew Research Center*, Washington, D.C.

- Malhotra, N. K., Sung, S. K., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15: 4), pp: 336-355.
- Marett, K., McNab, A. L., and Harris, R. B. 2011. "Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory," *AIS Transactions on Human-Computer Interaction* (3: 3), pp: 170-188.
- Margulis, S. T. 2003a. "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues* (59: 2), pp: 411-429.
- Margulis, S. T. 2003b. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59: 2), pp: 243-261.
- McCrae, R. R. 1984. "Situational Determinants of Coping Responses: Loss, Threat, and Challenge," *Journal of Personality and Social Psychology* (46: 4), pp: 919-928.
- Milne, G. R. 2000. "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue," *Journal of Public Policy & Marketing* (19: 1), pp: 1-6.
- 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 (John Wiley & Sons)* (18: 3), pp: 15-29.
- Milne, G. R., and Gordon, M. E. 1993. "Direct Mail Privacy-Efficiency Trade-Offs within an Implied Social Contract Framework," *Journal of Public Policy & Marketing* (12: 2), pp: 206-215.
- Milne, G. R., and Rohm, A. J. 2000. "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy & Marketing* (19: 2), pp: 238-249.
- Miyazaki, A. D., and Fernandez, A. 2000. "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing* (19: 1), pp: 54-61.
- Miyazaki, A. D., and Fernandez, A. 2001. "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *Journal of Consumer Affairs* (35: 1), pp: 27.
- Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2: 3), pp: 192-222.
- Nielsen. 2011. "State of the Media: The Social Media Report," *McKinsey Company*,
- Norberg, P. A., and Horne, D. R. 2007. "Privacy Attitudes and Privacy-Related Behavior," *Psychology & Marketing* (24: 10), pp: 829-847.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs* (41: 1), pp: 100-126.
- Nowak, G. J., and Phelps, J. 1992. "Understanding Privacy Concerns. An Assessment of Consumers' Information-Related Knowledge and Beliefs.," *Journal of Direct Marketing* (6: 4), pp: 28-39.
- Nowak, G. J., and Phelps, J. 1995. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters," *Journal of Direct Marketing* (9: 3), pp: 46-60.
- Nowak, G. J., and Phelps, J. 1997. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters," *Journal of Direct Marketing* (11: 4), pp: 94-108.

- O'Fallon, M., and Butterfield, K. 2005. "A Review of the Empirical Ethical Decision-Making Literature: 1996–2003," *Journal of Business Ethics* (59: 4), pp: 375-413.
- Okazaki, S., Li, H., and Hirose, M. 2009. "Consumer Privacy Concerns and Preference for Degree of Regulatory Control," *Journal of Advertising* (38: 4), pp: 63-77.
- Park, C. L. 1993. "Religious and Nonreligious Coping with the Death of a Friend," *Cognitive therapy and research* (17: 6), pp: 561-577.
- Paternoster, R., and Pogarsky, G. 2009. "Rational Choice, Agency and Thoughtfully Reflective Decision Making: The Short and Long-Term Consequences of Making Good Choices," *Journal of Quantitative Criminology* (25: 2), pp: 103-127.
- Paternoster, R. S., L. F.; Waldo, G. P.; Chiricos, T. G. 1982. "Perceived Risk and Deterrence: Methodological Artifacts in Perceptual Deterrence Research," *Journal of Criminal Law and Criminology* (73: 3), pp: 1238-1258.
- Pavlou, P. A., Huigang, L., and Yajiong, X. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal--Agent Perspective," *MIS Quarterly* (31: 1), pp: 105-136.
- Phelps, J. E., D'Souza, G., and Nowak, G. J. 2001. "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation," *Journal of Interactive Marketing (John Wiley & Sons)* (15: 4), pp: 2-17.
- Phelps, J. E., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19: 1), pp: 27-41.
- Piquero, A., and Tibbetts, S. 1996. "Specifying the Direct and Indirect Effects on Low Self-Control and Situational Factors in Offenders Decision Making: Toward a More Comparative Model of Rational Offending; ," *Justice Quarterly* (13: 3), pp: 481.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88: 5), pp: 879-903.
- Poll, S. 2010. "60% of Facebook Users Consider Quitting over Privacy."
- Reed, G. M., Taylor, S. E., and Kemeny, M. E. 1993. "Perceived Control and Psychological Adjustment in Gay Men with Aids1," *Journal of Applied Social Psychology* (23: 10), pp: 791-824.
- Reid, G. J., Gilbert, C. A., and McGrath, P. J. 1998. "The Pain Coping Questionnaire: Preliminary Validation," *Pain* (76), pp: 83–96.
- Rippetoe, P. A., and Rogers, R. W. 1987. "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat," *Journal of Personality and Social Psychology & Marketing* (52: 3), pp: 596-604.
- Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91), pp: 93-114.
- Rosenblum, D. 2007. "What Can Anyone Know: The Privacy Risk of Social Networking Sites," *IEEE Security and Privacy* (5: 3), pp: 40-49.
- Rosenstiel, A. K., and Keefe, F. J. 1983. "The Use of Coping Strategies in Chronic Low Back Pain Patients: Relationship to Patient Characteristics and Current Adjustment," *Pain* (17: 1), pp: 33-44.
- Rosenthal, R., and Rosnow, R. L. 1984. *Essentials of Behavioral Research*, New York: McGraw Hill Book Company.

- Rosenthal, S. L., Biro, F. M., Cohen, S. S., Succop, P. A., and Stanberry, L. R. 1995. "Strategies for Coping with Sexually Transmitted Diseases by Adolescent Females," *Adolescence* (30: 119), pp: 655-666.
- Sheehan, K. B. 2002. "Toward a Typology of Internet Users and Online Privacy Concerns," *Information Society* (18: 1), pp: 21-32.
- Sheehan, K. B., and Hoy, M. G. 1999. "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns," *Journal of Advertising* (28: 3), pp: 37-51.
- Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing* (19: 1), pp: 62-73.
- Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34: 3), pp: 487-A412.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35: 4), pp: 980-A927.
- Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20: 2), pp: 167-196.
- Solove, D. J. 2002. "Conceptualizing Privacy," *California Law Review* (90:), pp: 1087-1156.
- Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154: 3), pp: 477-560.
- Son, J.-Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32: 3), pp: 503-529.
- Stewart, K. A., and Segars, A. H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13: 1), pp: 36-49.
- Stone, E., and Stone, D. 1990. "Privacy in Organizations: Theoretical Issues, Research findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8), pp: 349-411.
- 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.
- Survey. 2009. "Social Networking and Reputational Risk in the Workplace", *Deloitte*.
- Tyre, M. J., and Orlikowski, W. J. 1994. "Windows of Opportunity: Temporal Patterns of Technological Adaptation in Organizations," *Organization Science* (5: 1), pp: 98-118.
- Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7: 6), pp: 415-443.
- Vroom, V. H. 1964. *Work and Motivation*, New York: Wiley.
- Weber, J. 1992. "Scenarios in Business Ethics Research: Review, Critical Assessment, and Recommendations," *Business Ethics Quarterly* (2: 2), pp: 137-160.
- Weinstein, N. D. 1993. "Testing Four Competing Theories of Health-Protective Behavior," *Health Psychology* (12: 4), pp: 324-333.
- Weinstein, N. D. 2000. "Perceived Probability, Perceived Severity, and Health-Protective Behavior," *Health Psychology* (19: 1), pp: 65-74.
- Westin, A. F. 1967. *Privacy and Freedom*, New York: Atheneum.
- White, T. B. 2004. "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology* (14: 1/2), pp: 41-51.

