

Copyright Warning & Restrictions

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted material.

Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be “used for any purpose other than private study, scholarship, or research.” If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of “fair use” that user may be liable for copyright infringement,

This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve violation of copyright law.

Please Note: The author retains the copyright while the New Jersey Institute of Technology reserves the right to distribute this thesis or dissertation

Printing note: If you do not wish to print this page, then select “Pages from: first page # to: last page #” on the print dialog screen



The Van Houten library has removed some of the personal information and all signatures from the approval page and biographical sketches of theses and dissertations in order to protect the identity of NJIT graduates and faculty.

ABSTRACT

APPROPRIATION OF PRIVACY MANAGEMENT WITHIN SOCIAL NETWORKING SITES

by
Catherine Dwyer

Social networking sites have emerged as one of the most widely used types of interactive systems, with memberships numbering in the hundreds of millions around the globe. By providing tools for their members to manage an ever-changing set of relationships, social networking sites push a constant expansion of social boundaries. These sites place less emphasis on tools that limit social boundaries to enable privacy.

The rapid expansion of online social boundaries has caused privacy shockwaves. Privacy offline is enabled by constraints of time and space. Online, powerful search engines and long term digital storage means private data have no expiration date. Within an online culture of anonymity and fluid self-presentation of identity, social networking sites can be turned into places of perceived safety but with privacy risks that actually extend indefinitely.

While these sites do deploy privacy management features, it is not understood how people use social networking sites, how they use privacy management features, and how these two are related. In order to create better privacy mechanisms for social software, designers must first understand how members manage their privacy in the current environment.

This dissertation introduces The Social Software Performance Model, which describes relevant factors and their interaction in order to explain patterns of privacy management. The Model is a synthesis of Adaptive Structuration Theory, the Fit

Appropriation Model and socio-technical systems theory. Adaptive Structuration Theory attempts to explain appropriation, defined as the process by which people integrate technology into their daily tasks and activities. A central premise of this research is that the appropriation perspective is a valuable lens for teasing apart how members of these sites adopt and adapt privacy management features.

Using Adaptive Structuration Theory, this dissertation developed and validated new measures that capture appropriation patterns related to privacy management within social networking sites. The research introduces three independent constructs that measure privacy management appropriation. They are the Use appropriation move, which measures actual use of privacy management features; the Familiarity appropriation move, which measure knowledge of privacy management features; and the Restricted Scope appropriation move, which measures the extent to which members independently limit the scope of their online social network to protect their privacy.

Survey data was collected from subjects in two different social networking sites, Facebook and MySpace, and used to evaluate hypotheses developed from The Social Software Performance Model. Using a partial least squares analysis, the research model explained 28.5% of the variance with respect to appropriation of privacy management features. This is a strong result for exploratory research.

This research makes a contribution by extending theories to a new context, by applying both the Adaptive Structuration Theory and the Fit Appropriation Model to the use of privacy management in social networking sites. Using types and sub-types of appropriation moves from Adaptive Structuration Theory, new measures were developed and validated. These new measures, with further efforts to establish validity

and reliability, can be adapted to understand appropriations for other forms of social software.

The main finding of the research is a method to evaluate the effectiveness of different implementations of privacy management within social networking sites. While information system theory has been primarily concerned with systems used in an organizational context, the results of this research shows these theories are relevant to new systems based on social interaction.

These new types of social software, generically labeled as Web 2.0, are among the most popular on the Internet. Besides Facebook and MySpace, examples of Web 2.0 include the video sharing site YouTube.com, and the photo sharing site Flickr.com. These sites thrive on intensive social interaction, and are growing in scope and importance. There has been little consensus among researchers as to how to measure the effectiveness of Web 2.0 systems. This lack of consensus presents a strategic opportunity for information systems theory, which has made determinations of effectiveness an important focus. This research has adapted information systems theory to study the effectiveness of privacy management.

The development of privacy management has proven to be a difficult problem, and a deeper understanding of its effectiveness is expected to improve the overall design of these systems. By adapting information systems theory to the use of privacy management within social networking sites, this research shows that information systems theory can also be used applied to Web 2.0 applications. This provides a foundation for the further development of methods to measure the effectiveness of additional components within social software.

**APPROPRIATION OF PRIVACY MANAGEMENT
WITHIN SOCIAL NETWORKING SITES**

**by
Catherine Dwyer**

**A Dissertation
Submitted to the Faculty of
New Jersey Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy in Information Systems**

Department of Information Systems

May 2008

Copyright © 2008 by Catherine Dwyer

ALL RIGHTS RESERVED

APPROVAL PAGE

**APPROPRIATION OF PRIVACY MANAGEMENT
WITHIN SOCIAL NETWORKING SITES**

Catherine Dwyer

4/14/2008

Dr. Starr Roxanne Hiltz, Dissertation Advisor
Distinguished Professor Emeritus, Information Systems, NJIT

Date

3/24/08

Dr. Katia Passerini, Committee Member
Assistant Professor, Joint appointment with Information Systems and the School of
Management, NJIT

Date

3/24/08

Dr. George Widmeyer, Committee Member
Associate Professor, Information Systems, NJIT

Date

3/24/08

Dr. Naomi Rotter, Committee Member
Professor, School of Management, NJIT

Date

3/24/08

Dr. Marshall Scott Poole, External Committee Member
Professor, Speech Communication, University of Illinois at Urbana-Champaign

Date

BIOGRAPHICAL SKETCH

Author: Catherine Dwyer
Degree: Doctor of Philosophy
Date: May 2008

Undergraduate and Graduate Education:

- Doctor of Philosophy in Information Systems,
New Jersey Institute of Technology, Newark, NJ, 2008
- Master of Science in Computer Science,
Pace University, New York, NY, 1996
- Master of Arts In Music Education,
The Manhattan School of Music, New York, NY, 1984
- Bachelor of Arts in English and Political Science,
Fordham University, Bronx, NY, 1979
Magna cum laude in cursa honorum

Major: Information Systems

Presentations and Publications:

Dwyer, C. (2007). *Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS), Hawaii.