- Wirtz, J., Lwin, M. O., and Williams, J. D. 2007. "Causes and Consequences of Consumer Online Privacy Concern," *International Journal of Service Industry Management* (18: 4), pp: 326-348.
- Xiao, B. 2010. Product-Related Deceptive Information Practices in B2c E-Commerce: Formation, Outcomes, and Detection. Vancouver: University of British Columbia.
- Xu, H. 2007. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," in *Proceedings of the International Conference on Information Systems*, Montreal, Canada, pp. 1-14.
- Xu, H., Dinev, T., Smith, J. H., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12: 12), pp. 798-824.
- Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2009. "The Role of Push--Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26: 3), pp: 135-173.
- Xue, Y., Liang, H., and Wu, L. 2010. "Punishment, Justice, and Compliance in Mandatory It Settings," *Information Systems Research* pp: 1-17.
- Zhang, N. A., Wang, C. A., and XU, Y. 2011. "Privacy in Online Social Networks," in *Proceedings of the International Conference on Information Systems*, Shanghai, China, pp. 1-21.

Appendices

Appendix A: Supporting Material for Chapter 3

Appendix A1: Hypothetical Scenarios and Graphical Interfaces

Description of Scenario 1: City Spot

John and his wife are business professionals who live in New York. They have an active social life. They like to go out several nights a week to have dinner and/or drinks with their friends, see music and dance shows at different music clubs of New York, watch sports games etc.

Tonight, John is at a restaurant with his wife. While they are ordering their meals, the waiter tells John and his wife that if they check in to their restaurant using an application called ‘City Spot’ on Facebook, the restaurant will offer them 30% off their total bill or two entrees for the price of one. After doing some research, John learns that it is a free application that is launched to let people search and receive great deals from many local businesses (e.g., individual deals for a discount, free merchandise or other rewards; friend deals, which you and your friends claim together; loyalty deals for being a frequent visitor; and charity deals whereby businesses pledge to donate to a cause when you check in) and share those deals with their friends.

The application runs on mobile devices such as smart phones (i.e., iPhones or Android phones) and users check in at venues by selecting from a list of venues that the application locates in the nearby area. John has a smart phone that would allow him to do so if he likes.

John certainly would like to receive a discount on the bill. He also realizes that using this application could let the family save considerable amounts of money every week since most of the places they regularly visit do offer exciting weekly deals. He already logs into his Facebook account very often and spends a significant amount of time on the site. John notices that 23 of his friends are already using this application and that he could invite other friends to use it. Overall, John thinks this might be a good way to find out about the deals in New York and benefit from them.

John also realizes that he would have to authorize the application on Facebook to be able to use it. When John clicks on the invitation link, the application requests his permission to take several actions and to access some of his personal information on Facebook. John is not very happy about every request of the application and wonders if he could do something about it. Please see the box below for the requested permissions.

Imagine that you are John and answer the following questions considering the scenario given and the application interface provided below (please see the box with the application’s requests for permission).

Description of Scenario 2: Whole Ancestry

John knows that his great-grandparents and their extended families immigrated to United States from Southern Italy between the years 1910 and 1940. John only knows that the majority of the family immigrated to the southern states around the 1910s to escape from World War I, and that the rest of the family followed after the 1920s and immigrated to different parts of the States. Because of his deep interest in learning the story of his family, John made several searches on the Internet but could not find out much.

One day, John receives an invitation from a friend to use an application called ‘Whole Ancestry’ on Facebook. After doing some research, John learns that it is a free application that allows its subscribers to build a family tree and get in touch with members of their families, not only those they already know, but also distant ones whom they may not know. The application provides easy access to more than 4.2 billion names from worldwide collections of family history records, including more than 158 million digitized images, 300 million names from death records, 100 million pages of newspapers, 75 million names from military records, 5 million names from passenger and immigration lists, 8,000 yearbooks from high schools, colleges, and military schools, and many others. Whole Ancestry continues to digitize and publish tens of millions of historical family records online each month.

John certainly would like to learn more about his family. He already logs into his Facebook account very often and spends a significant amount of time on the site. John notices that 23 of his friends are already using this application and he could invite other friends (i.e., family members) to use it if he chooses to add them to his family tree. Overall, John thinks that using this application could help him search for distant family members and connect with them.

John also realizes that he would have to authorize the application on Facebook to be able to use it. When John clicks on the invitation link, the application requests his permission to take several actions and to access some of his personal information on Facebook. John is not very happy about every request of the application and wonders if he could do something about it. Please see the box below for the requested permissions.

Imagine that you are John and answer the following questions considering the scenario given and the application interface provided below (please see the box with the application’s requests for permission).

Description of Scenario 3: Site Share

John has recently moved to New York for a new job. He used to have a very active social life as he was going out several nights a week to have dinner and/or drinks with his friends, to see music and dance shows at different music clubs, and to watch sports games. While John currently does not have any friends in this new city, he would like to make new friends and socialize as he used to do.

One day, John receives an invitation from a new colleague to use an application called ‘Site Share’ on Facebook. After doing some research, John learns that it is a free application that allows its users to share the experiences they’ve had with local businesses, and lets business owners share information about their business with Site Share’s users. For example, Site Share provides local search capabilities (e.g., one can search for a hair salon in a specific neighborhood), ratings for businesses, and user reviews. Site Share also implements a reputation system for each of its site members. This allows a Site Share user to browse through ratings and reviews of the most popular and respected users. Based on his research, John also realizes that he could personalize the reviews based on his social network and screen out those reviewers who do not share his interests so that he could focus solely on relevant recommendations.

The application also runs on mobile devices such as smart phones (i.e., iPhones or Android phones) and offers the same functionalities on-the-go so that users may share their whereabouts with their friends, see who’s nearby, and discover new places in the neighbourhood. John has a smart phone that would allow him to search for information if he likes.

John certainly would like to learn about the venues and the people in this new city. He already logs into his Facebook account very often and spends a significant amount of time on the site. John also notices that 23 of his friends are already using this application and that he could invite other friends to use it. Overall, John thinks this might be a good way to find out about the new venues and interact with new people.

John also realizes that he has to authorize the application on Facebook to be able to use it. When John clicks on the invitation link, the application requests his permission to take several actions and to access some of his personal information on Facebook. Please see the box below for the requested permissions.

Imagine that you are John and answer the following questions considering the scenario given and the application interface provided below (please see the box with the application’s requests for permission).

Description of Scenario 4: Healthy Living

John has been smoking, eating mostly unhealthy foods, and was not physically active in the past ten years. After luckily surviving a severe heart attack, he decided to visit a doctor and learned that he is considered obese. He has been advised to lose at least 25 percent of his body fat. John decides to lose weight and quit smoking under the control of doctors and dieticians to be able to avoid future health-related problems; however he certainly feels that he would need motivation and peer support during this transformation.

One of his friends recommends that John use an application called ‘Healthy Living’ on Facebook. After doing some research, John learns that it is a free application that offers expert content on diet, nutrition, fitness, wellness, and lifestyle to inform and empower its users, enable them transform smart food choices into natural habits, and overall make it easier to live better and healthier lives. Some of the core functionalities of the application include a food diary, fitness and exercise diary, motivation articles, healthy diet recipes, calorie, weight and nutrition goal charts, a quit coach, and community support. For example, the application provides a comprehensive food and fitness tracker leveraging the largest online food and fitness database through MyPlate – a tracking tool that presents the nutrition value of the food eaten, calories burned during exercise, calories to be burned to reach a target weight in daily, monthly, and yearly reports. The application also empowers members to quit smoking through MyQuit Coach – a smoking cessation tool offering a personalized quitting plan, while also providing support and encouragement from social circles, and engaging the community through challenges that encourage short-term and long-term healthy living changes. The application also provides a large database of recipes with healthy meal options. Recipes allow members to create and share food options based on dietary preference while still providing detailed nutrition data. Most importantly, the platform serves as a platform for community members to connect, inform, and inspire. Throughout the site, members are encouraged to interact with each other in Groups and Forums, where they can share their goals and experiences.