Dwyer, C., Hiltz, S. R., & Jones, Q. (2006). *Discovering Boundaries for Mobile Awareness: An Analysis of Relevant Design Factors*. Paper presented at the Americas Conference on Information Systems, Acapulco, Mexico.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace*. Paper presented at the Thirteenth Americas Conference on Information Systems, Keystone, Colorado.

Dwyer, C., Hiltz, S. R., & Widmeyer, G. (2008). *Understanding Development and Usage of Social Networking Sites: The Social Software Performance Model*. Paper presented at the 41st Annual Hawaii International Conference on System Sciences (HICSS), Hawaii.

To Jim, Maura, and Catherine

ACKNOWLEDGMENT

I would like to express my deepest gratitude and affection to Dr. Starr Roxanne Hiltz, for her dedication, support, encouragement, and assistance. Roxanne is an advisor, researcher, teacher, mentor, collaborator and friend without peer.

Special thanks are given to my committee members Dr. Katia Passerini, Dr. George Widmeyer, Dr. Naomi Rotter, and Dr. Marshall Scott Poole for their assistance and careful attention to my research. I am grateful to George for collecting and clipping news articles from the business press on social networking sites. I especially want to thank my entire committee for their enthusiasm in tackling a research topic new to all of them.

Many of the ideas described here came to fruition after I was given numerous opportunities to present my work at IS Seminar. For the many students and faculty who listened attentively and gave me invaluable feedback, I thank you. I also want to thank Professors Michael Bieber, Il Im, Murray Turoff, Quentin Jones, Jerry Fjermestad and Brook Wu for their support. I also wish to thank Liz Avery Gomez for her assistance and companionship in the program. I also want to acknowledge Dean Susan Merritt of Pace University. Without her financial support and encouragement, I would not have pursued this degree.

Finally my deepest thanks, appreciation and love to my husband Jim, who has been my support for many years. I also need to especially thank my daughters Maura and Catherine, who introduced me to social networking sites. They were my first subjects as they became ardent users of MySpace and then Facebook. I am grateful to them and their

friends, who cheerfully and honestly answered my (many) questions. Any parent of teenagers will know what a sacrifice it is for a child to allow a parent access to their online profile, let alone be the subject of intense scrutiny. This dissertation would not have been possible without their help.

TABLE OF CONTENTS

Chapter	Page
1 INTRODUCTION	1
1.1 Objective	1
1.2 Background.....	3
1.3 Relevance to Information Systems Research.....	5
1.4 Research Question.....	6
1.5 The Scope of This Research	7
1.6 Dissertation Outline.....	8
2 A REVIEW OF SOCIAL NETWORKING SITES.....	10
2.1 Definition of Social Networking Sites.....	10
2.2 Typical Use	12
2.3 Examples of Social Networking Sites	13
2.3.1 Description of Facebook	13
2.3.2 Description of MySpace.....	14
2.4 Defining Your Online Identity	15
2.5 Growing Your Social Network	19
2.6 Social Implications of Social Networking Sites	21
2.7 Web Crawl Studies of Social Networking Sites	25
2.8 Privacy and Social Networking Sites	27
2.9 Privacy Issues and Internet Use	29
2.9.1 Development Internet Privacy Scale	30

TABLE OF CONTENTS (Continued)

Chapter	Page
2.9.2 Information Privacy Research	32
2.9.3 Information Privacy Within Social Networking Sites	33
2.10 Privacy Implications	35
2.10.1 Privacy Risk From Information Disclosure	36
2.10.2 Use of Privacy Settings to Restrict Access	39
2.11 Attitudes Regarding Privacy	40
2.12 Discussion of Social Networking Sites and Privacy	43
2.13 Summary	45
3 THEORETICAL FOUNDATION.....	47
3.1 Structuration Theory and Information Systems	47
3.2 The Adaptive Structuration Theory	52
3.3 The Fit Appropriation Model	62
3.4 Meta-Analysis Results	67
3.5 Feedback Within Socio-technical Systems	69
3.6 Socio-technical Systems Theory and Information Systems	71
3.7 Summary.....	73
4 THE SPIRIT OF PRIVACY MANAGEMENT WITHIN SOCIAL NETWORKING SITES	75
4.1 The “Spirit” of Facebook and MySpace	75
4.2 Privacy Support Within Social Networking Sites	77
4.3 Privacy Management on Facebook	78

TABLE OF CONTENTS

(Continued)

Chapter	Page
4.4 Privacy Management on MySpace	82
4.5 Complexities of Privacy Management	86
4.6 Problems with Privacy Management	87
4.7 Appropriation of Privacy Management	88
5 THE SOCIAL SOFTWARE PERFORMANCE MODEL.....	91
5.1 Research Questions	91
5.2 Foundations of The Conceptual Model.....	93
5.3 The Social Software Performance Model	94
5.4 Empirical Test of a Portion of the Social Software Performance Model	98
5.5 Appropriation and Appropriation Moves	99
5.6 Appropriation Support	101
5.7 Individual Factors and Habitual Routines	103
5.8 Hypotheses and Research Questions	104
5.8.1 Variables	104
5.8.2 Hypotheses	105
5.9 Open Research Questions	110
6 DESIGN OF THE SURVEY INSTRUMENT.....	111
6.1 Description of Appropriation of Privacy Management Instrument	113
6.1.1 Demographics	113
6.1.2 Usage	113

TABLE OF CONTENTS

(Continued)

Chapter	Page
6.1.3 Concern for Internet Privacy.....	114
6.2 Appropriation Moves	114
6.2.1 Faithful Appropriation Moves	115
6.2.2 Unfaithful (Ironie) Appropriation Moves.....	116
6.2.3 Other Measures	117
7 METHODOLOGY AND UNIVARIATE RESULTS	119
7.1 Survey Methodology	119
7.2 Identifying the Target Population	119
7.3 Survey Administration for MySpace	121
7.4 Survey Administration for Facebook	122
7.5 Calculating the Confidence Level	123
7.6 Analysis of Missing Data	124
7.7 Demographic Data	124
7.8 Site Usage Data	126
7.9 Univariate Results for Independent Variables	130
7.10 Univariate Results for Dependent Variables	132
7.10.1 Univariate Results for Use Appropriation Move	132
7.10.2 Univariate Results for Familiarity Appropriation Move	133
7.10.3 Univariate Results for Restricted Scope Appropriation Move	135
7.10.4 Univariate Results for Rejection Appropriation Move	136

TABLE OF CONTENTS (Continued)

Chapter	Page
7.10.5 Univariate Results for One Sided Profile Browsing	137
7.10.6 Univariate Results for Distrust in Other Members	140
7.10.7 Univariate Results for Unfaithfulness Measures	142
7.10.8 Univariate Results for Value of Privacy Measure	142
7.10.9 Univariate Results for Trust in Site	144
8 SUMMARY OF QUALITATIVE DATA.....	145
8.1 Benefits of Social Networking Use	145
8.2 Greatest Concern With Regard to Use	147
8.3 Effectiveness of Privacy Management	149
8.4 Reports of Personal Experiences With Privacy Issues	150
9 RELIABILITY TESTS AND FACTOR ANALYSIS	154
9.1 Validity and Reliability	154
9.2 Tests of Reliability and Normal Distribution	156
9.3 Factor Analysis and Identification of Factors	157
9.4 Evaluation of Hypotheses	162
9.5 Main Effects	163
9.6 Open Research Questions	174
10 PLS ANALYSIS OF FINDINGS	182
10.1 Overview of PLS	182
10.2 Establishing Validity and Reliability Using PLS	185

TABLE OF CONTENTS (Continued)

Chapter	Page
10.3 Redundancy Analysis	188
10.4 PLS Analysis of Research Model	192
10.5 PLS Analysis For Unfaithful Moves	195
10.6 PLS Analysis of Faithfulness	198
11 EXPLORATION OF FINDINGS USING PLS AND QUALITATIVE ANALYSIS.....	200
11.1 Adding Social Context to The Research Model	200
11.2 Revisions to the Research Model	202
11.3 Validity Tests for Revised Model	204
11.4 Discussion of Revised Model	205
11.5 Identification of Privacy Management Strategies	209
11.6 Comparing Default Privacy Levels on Facebook Versus MySpace	216
11.7 Comparing Groups by Use Profile.....	217
12 SUMMARY AND CONCLUSIONS	222
12.1 Development of The Theoretical Model	223
12.2 Summary of Findings	226
12.3 Implications for Design.....	235
12.4 Re-evaluation of The Social Software Performance Model	239
12.5 Contributions	242
12.6 Limitations	244
12.7 Future Research	245

TABLE OF CONTENTS
(Continued)

Chapter	Page
APPENDIX A SUMMARY OF MISSING DATA.....	249
APPENDIX B CONSENT FORM AND SURVEY INSTRUMENT.....	252
APPENDIX C PILOT STUDIES	265
REFERENCES	288

LIST OF TABLES

Table	Page
5.1 Privacy Management Components	102
7.1 Summary of Demographic Data	125
7.2 Summary of Site Usage Data	127
7.3 Summary of Information Subjects Include in Their Profile	129
7.4 Summary of Results for Concern for Internet Privacy Construct	131
7.5 Level of High Use for Facebook Versus MySpace Members	132
7.6 Summary of Responses for Use Appropriation Move	133
7.7 Summary of Results for Familiarity Appropriation Move	134
7.8 Summary of Results for Restricted Scope Appropriation Move	135
7.9 Summary of Results for Rejection Appropriation Move	137
7.10 Summary of Results for One Sided Profile Browsing	138
7.11 Cross Tabulation To Determine One Sided Profile Browsing	139
7.12 Summary of Responses for Distrust Measures	140
7.13 Summary of Results for Unfaithfulness	141
7.14 Summary of Responses for Measure of Value in Privacy	143
7.15 Summary of Results for Trust in Site	144
8.1 Summary of Prior Issues With Privacy	151
9.1 Summary of Reliability Tests for Research Constructs	157
9.2 Initial Factor Loading for Research Measures	158

LIST OF TABLES **(Continued)**

Table	Page
9.3 Rotated Factor Solution	160
9.4 Summary of Hypothesis Tests for H1	163
9.5 Summary of Hypothesis Tests for H2	164
9.6 Summary of Hypothesis Tests for H3	165
9.7 Summary of Hypothesis Tests for H4	166
9.8 Summary of Hypothesis Tests for H5	167
9.9 Summary of Hypothesis Tests for H6	168
9.10 Summary of Hypothesis Tests for H7	169
9.11 Summary of Hypothesis Tests for H8	170
9.12 Summary of Hypothesis Tests for H9	171
9.13 Summary of Hypothesis Tests for H10	172
9.14 Summary of Hypothesis Tests for Outcomes by Gender	175
9.15 Summary of Hypothesis Tests for Outcomes by Age	176
9.16 Summary of Hypothesis Tests for Outcomes by School Status	177
9.17 Summary of Hypothesis Tests for Outcomes by Ethnicity	178
9.18 Summary of Hypothesis Tests for Outcomes by Privacy Experience	179
10.1 Summary of Faithful Appropriation Moves Formative Construct	190
10.2 Summary of Indicators for Faithfulness Reflective Construct	192
11.1 Quality Criteria for Revised Familiarity Model	204
11.2 Test of Discriminant Validity for Revised Model	204

LIST OF TABLES (Continued)

Table	Page
11.3 Results for the Distrust2 Indicator	206
11.4 Quality Measures for Revised Model Applied to Faithful Moves	209
11.5 Comparing Groups Based on Use Profile	219
11.6 Comparing All Groups Based on Use Profile	220
12.1 Summary of Hypothesis Tests	232
A.1 Summary of Missing Data.....	250
C.1 Faithfulness of Appropriation Scale.....	270
C.2 Familiarity Appropriation Move.....	271
C.3 Actual Use Appropriation Move.....	272
C.4 Partial Appropriation Move.....	273
C.5 Using Fake Information.....	274
C.6 Summary of Results for Bad Opinion Construct.....	275
C.7 Rejection of Privacy Settings.....	277
C.8 Principal Components Matrix.....	279
C.9 Rotated Component Matrix.....	281
C.10 Results for Faithful Appropriation Move.....	285
C.11 Results for Negative Appropriation Move.....	286
C.12 Results for Faithfulness of Appropriation Scale.....	286
C.13 Effect Size for Appropriation Moves.....	286