The application also runs on mobile devices such as smart phones (i.e., iPhones or Android phones) and offers the same functionality on-the-go so that users may check their food preferences while eating outside or grocery shopping, and even ask for peers’ opinions. John has a smart phone that would allow him to do so if he likes.

John certainly would like to change his habits to feel healthier. He already logs into his Facebook account very often and spends a significant amount of time on the site. John notices that 23 of his friends are already using this application and he could invite other friends to use it if he wants them to be involved in his local social support network. Overall, John thinks this might be a good way to keep track of his health and get the social support he needs.

John also realizes that he would have to authorize the application on Facebook to be able to use it. When John clicks on the invitation link, the application requests his permission to take several actions and to access some of his personal information on Facebook. John is not very happy about every request of the application and wonders if he could do something about it. Please see the box below for the requested permissions.

Imagine that you are John and answer the following questions considering the scenario given and the application interface provided below (please see the box with the application's requests for permission).

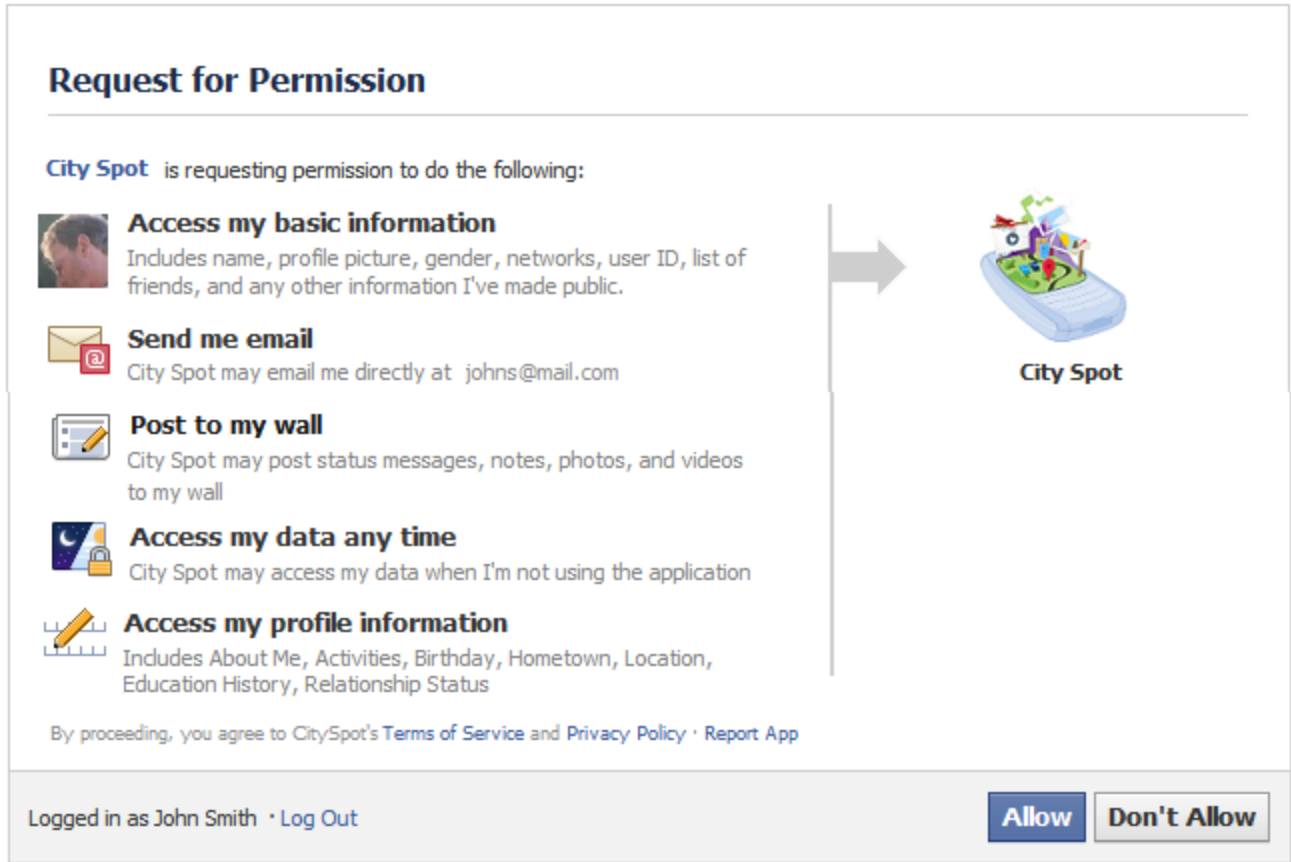


Figure 15: Application Interface for Scenario 1: City Spot

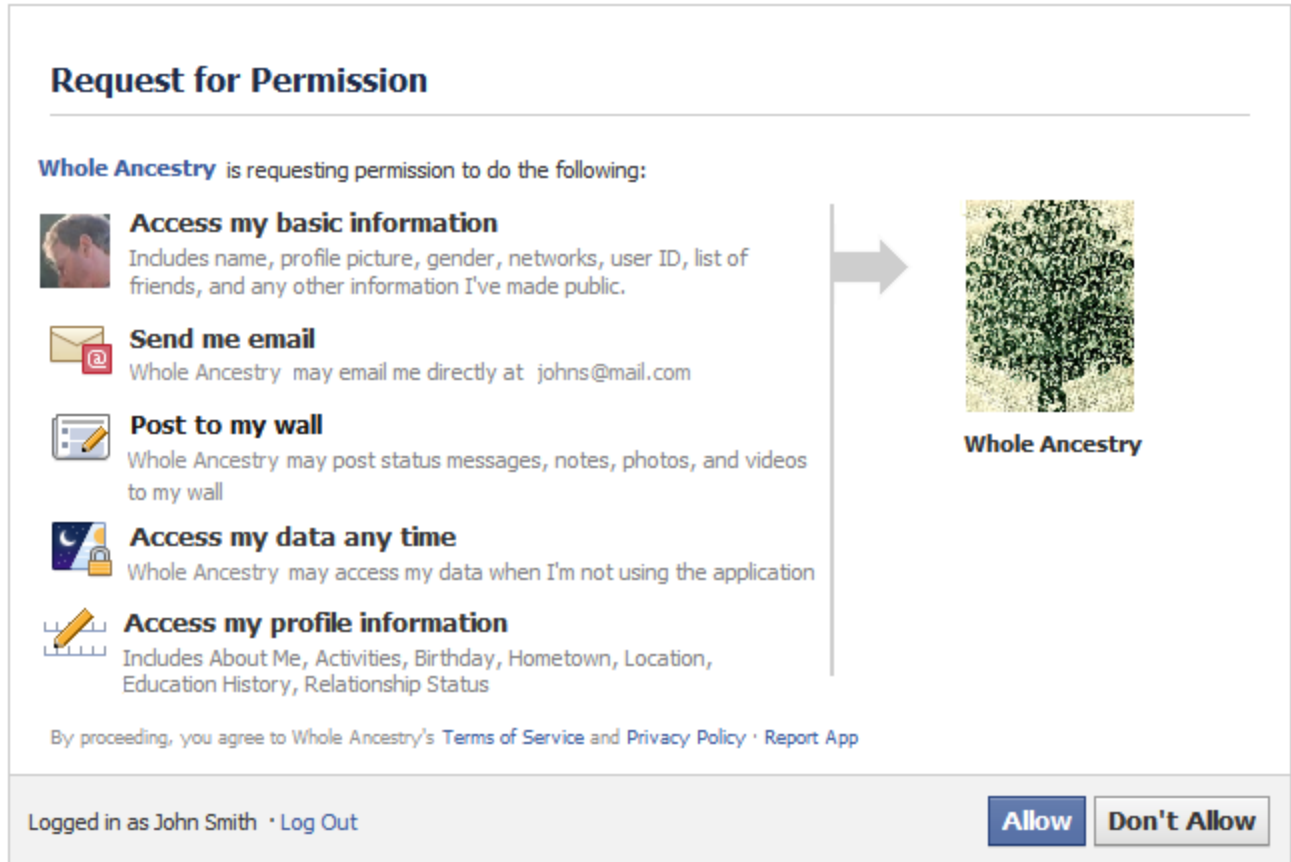


Figure 16: Application Interface for Scenario 2: Whole Ancestry

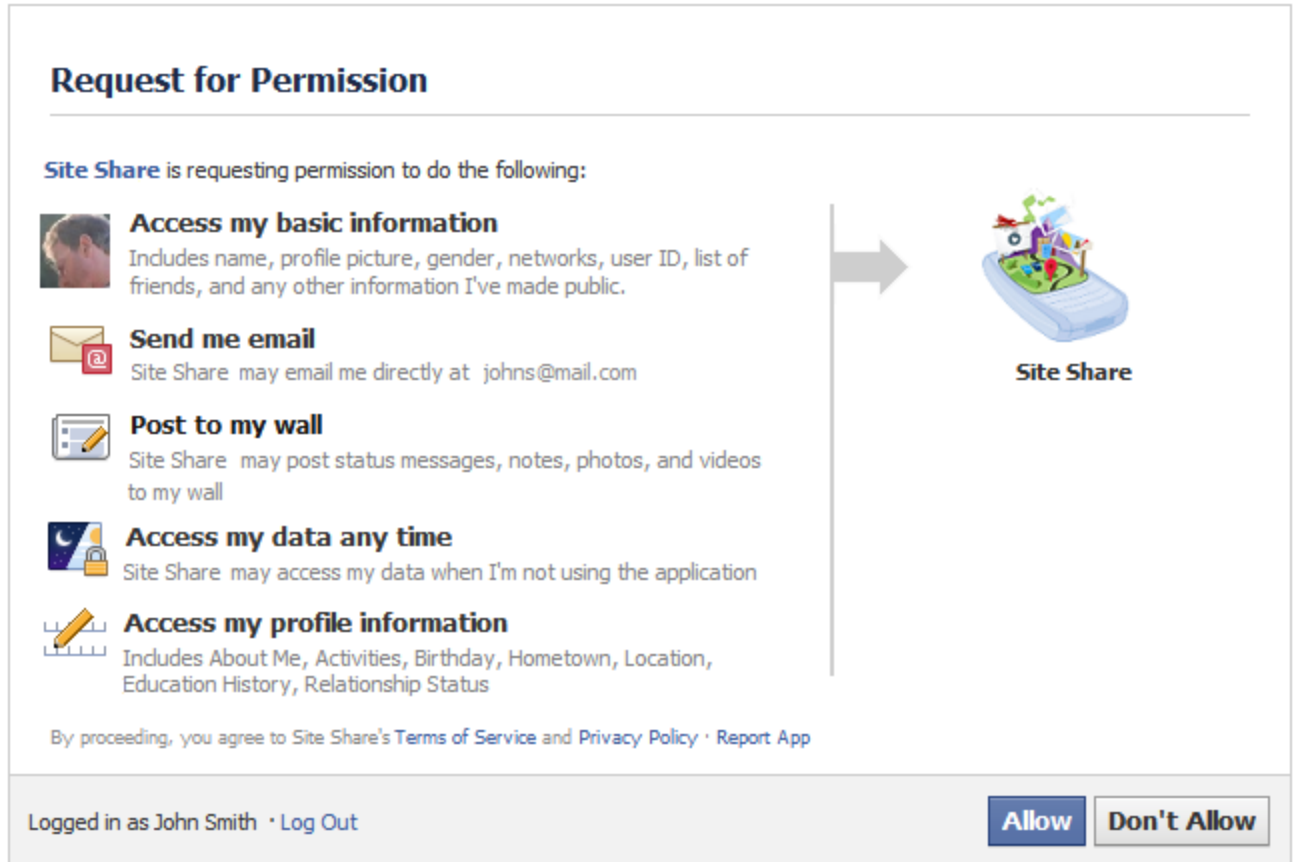


Figure 17: Application Interface for Scenario 3: Site Share

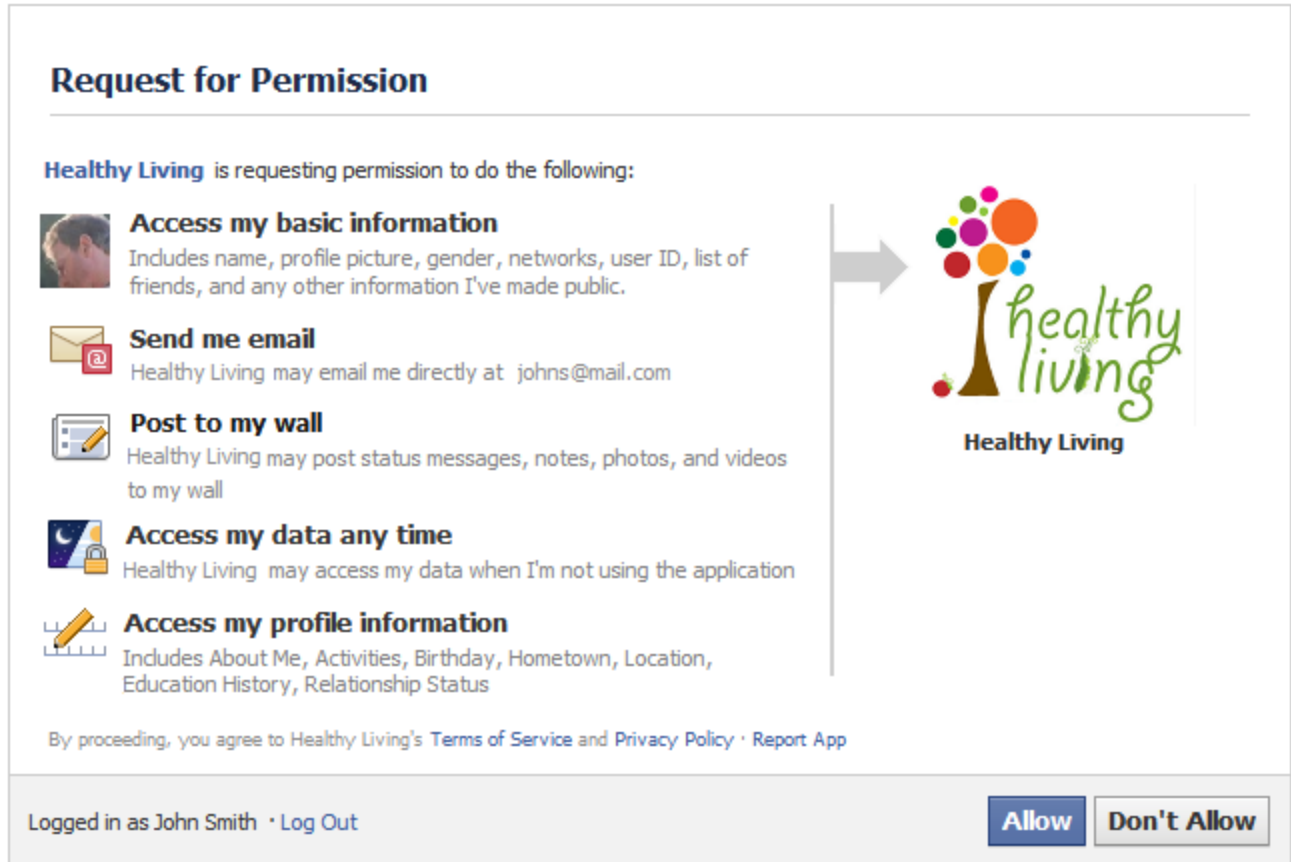


Figure 18: Application Interface for Scenario 4: Healthy Living

Appendix A2: Scenarios with Different Types of Benefits

Scenario #	Scenario Name	Type of Benefit
Scenario 1	Whole Ancestry	Social Benefit
Scenario 2	Site Share	Utilitarian & Social Benefit
Scenario 3	Healthy Living	Utilitarian & Social Benefit
Scenario 4	City Spot	Utilitarian Benefit

** Whole Ancestry represents an application with social benefits, City Spot represents a scenario with utilitarian benefits, and Site Share and Healthy Living represent scenarios with mixed type of benefits. Questions asked to capture different types of benefits are presented below.

Question for Social Benefit: Overall, I believe using this application could bring some social, psychological, and emotional benefits in to my life. (Not at all _____ Very Much)

Questions for Utilitarian Benefit: Overall, I believe using this application could bring some utilitarian benefits (i.e. financial benefits, efficiency, time savings etc.) in to my life. (Not at all _____ Very Much)

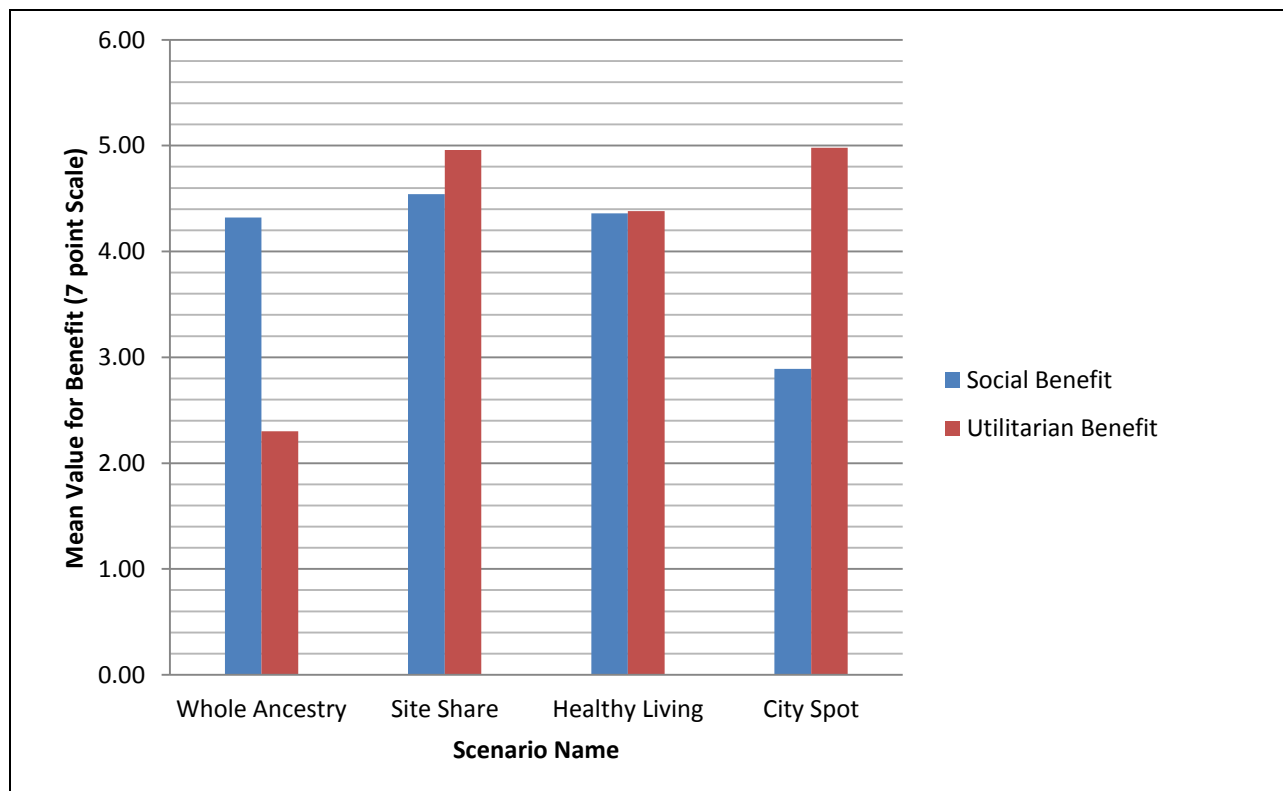


Figure 19: Mean Value of Different Types of Benefit Perceived in Each Scenario

Appendix A3: Sample Demographics

Table 24: Exclusion Criteria

Questions	Frequency	Percentage
<i>Facebook User</i>		
Are you a Facebook user?		
Yes	197	100
No (Exclude)	0	0
<i>Active Facebook User</i>		
How often do you login to Facebook?		
Several times a day	26	13
About once per day	17	9
3-5 times per week	41	21
1-2 times per week	110	56
Every few weeks (Exclude)	0	0
Less often (Exclude)	0	0
Never (Exclude)	0	0

Table 25: Profiles of Responding Participants

Questions	Frequency	Percentage
<i>Gender</i>		
What is your gender?		
Female	106	54
Male	91	46
<i>Age</i>		
What is your age?		
19–25	0	0
26–35	43	22
36–45	54	27
46–55	38	19
56–65	35	18
66–75	18	9
76–85	9	5
<i>State</i>		
What US State do you currently live in?		
<i>Highest Level of Education</i>		
Please indicate the highest level of education you have attained:		
Less than high school	34	17
High school degree	30	15
College degree	35	18
Undergraduate degree	62	31
Graduate degree	33	17

Questions	Frequency	Percentage
Other _____	3	2
<i>Knowledge of Computers and IT of the Participant</i>		
How would you rate your knowledge of computers and information technologies?	3	2
1 (Very Low)	7	4
2	9	5
3	43	22
4	59	30
5	48	24
6	28	14
7 (Very High)		
<i>Years of computer usage</i>		
For how many years have you been using computers?		
1-3	2	1
4-5	1	1
6-8	10	5
9-10	25	13
11-15	61	31
16-20	46	23
over 20 years	52	26
<i>Years of Internet usage</i>		
For how many years have you been using the Internet?		
1-3	4	2
4-5	2	1
6-8	15	8
9-10	38	19
11-15	83	42
16-20	39	20
over 20 years	16	8
<i>Use of Social Network</i>		
How often do you connect to your social network account(s) (i.e. Facebook, Twitter, MySpace, Google+, LinkedIn, hi5, Digg, Renren etc.) in general?	21	11
Anytime I am connected to the Internet	15	8
Several times a day	36	18
About once per day	83	42
3-5 times per week	42	21
1-2 times per week		
<i>Average Facebook Use Time</i>		
How much time (approximately) do you spend on Facebook?		
Up to 15 minutes per month	3	2
Up to 15 minutes per week	26	13
Up to 15 minutes per day	50	25
Up to 1 hour per day	67	34
Up to 3 hours per day	28	14

Questions	Frequency	Percentage
More than 3 hours per day	23	12
<i>Years of Facebook usage</i> For how many years have you been using Facebook?		
I am a user since 2011	13	7
I am a user since 2010	29	15
I am a user since 2009	54	27
I am a user since 2008	37	19
I am a user since 2007	30	15
I am a user since 2006	12	6
I am a user since 2005	15	8
I am a user since 2004	7	4
<i>Awareness on Facebook Applications</i> Are you aware of Facebook Applications?		
Yes (Score: 1)	185	94
No (Score: 2)	12	6
<i>Experience with Facebook Applications</i> Do you use Facebook Applications?		
Never	37	19
Rarely	45	23
Sometimes	66	34
Often	34	17
Always	15	8
<i>Number of Facebook Applications</i> Approximately how many Facebook Applications do you currently use?		
None	44	22
1-3	84	43
4-5	32	16
6-9	24	12
10-14	7	4
15-25	3	2
More than 25	3	2
<i>Number of Facebook Friends</i> Approximately how many friends do you have on Facebook?		
0-50	37	19
50-100	46	23
100-200	30	15
200-300	37	19
300-500	31	16
500-1000	11	6
>1000	5	3