LIST OF FIGURES

Figure	Page
2.1 Cathy's Facebook profile	16
2.2 A profile from MySpace	19
2.3 Friends are organized in a list, and are easy to see and contact	20
3.1 Model of Adaptive Structuration Theory, from Majchrzak, 2000	60
3.2 Fit Appropriation Model, from Dennis et al., 2001	66
3.3 The structure of a socio-technical system, based on Hughes, 1989	70
4.1 GUI for privacy management on Facebook	79
4.2 Facebook offers granular privacy control	80
4.3 Facebook supports control over access to contact information	81
4.4 Privacy management in MySpace	82
4.5 Options to control spam in MySpace	84
4.6 Privacy settings control the visibility of profiles	85
5.1 Conceptual Model: Social Software Performance Model	95
5.2 Components of model to be tested	99
10.1 Redundancy analysis of Faithful appropriation moves	189
10.2 PLS evaluation of Faithful Privacy Management model	193
10.3 PLS analysis of Unfaithful moves	196
10.4 Summary of results for Faithfulness	198
11.1 Initial model of Familiarity appropriation move	201

LIST OF FIGURES (Continued)

Figure	Page
11.2 Revised Model for Familiarity Appropriation Move, adding two trust related constructs	203
11.3 Revised model results as applied to Faithful appropriation moves	208
11.4 Example of a bare bones "shell" profile from Facebook	211
12.1 Conceptual model: The Social Software Performance Model	224
12.2 Results for PLS analysis of Faithful appropriation moves	233
12.3 The Social Software Performance Model, v. 2.0	240

CHAPTER 1

INTRODUCTION

1.1 Objectives

The goals of social networking sites are to provide support for the development and maintenance of social relationships, to make connections and inter-connections more apparent, and to make it easier to contact others.

To achieve these goals, social networking sites provide *structures* in support of interpersonal relationships. These structures are the tools, functions, rules, and resources that make up the site's design and features. A social networking site provides structures in support of social interaction in the same way that Group Decision Support Systems (GDSS) provide structures in support of the group decision process (DeSanctis & Poole, 1991). Just as GDSS supports the "structuring" of the decision process, so do social networking sites support the "structuring" of social interaction. The structures provided by social networking sites include digital self-presentation, visualization of social networks, and communication support. One final structure, privacy management, will be the focus of this research.

The goal of this research is to accurately explain and model how members *appropriate* privacy management structures within social networking sites. Appropriation refers to way in which users adapt and adopt technology in order to carry out tasks (DeSanctis & Poole, 1994; Dourish, 2003).

Different implementations of social networking sites may vary in the structural features they include. However, differences in features do not fully explain differences in outcomes. Equally important are differences in how members of these sites choose to use

or not use the structures at their disposal. In understanding how members make use of privacy management within social networking sites, it is important to note that social networking sites provide one source of structure; other privacy structures come from members' individual beliefs, social norms, and privacy standards set by industry and governmental entities. It is this complex combination of privacy structures that members grapple with when using social networking sites.

In arguing for Adaptive Structuration Theory, DeSanctis and Poole note that the use of GDSS has shown mixed results. Similar mixed results are in evidence in terms of the use of privacy management tools within software. Subjects express concern, but show little interest in using privacy features (Stark and Hodge 2004; Gross and Acquisti 2005; Iachello, Smith et al. 2005; Buchanan, Paine et al. 2007). It is argued here that privacy management tools place members on "unfamiliar cognitive ground," as is the case with GDSS (DeSanctis & Poole, 1991, p. 150). So with GDSS and decision processes, privacy online cannot be managed in the same way as privacy is managed in the offline world. Just as groups must adapt to GDSS, people must adapt to managing privacy online. It is this adaptation process that is the focus of this research.

When adapting privacy management settings, members can use them as intended by system designers, or choose not to. So the use of privacy management tools can lead to both intended and unintended consequences (i.e., with respect to the intent of the designers). Members can adjust privacy settings in small ways that actually help the functioning of the system. Or they can appropriate them in a way that can diminish the overall effectiveness of system. These effects are difficult to predict ahead of time, but they can be described using Adaptive Structuration Theory.

The objective of this research is to apply Adaptive Structuration Theory to privacy management within social networking sites. Specifically, this dissertation documents how appropriation moves with respect to privacy management have been identified, and measures have been created. These measures were used to test the impact of individual concerns about privacy on appropriation of privacy management. In addition, these measures were used to examine the effectiveness of privacy management tools within two different sites. This dissertation describes a study that examined two different implementations of privacy management, and the type of appropriation moves carried out by members of social networking sites.

1.2 Background

Social networking sites are systems that offer free accounts, with ways to display profile information, visualize connections to friends, and share digital media with few if any limits on the amount of information posted or the size of the files hosted. Compare this to just a few years ago, when internet providers charged fees for web site hosting and e-mail accounts, and limited the server space available to just a few megabytes.

Just within the last few years, social networking sites have become extremely popular, boasting memberships in the millions. The success of these sites would not be possible without substantial technical and financial developments. On the technical side, the cost of data storage and computational power has decreased, while the number of people with high bandwidth access to the internet has increased. On the financial side, advertisers have noticed a transition in consumer behavior from watching television to going online. In response, companies are moving their advertising dollars to the Internet.

Therefore the business model of these sites, with free accounts and no limit on storage, can be supported with advertising.

When a person uses a social networking site, all their activity takes place on networked computers, with little if any information saved to the client machine. This gives members great flexibility. They can check in from any computer, see their profile, and use the site. Since everyone's profile is kept by the site, it is simple to find a friend – just do a search, and the site, using the information posted individually and pooled on networked computers, quickly delivers their picture and profile.

What makes these sites powerful and popular is the technology infrastructure that creates a digital space where every social transaction is captured and recorded in real time. The combined efforts of members of a social networking site take on a logarithmic quality. Members can find someone who shares their interest in French poetry, or reconnect to classmates from 10 years ago. This is possible because any activity is digitized, and saved within a computing structure that has no practical limits as to what information it can absorb, maintain, and index for speedy retrieval.

From an information systems perspective, the real time capture and storage of every social activity within a digital space raises compelling research questions. There is the opportunity to model behavior based on a richer data set than has ever been collected. The digital recording of interactions, that in offline settings leave no trace, is an important subject for additional exploration. The existence of these recordings, with no stated expiration date, can cause social and personal disruptions. All these issues are highly compelling, and deserve further study.

1.3 Relevance to Information Systems Research

This research dissertation describes a study of social networking sites, a type of information system used by individuals, primarily for their own enjoyment. As millions of people join these sites and begin to share and interact, the amount of potentially sensitive information saved is growing enormously. Concerns regarding the privacy and fundamental security of this information have been the subject of a rigorous public debate by parents, educators, and law enforcement personnel (Chiaramonte & Martinez, 2006; Hempel, 2005; Schrobsdorff, 2006; Stone, 2007).

How is the privacy of this information being maintained? How can it be maintained more effectively and safely? These are important questions, but ones that today cannot be clearly answered. Even though privacy management has been targeted as a grand challenge by the Computing Research Association (CRA, 2003), there is no established definition as to what exactly is meant by effective privacy management. Nor has it been determined what factors influence that effectiveness. For all intents and purposes effective privacy management has not been defined. Therefore, this research is relevant to information systems because it will contribute to a definition of effective privacy management.

This research is also relevant to important concerns developed in prior information systems research. This topic captures the interaction of social and technical components, a traditional focus of information systems. Important theories in information systems have been developed to describe use of systems within an organizational context. It is not known to what extent these theories relate to system use in a non-organizational context. The consideration of systems used outside of an organizational context has

begun to gain some attention, specifically the application of the Technology Acceptance Model to hedonic information systems (Van der Heijden, 2004). Within hedonic information systems, the primary motivation for users is personal pleasure.

How can the effectiveness of hedonic information systems be determined? Are theories from information systems relevant to this question? How do these theories need to be adapted to account for the removal of organizational context? Do social norms play a similar role as organizational context? This research will not answer all of these questions, but a better understanding of the use of privacy management within social networking sites obtained by application of Adaptive Structuration Theory will be a step in the right direction.

1.4 Research Question

The problem this research dissertation addressed is how to produce a clearer picture of current privacy management practices. This was accomplished by developing empirical measures that capture the appropriation process with regard to privacy management on social networking sites. A deeper understanding of the appropriation process can help define factors influencing the effectiveness of privacy management. Using the terminology of Adaptive Structuration Theory (DeSanctis & Poole, 1994), one measure of a system's effectiveness is the degree to which users appropriate that technology in a positive and faithful way.

The steps that were taken to solve this problem are the following. Measures for appropriation moves related to privacy management in social networking sites were administered to members of two different social networking sites, Facebook and

MySpace. These sites were selected due to their differing philosophy with regards to privacy management. The results were analyzed, and the measures for appropriation moves were validated. Correlation functions tested the degree of association between an implementation of privacy management and an individual's appropriation moves. In addition, correlation functions were applied to determine the relationship between privacy concern, frequency of use, and the nature of appropriation moves.

1.5 The Scope of This Research

The scope of this research was an analysis of privacy management on two specific social networking sites. The population for the study was not the full population of these two sites. Instead it was drawn from a smaller population, i.e., those members of the NJIT community that participate in these sites. This includes students, faculty, staff and alumni. The measures of interest captured information on appropriation moves with respect to privacy management. These are new measures that have not been subjected to a rigorous test of validity and reliability. The results from this research provide a preliminary test of these measures.

While the larger research question is a definition of effectiveness with respect to privacy management, this research will not be able to address the full scope of such a definition. It sheds light on just one aspect of effectiveness. Specifically, it illuminates the relationship between two particular implementations of privacy management and how they are appropriated by members of those sites.

1.6 Dissertation Outline

This dissertation documents the theoretical development and justification for a research plan to study the appropriation of privacy management within social networking sites. The specific nature of social interaction within social networking sites, along with a summary of prior research, is described in Chapter 2. Chapter 3 provides a brief summary of the theoretical foundation of this dissertation. It provides an overview of Adaptive Structuration Theory (DeSanctis & Poole, 1994), which emphasizes the importance of appropriation, and the Fit Appropriation Model (Dennis, Wixom, & Vandenberg, 2001), which describes how system design can influence appropriation. Chapter 3 also describes socio-technical systems theory.

Chapter 4 breaks out in more detail the exact functioning of privacy management within two social networking sites. This chapter describes and analyzes known problems with the current state of privacy management, and argues that these problems can be better understood and documented by applying an appropriation perspective.

Chapter 5 introduces a new conceptual model that describes the development and use of social software. The Social Software Performance Model extends the Fit Appropriation Model by adding a feedback loop from socio-technical systems theory. Chapter 5 also describes the research questions and hypotheses tested in this research.

Chapter 6 describes the design of the research instrument and an explanation of the new measures introduced in this research. Chapter 7 describes the survey methodology and provides univariate results. Chapter 8 provides a summary of qualitative data captured with the survey. Chapter 9 describes the results of multi-variate data analysis, which includes reliability tests, factor analysis, and evaluation of

hypotheses. Chapter 10 describes the results of testing of the research model using partial least squares (PLS) analysis, and provides a discussion of the research's overall results. Chapter 11 provides an extension of the model, supported by additional PLS analysis and a summary of qualitative data. Chapter 12 presents summary and conclusions. The appendices include a table of missing data, the consent form, the survey instrument, and a copy of NJIT IRB approval, a summary of pilot studies, followed by references.

CHAPTER 2

A REVIEW OF SOCIAL NETWORKING SITES

This chapter provides an overview of social networking sites. It will explain the history of these sites, how people use them, and describe the nature of online profiles and linked social networks. It also includes a summary of academic research in this area. Although this is a very new field and research has only been published in the last few years, there have been important ethnography studies, as well as intensive studies of use associated with a particular university.