Appendix A4: Validity Analysis

Table 26: Composite Reliability, AVE, and Latent Variable Correlations

	CR	CA	R ²	AVE	1	2	3	4	5	6	7	8	9	10	11	12
1. B	0.97	0.96	0.74	0.90	0.95											
2. LB	0.96	0.94	0.00	0.85	0.85	0.92										
3. IB	0.97	0.96	0.00	0.90	0.80	0.82	0.95									
4. T	0.96	0.95	0.71	0.79	-0.35	-0.37	-0.32	0.89								
5. ST	0.97	0.97	0.00	0.91	-0.29	-0.28	-0.28	0.83	0.95							
6. SeT	0.98	0.97	0.00	0.92	-0.32	-0.28	-0.21	0.76	0.82	0.96						
7. TA	0.96	0.95	0.46	0.86	0.30	0.44	0.44	-0.45	-0.35	-0.31	0.93					
8. E	0.98	0.97	0.00	0.95	0.43	0.48	0.50	-0.67	-0.52	-0.45	0.62	0.98				
9. SE	0.98	0.97	0.00	0.94	0.21	0.27	0.26	-0.34	-0.27	-0.28	0.50	0.42	0.97			
10. C	0.94	0.90	0.00	0.84	-0.12	-0.16	-0.17	0.46	0.39	0.38	-0.34	-0.38	-0.37	0.91		
11. PFC	0.96	0.95	0.43	0.84	-0.04	-0.03	0.04	0.53	0.48	0.46	-0.05	-0.25	-0.08	0.12	0.92	
12. EFC	0.95	0.92	0.22	0.81	0.26	0.30	0.34	0.07	0.17	0.14	0.25	0.14	0.02	-0.07	0.42	0.90

• **1. B** = Perceived Benefits of Use; **2. LB** = Perceived Likelihood of Benefits; **3. IB** = Perceived Importance of Benefits; **4. T** = Perceived Threats to Information Privacy; **5. ST** = Perceived Susceptibility of Privacy Threat; **6. SeT** = Perceived Severity of Privacy Threat; **7. TA** = Perceived Threat Avoidability; **8. E** = Perceived Effectiveness of Privacy Controls; **9. SE** = Self-Efficacy; **10. C** = Perceived Cost of Using Privacy Controls; **11. PFC** = Problem-Focused Coping; **12. EFC** = Emotion-Focused Coping

• **CR** = Composite Reliability; **CA** = Cronbachs Alpha; **R²** = R Square; **AVE** = Average Variance Extracted

• Diagonal elements display the square root of AVE for factors measured with reflective items.

Table 27: Cross Loadings

	1	2	3	4	5	6	7	8	9	10	11	12
1a	0.94	0.80	0.75	-0.36	-0.28	-0.30	0.29	0.40	0.19	-0.13	-0.06	0.22
1b	0.95	0.79	0.76	-0.31	-0.26	-0.28	0.26	0.36	0.17	-0.12	-0.02	0.27
1c	0.97	0.82	0.76	-0.32	-0.28	-0.30	0.28	0.41	0.21	-0.10	-0.01	0.23
1d	0.94	0.79	0.75	-0.36	-0.29	-0.32	0.32	0.46	0.21	-0.12	-0.06	0.27
2a	0.75	0.94	0.83	-0.34	-0.29	-0.29	0.36	0.41	0.22	-0.16	0.00	0.28
2b	0.77	0.92	0.79	-0.30	-0.23	-0.24	0.42	0.41	0.29	-0.12	0.01	0.25
2c	0.75	0.93	0.76	-0.33	-0.24	-0.24	0.43	0.43	0.25	-0.14	-0.03	0.30
2d	0.76	0.90	0.76	-0.42	-0.27	-0.26	0.43	0.52	0.25	-0.17	-0.11	0.27
3a	0.76	0.82	0.95	-0.28	-0.24	-0.19	0.43	0.46	0.24	-0.15	0.06	0.32
3b	0.79	0.83	0.96	-0.33	-0.29	-0.23	0.40	0.49	0.26	-0.14	-0.02	0.26
3c	0.75	0.81	0.96	-0.30	-0.27	-0.20	0.46	0.49	0.27	-0.19	0.05	0.34
3d	0.72	0.76	0.92	-0.29	-0.27	-0.19	0.39	0.47	0.23	-0.15	0.05	0.39
4a	-0.34	-0.37	-0.33	0.91	0.76	0.68	-0.40	-0.64	-0.33	0.43	0.46	0.03
4b	-0.38	-0.40	-0.36	0.91	0.76	0.69	-0.41	-0.62	-0.30	0.42	0.43	0.01
4c	-0.38	-0.39	-0.33	0.91	0.77	0.71	-0.41	-0.62	-0.35	0.44	0.48	0.04
4d	-0.24	-0.26	-0.22	0.86	0.77	0.72	-0.33	-0.57	-0.29	0.40	0.44	0.13
4e	-0.30	-0.31	-0.26	0.90	0.74	0.67	-0.41	-0.59	-0.27	0.39	0.51	0.11
4f	-0.22	-0.26	-0.19	0.84	0.62	0.55	-0.42	-0.54	-0.26	0.39	0.49	0.07
5a	-0.30	-0.30	-0.29	0.74	0.96	0.80	-0.38	-0.56	-0.26	0.39	0.49	0.14
5b	-0.28	-0.26	-0.26	0.71	0.97	0.79	-0.34	-0.50	-0.25	0.38	0.48	0.16
5c	-0.27	-0.25	-0.27	0.79	0.95	0.78	-0.32	-0.49	-0.24	0.37	0.45	0.16
5d	-0.26	-0.25	-0.24	0.72	0.93	0.77	-0.30	-0.43	-0.27	0.36	0.38	0.20
6a	-0.29	-0.23	-0.18	0.69	0.76	0.95	-0.27	-0.41	-0.27	0.36	0.41	0.16
6b	-0.33	-0.29	-0.22	0.73	0.78	0.97	-0.30	-0.44	-0.28	0.37	0.46	0.12
6c	-0.31	-0.29	-0.22	0.76	0.83	0.97	-0.32	-0.43	-0.26	0.37	0.46	0.13
6d	-0.30	-0.25	-0.20	0.72	0.80	0.95	-0.30	-0.44	-0.28	0.38	0.42	0.13
7a	0.27	0.41	0.39	-0.46	-0.37	-0.33	0.92	0.59	0.51	-0.35	-0.10	0.18
7b	0.30	0.42	0.41	-0.41	-0.33	-0.29	0.93	0.59	0.47	-0.32	-0.02	0.26
7c	0.28	0.41	0.42	-0.38	-0.32	-0.29	0.95	0.57	0.48	-0.33	-0.02	0.20
7d	0.26	0.39	0.43	-0.40	-0.30	-0.24	0.91	0.55	0.39	-0.26	-0.03	0.28
8a	0.44	0.47	0.49	-0.67	-0.52	-0.44	0.61	0.98	0.42	-0.37	-0.25	0.12
8b	0.41	0.47	0.48	-0.68	-0.53	-0.46	0.58	0.98	0.39	-0.38	-0.28	0.14
8c	0.41	0.47	0.50	-0.63	-0.48	-0.42	0.63	0.97	0.41	-0.35	-0.22	0.16
9a	0.20	0.28	0.27	-0.31	-0.24	-0.25	0.50	0.39	0.98	-0.37	-0.07	0.02
9b	0.20	0.25	0.25	-0.35	-0.29	-0.30	0.49	0.42	0.96	-0.34	-0.08	0.04
9c	0.19	0.26	0.24	-0.32	-0.26	-0.27	0.47	0.40	0.97	-0.35	-0.08	0.00

	1	2	3	4	5	6	7	8	9	10	11	12
10a	-0.07	-0.10	-0.13	0.37	0.32	0.30	-0.32	-0.29	-0.31	0.92	0.06	-0.09
10b	-0.18	-0.22	-0.20	0.51	0.43	0.43	-0.35	-0.43	-0.32	0.94	0.19	-0.11
10c	-0.08	-0.10	-0.11	0.37	0.31	0.31	-0.24	-0.30	-0.40	0.88	0.07	0.01
11a	-0.08	-0.10	-0.02	0.53	0.42	0.43	-0.08	-0.26	-0.08	0.16	0.90	0.29
11b	-0.04	-0.03	0.03	0.49	0.41	0.40	-0.06	-0.26	-0.08	0.08	0.94	0.35
11c	-0.04	-0.04	0.01	0.52	0.47	0.46	-0.07	-0.25	-0.08	0.10	0.94	0.41
11d	-0.03	0.00	0.05	0.47	0.45	0.42	-0.04	-0.24	-0.07	0.13	0.88	0.42
11e	0.01	0.01	0.08	0.41	0.43	0.37	0.03	-0.16	-0.06	0.09	0.92	0.44
12a	0.21	0.26	0.30	0.14	0.20	0.18	0.21	0.03	0.03	-0.07	0.47	0.80
12b	0.25	0.26	0.30	0.05	0.15	0.12	0.19	0.12	0.02	-0.03	0.33	0.93
12c	0.25	0.28	0.32	0.00	0.11	0.10	0.22	0.17	-0.01	-0.06	0.32	0.94
12d	0.24	0.29	0.32	0.06	0.15	0.10	0.26	0.20	0.03	-0.10	0.37	0.93

Appendix B: Supporting Material for Chapter 4

Appendix B1: Graphical Interfaces for Healthy Living

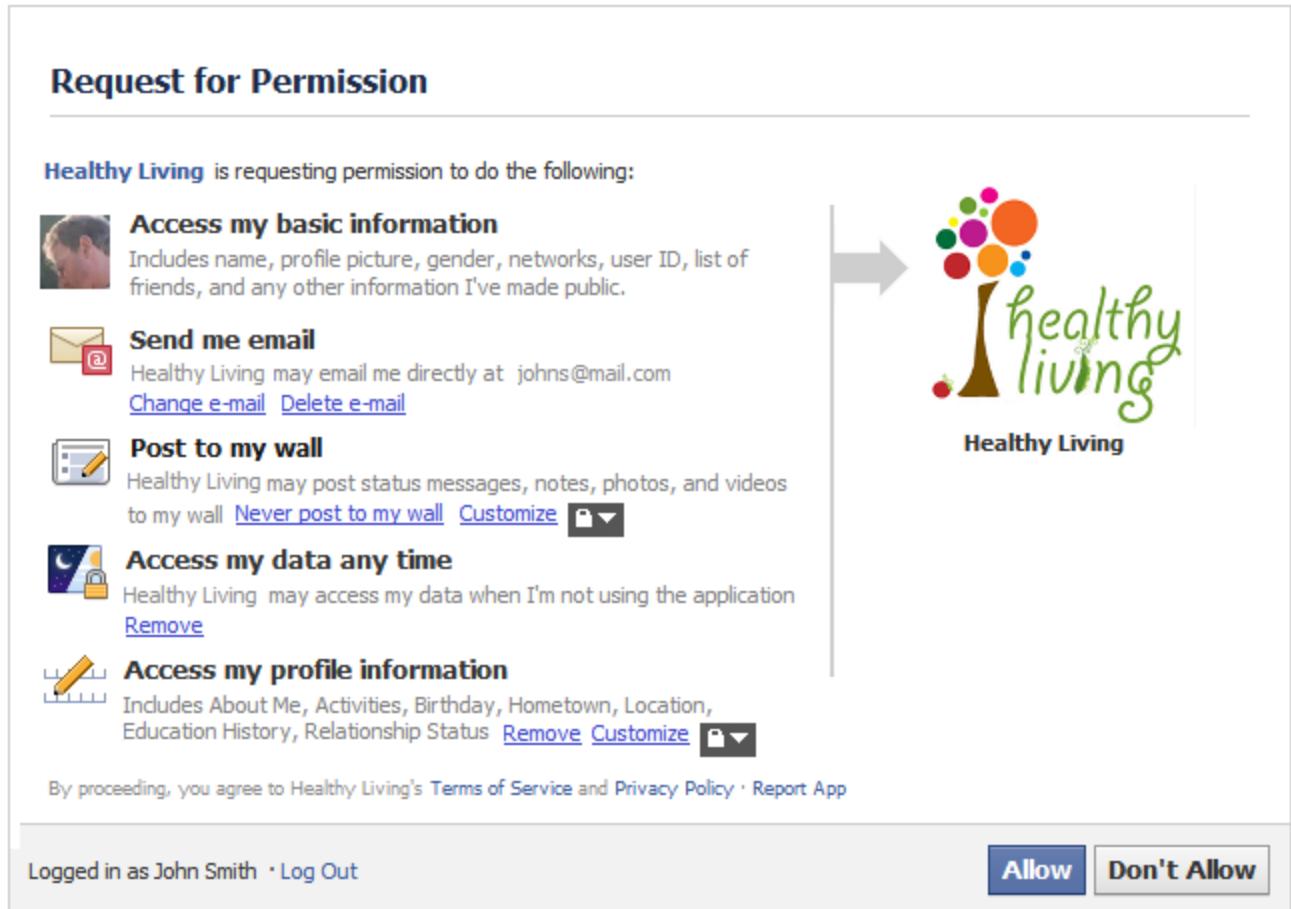




Figure 20: Interface for Low Request and High Privacy Control (Group 1)

Request for Permission


Healthy Living is requesting permission to do the following:





Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.




Send me email
Healthy Living may email me directly at johns@mail.com
[Change e-mail](#) [Delete e-mail](#)




Post to Facebook as me
Healthy Living may post status messages, notes, photos, and videos on my behalf [Never post to my wall](#) [Customize](#) 




Access my data any time
Healthy Living may access my data when I'm not using the application
[Remove](#)





Send me SMS messages
Healthy Living may send SMS messages to my phone [Remove](#)




Check-ins
Healthy Living may read my check-ins and friends' check-ins [Remove](#)



Access my profile information
Includes Likes, Music, TV, Movies, Books, Quotes, About Me, Activities, Interests, Groups, Events, Notes, Birthday, Hometown, Current Cities, Work History, Photos, Videos, and Facebook Statuses [Customize](#) 



Access my contact information
Healthy Living may access my current address and phone number
[Remove](#)



Healthy Living

By proceeding, you agree to Healthy Living's [Terms of Service](#) and [Privacy Policy](#) · [Report App](#)

Logged in as John Smith · [Log Out](#)

Allow

Don't Allow

Figure 21: Interface for High Request and High Privacy Control (Group 2)