2.1 Definition of Social Networking Sites

Social networking sites are online destinations where members present a digital profile, show their online social network, and maintain or develop new online relationships. boyd and Ellison define social networking sites as “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system,” (boyd & Ellison, 2007).

The concept of a social networking site dates back to the 1960s, with the Plato computer based education tool, developed at the University of Illinois. The first contemporary social networking site, SixDegrees.com, was launched in 1997 (boyd, 2004). SixDegrees.com derived its inspiration from the phrase “six degrees of separation,” made famous in the small world experiments conducted by Stanley Milgram,

who proposed every person could be connected to every other person by no more than six or seven connections or hops (Milgram, 1967).

Members of SixDegrees.com created profiles, and then started making connections to other members. These two ingredients make up the basic functionality of a social networking site, but this version did not achieve critical mass and it shut down in 2000 (boyd & Ellison, 2007). SixDegrees.com was just a little ahead of its time, because a few years later significant increases in communications bandwidth coupled with a sharp drop in the cost of data storage dramatically changed the business model of these sites (Dwyer, Hiltz, & Widmeyer, 2008).

The first commercially successful social networking site was Friendster. It was launched in beta during the fall of 2002, and by January 2004 had acquired over five million members, basically by word of mouth (boyd, 2004). Friendster benefited from better alignment with the marketplace. By the time it came online, there were existing cyber-connected social groups plus an improved telecommunications infrastructure in place. Friendster was a hit with several close knit communities, specifically gay men, bloggers, and participants in the Burning Man festival (boyd & Ellison, 2007).

The components of Friendster have set the model for the social networking sites that followed. Friendster members show a profile with demographic information, interests and relationship status. Members can link to other members, a process called “friending” (boyd, 2004).

In addition, members can write and post public testimonials that are addressed to one friend, but visible to anyone viewing that profile. Boyd and Ellison identify friending and testimonials as the key functionality that moved Friendster away from simple dating

sites (boyd & Ellison, 2007). Friendster was a bridge between dating sites and the social networking sites that have since emerged. In addition to its use for dating, Friendster became a platform for electronic self presentation and cyber-identity construction. The elements of this construction include manipulation of image, expansion of social networks, and a good dose of competitiveness and voyeurism (Donath, 2007). Self presentation within a digital platform greatly expanded the possible ways to “perform” your identity, making the profile a creative, competitive and dynamic performance, rather than a static representation.

2.2 Typical Use

When people join social networking sites they first create a profile, then begin making connections to existing friends as well as people they meet through the site. The profile is a list of identifying information. It can include your real name, or a pseudonym. It also can include photographs, birthday, hometown, religion, ethnicity, and favorite movies, music and books.

After creating a profile, members begin to make connections with other members. This is typically done by sending a “friend” message, which must be reciprocated by the other party. “Friending” another member gives them access to your profile, adds them to your social network, and vice versa. The size of these friend networks quickly becomes large, and seems to be an object of competition among members. An illustration of this can be seen at the University of California, Davis, where students created a Facebook varsity team. Membership is limited to those with 500 UC Davis friends or more. As of

June 2006, the leading student had 1,365 friends in their UC Davis network (DavisWiki, 2006).

With a profile and a social network, members use these sites for a number of purposes. The root motivation is communication and maintaining relationships. Members take advantage of the ability to publish digital content in various formats. Popular activities include updating others on activities and whereabouts, sharing photos and archiving events, getting updates on activities by friends, displaying a large social network, presenting an idealized persona, sending messages privately, and posting public testimonials (and having others post to theirs).

2.3 Examples of Social Networking Sites

Social networking is now one of the most popular activities on the Internet. Social networking sites have evolved around a variety of interests. They include business (LinkedIn and Ryze), meeting others (Orkut and MySpace), receiving and giving recommendations (Tribe), and photo sharing (Flickr). Sites have developed that target pre-teens (ClubPenguin), and are associated with particular schools (Facebook). Here are descriptions of two popular social networking sites that will be the focus of this research dissertation.

2.3.1 Description of Facebook

Facebook was created in February 2004 by Mark Zuckerberg, a student at Harvard University. Harvard distributed a hard copy “face book” that included information about each member of the freshmen class. Zuckerberg decided it would also work very well as an online resource. When first introduced, Facebook was for college students only. You

needed to have a valid school email address in order to obtain an account. In 2005 Facebook opened the site to high school students, and as of 2007 membership became available to anyone. Recently it has become the focus of academic research, perhaps because of its association with colleges and universities (Hempel, 2005).

2.3.2 Description of MySpace

MySpace is among the most popular and fastest growing social networking sites, drawing more traffic on the Internet on a consistent basis compared to nearly any other web site¹. MySpace has also been the focus of much public concern from parents, educators, and law enforcement (Chiaramonte & Martinez, 2006; Hempel, 2005; Schrobsdorff, 2006; Spring, 2007; Stone, 2007).

Despite its large size and controversial reputation, MySpace has not been the focus of a great deal of academic research. This is partly due to the rapid development of social networking sites, blooming so quickly that academic research is just beginning to catch up. MySpace is popular among both established and aspiring musicians, providing a platform for presenting samples of their work.

What functionality do social networks provide? Social networking sites feature a combination of the following functions (Webb, 2004):

- **Identity:** who you are, and how you want to be presented to others. This is implemented through profiles. Profiles are opportunities for members to create a digital self presentation of their interests and characteristics. There is often great variability in what features the social networking sites makes available. Since the creation and maintenance of a profile is the main method in which users 'present' themselves to other users, skilled management of your profile has an impact on your ability to make new connections and friendships.