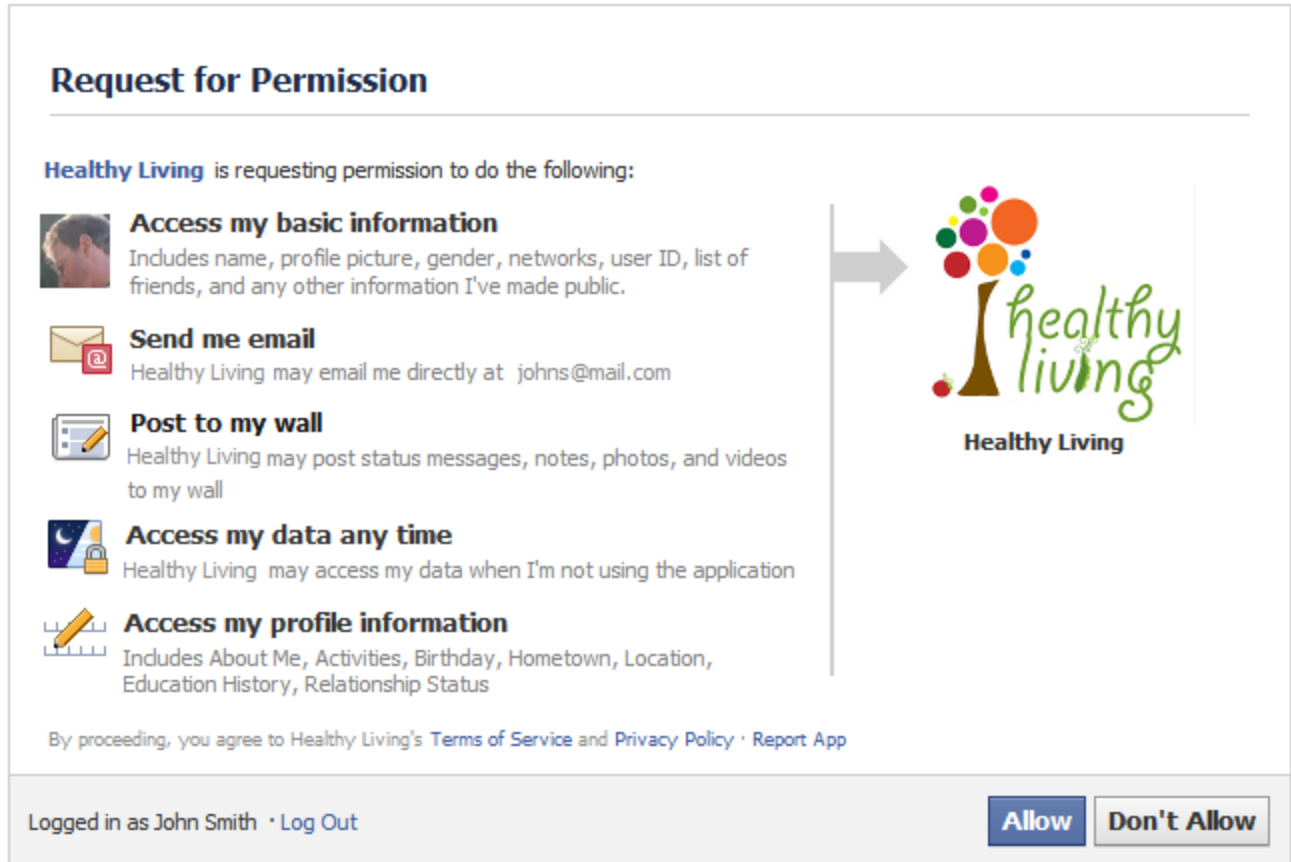


Figure 22: Interface for Low Requests and Low Privacy Control (Group 3)

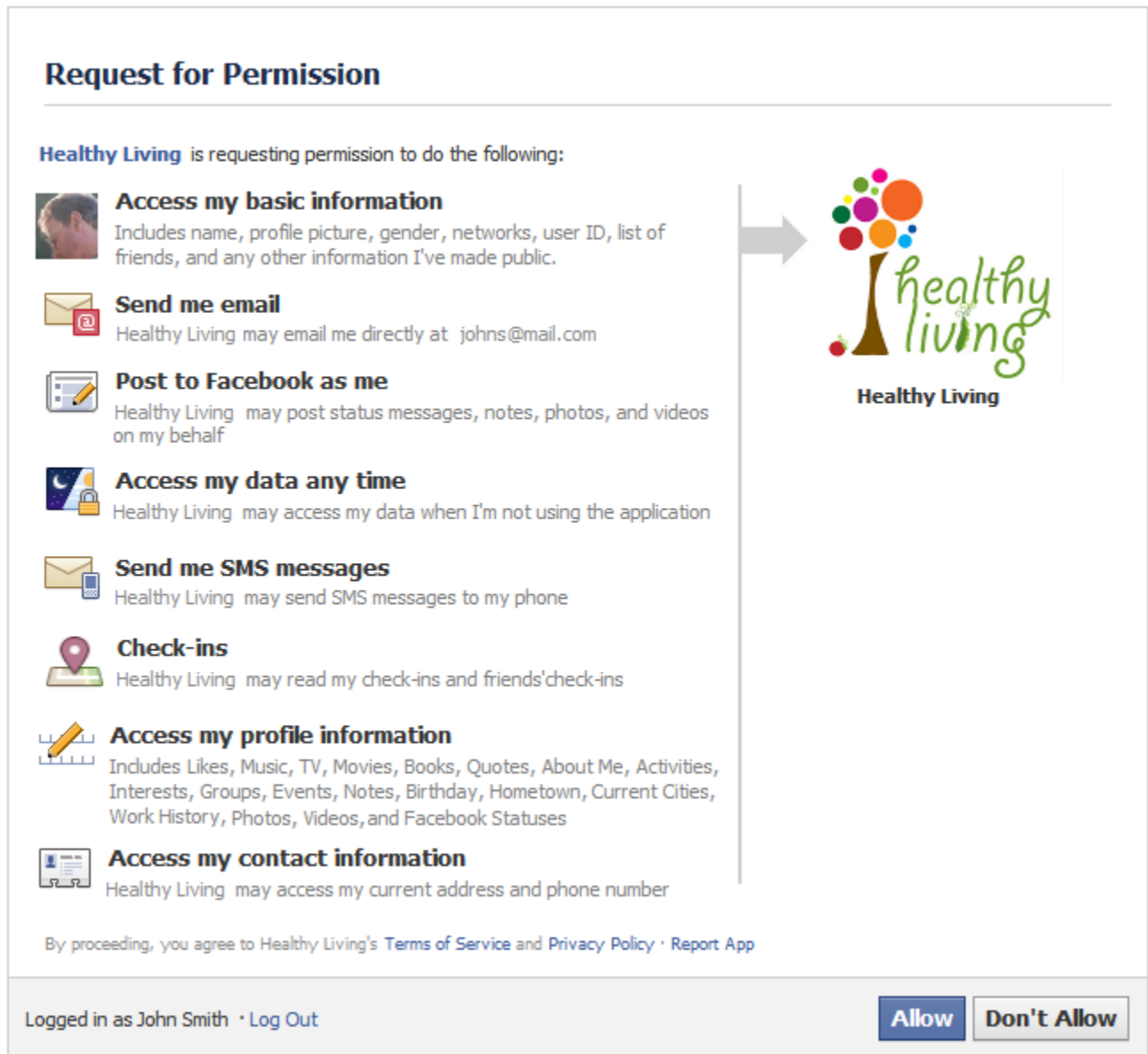


Figure 23: Interface for High Requests and Low Privacy Control (Group 4)

Table 28: Sample Demographics for Study 3

	Age	%	Male	Female
Age	13-18	0		
	19-25	27%	45%	55%
	26-34	27%	45%	55%
	35-44	18%	45%	55%
	45-54	13%	40%	60%
	55-64	8%	40%	60%
	65+	7%		
	85+	0		
Education			States %	
	< High school		CA	18
	High school	117	TX	11
	College / Uni	121	NY	10
	Trade/Assoc.	130	FL	8
	Bachelor's	228	IL	6
	Graduate	137	PE	5
	Other	17	OH	5
	Total	747	MI	5
			GA	5
			NC	4
			NJ	4
			MA	4
			Others	15