¹ www.alex.com, accessed on 7/2/07

- **Presence:** this is an indication of whether a user is available for synchronous chat. It indicates whether you are online and using the site.
- **Relationships:** this is the representation of your social network. It includes how friendships with others are presented, and to what degree those relationships are visible to others.
- **Conversations:** This feature refers to mostly asynchronous communication. These typically involve private one to one messages, or public postings, where communication between the author and target is displayed in a public area visible to others on the site.
- **Groups:** Groups enable networks organized around a club or activity to form. Most sites allow ad hoc groups to be established and maintained with conferencing functionality.
- **Reputation:** This feature refers to how social norms are communicated to members. This can take the form of ranking systems, among all users or within a friend's network. For example, in MySpace, a user can specify their "top eight," or the eight friends they wish to have displayed along with their profile. This limit is both an interface issue (there is just so much space for "friends") as well as a key component of a reputation system.
- **Sharing:** One of the most popular activities in social networking sites is sharing of multimedia, such as pictures, video, and songs. Facebook allows users to set up albums of photographs, and tag friends within the photos. MySpace has available digital copies of many artist's popular songs, which can be loaded into your profile and played when the profile is accessed.

2.4 Defining Your Online Identity

In Facebook and MySpace, the profile performs several important functions. It is the home base of the member. It contains links to all their photographs, messages, and links to friends. It is a persistent representation of a member's identity, which can be continually updated.

facebook Profile edit Friends Networks Inbox

Search

Applications edit

- Photos
- Groups
- iLike
- Events
- Marketplace
- Causes
- more

HSBC Mortgages
We'll cut the closing costs
You cut the grass.
www.hsbc.com

ABC.com Season Premieres
Watch full episodes of
Dancing With The Stars, The Bachelor & more!
abc.com/player

ABC.com Season Premieres
Watch full episodes of
Dancing With the Stars, The Bachelor & more!
abc.com/player

Free Streaming Stock Quotes - Scottrade
Live stock charts.
Streaming interday, daily and weekly charts.
www.scottrade...

Cathy Dwyer
is writing her dissertation proposal.
Updated last Wednesday edit

Networks: NJIT Alum, Pace Faculty, New York, NY

Sex: Female

Relationship Status: Married

Birthday: October 29

Hometown: New York, NY

Political Views: Other

Mini-Feed
Displaying 1 story. See All

Today

P Cathy started listening to a station on Pandora.
Feist Radio

Information

Contact Info edit

Emails: cad7@njit.edu, cdwyer@pace.edu, profcdwyer

ATM:

Personal Info edit

Activities: Lecturer in IS at Pace University

Interests: Here is a great example of a mashup. Looking for a new apartment? Go to <http://www.housingmaps.com/> to search by city and price. You can even find places to live in NYC for less than \$750!

Favorite Music: New stuff on the Internet. Check out <http://jamiestreet.com>. It is a combination indie music download store and social networking site. You can download some songs for free, or buy others (some for 14 cents). Amazon.com just bought a stake in them. Wonder if it will give iTunes a run for its money.

Favorite TV Shows: Johnny Cash, Regina Spektor, Citizen Cope, Bob Marley, State Radio, Fiest

Favorite Movies: CSI, Entourage, 24, MythBusters

Favorite Books: The Matrix, Motorcycle Diaries, Capote, Chinatown

Biography of LBJ by Robert Caro, Secret Knowledge by David Hockney, Presentation of Self in Everyday Life, Guns, Germs and Steel

NJIT Friends
11 friends at NJIT. See All

Figure 2.1 Cathy's Facebook profile.

Figure 2.1 is an example of a profile from Facebook. It includes a photograph, contact information, personal information regarding interests and activities, and links to Cathy's friends on Facebook. Profiles are also part of MySpace, and have similar components (see Figure 2.2).

From a functional perspective, the profile acts as a portal into the site. It contains tools for self expression and identity construction (Lange, 2007; Liu, 2007). According to

the social-identity theory, people have many identities that are developed and relate to structured relationships with others (Lindzey & Aronson, 1985).

In both Facebook and MySpace, members have a public area where friends can post comments. In Facebook this area is called “The Wall,” in MySpace it is called “Friend’s Comments.” It is the virtual equivalent of a public whiteboard on your office or dorm room door. Friends can write notes for you, but they are visible to anyone else who looks at your profile.

Comments or wall postings are usually short statements, sometime meant to be funny or silly. The public nature of the comment adds to their importance. It is an example of signaling, i.e., publicly indicating both the friendship relationship and the nature of your message. Included along with the message is a picture of the person who posted it.

As described in (Donath & boyd, 2004) and (Donath, 2007), the public nature of both profile construction and public messaging can be understood in the context of signaling theory. Signaling theory, borrowed from economics and biology, is a study of the relationship between public signals and the values and meaning they transmit. In biology, a gazelle will jump wildly up and down, rather than running off when it sees a predator. The intended signal is that the animal is too fast to catch, because otherwise it would not waste time jumping up and down. Of specific interest to signaling theory is explaining why certain signals are found to have reliability while others may not. One way to measure the reliability of a signal is to examine the consequences of the signal being deceptive. In the case of the gazelle, the cost for wasting time jumping up and down if the animal is really not that fast is that it will be caught by a predator. In general,

the idea is that the consequences triggered if a deceptive signal is uncovered must be substantial for it to be considered reliable.

Lifting a heavy weight is an example of an assessment signal, and it is considered a reliable signal of strength. Another type is referred to as a conventional signal, which is not considered as reliable. For conventional signals, it is social convention, not an externally validated quality, which signals the intended value. It is really social norms that reinforce the value of conventional signals, and these signals are relevant to understanding the creation of a profile and connection to an online social network.

Within social networking sites, a member's profile, plus their online social network, along with the comments they post, all can signal the value of relationships with others. By agreeing to be publicly identified as a member of your online social network, a friend is signaling the value of your relationship. In the offline as well as the online world, people are judged based on the company they keep.

Profiles provide a platform for sharing of media, for example music and videos. One factor in the success of these sites is their ability to provide integrated tools for personal multi-media publishing (Dwyer et al., 2008). In addition to sharing video, many participants are active creators and distributors of video content. Inexpensive digital video cameras and editing software for desktop computers have opened this arena as an active platform of self expression. Lange has published a study on how the creation and distribution of video influences online social networks. She has found that the public nature of video publication has an influence on the techniques creators employ in describing their identity (Lange, 2007).



Figure 2.2 A profile from MySpace.

2.5 Growing Your Social Network

After creating a digital profile, new members of social networking sites actively begin to make connections with other members of the site. The process of adding to your online social network is referred to as friending. The friend relationship in social networking sites is reciprocal. In order for a new person to be listed as your friend, both must acknowledge the relationship. Then the friend link becomes part of both social networks.

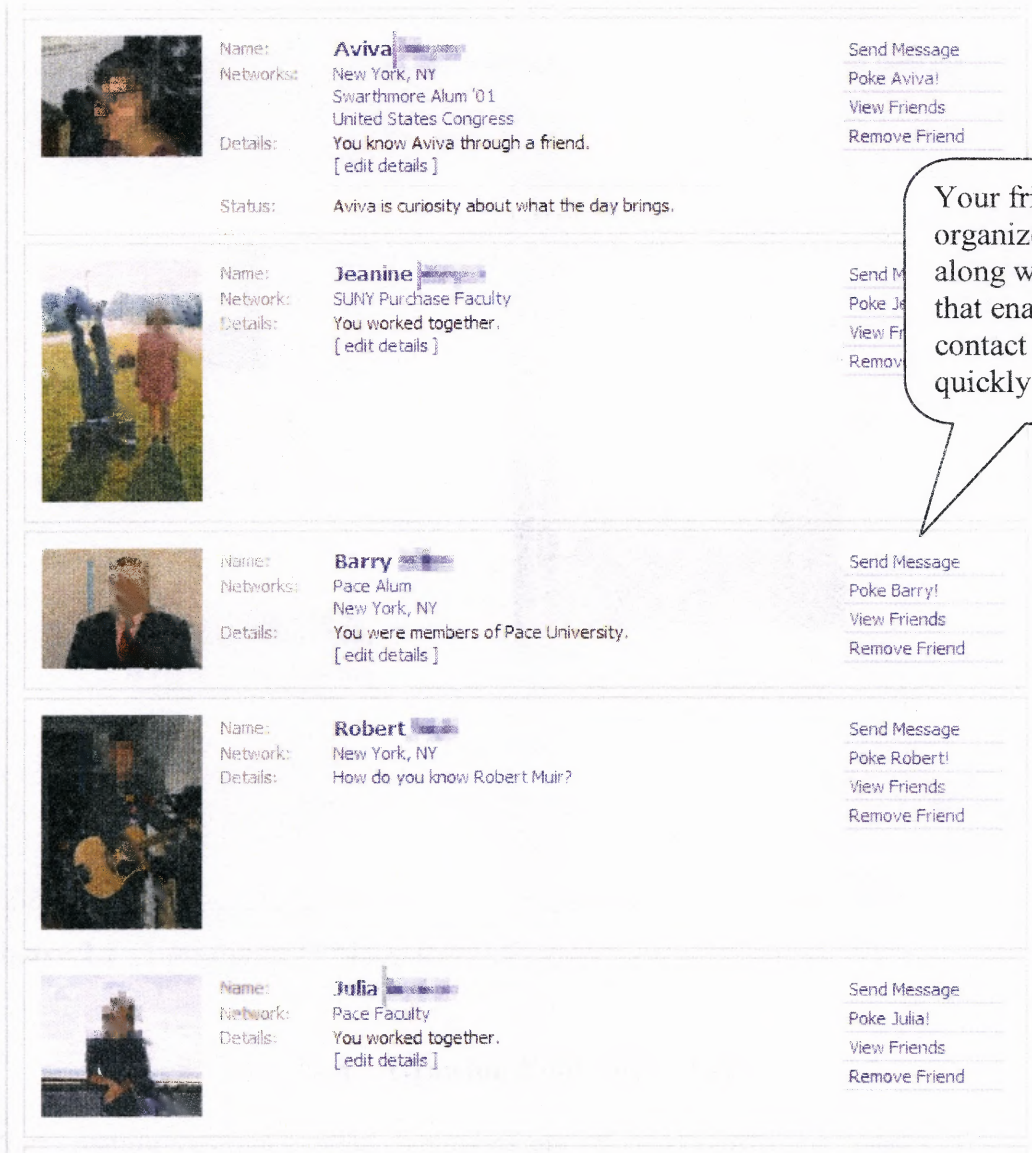


Figure 2.3 Friends are organized in a list, and are easy to see and contact.

An advantage that social networking sites have over other methods of computer mediated communication such as email or instant messenger is that communication can be organized by person rather than by tool. You do not need to remember someone's obscure email address or instant messenger screen name. Now you can find their picture in a list of your friends, and choose from a variety of quick links to initiate contact (see Figure 2.3). In addition, your friend's profile can serve as an entry in your digital address

book. If it turns out you need to contact a friend via another mode, such as email or even phone, you can look up their contact information on their social networking profile. When a member updates contact information on their profile, these updates are available to all their friends, who do not have to struggle with outdated contact information residing in email address books or instant messenger buddy lists.

2.6 Social Implications of Social Networking Sites

Social networking sites are rapidly evolving socio-technical systems. This can create differences in expectations and circumstances of conflict between the users and creators of social networking sites.

danah boyd (who, like e.e. cummings, does not capitalize her name) has published a series of articles that explore the social implications of the use of these sites. The basis of her research has been an intensive ethnographic study of social networking sites, beginning with Friendster, but over time expanding to include other sites, such as MySpace. She has carried out hundreds of in depth interviews with users of social networking sites, conducted dozens of focus groups, and by setting up identities on these sites, has gained access to thousands of profiles (Donath & boyd, 2004). With Jeffrey Heer, she has used a visualization tool to analyze the nature of connections between members of Friendster (boyd & Heer, 2006).

boyd and Ellison (2007) note that many social applications, such as buddy lists (from instant messenger) and blog rolls (lists of favorite bloggers) contain the structure of social networks both implicitly and explicitly in their design. It is the successful ability to represent a social network both visually (through photos of its members) and dynamically

(providing active links as well as information about social connections) that has driven the popularity of social networking sites.

How does the use of technology change the nature of social interaction? boyd and Heer suggest that “the architectural structure of digital life alters the ways in which conversations can and do occur . . . digital communication now incorporates multiple forms of media bridging the physical and digital,” (boyd & Heer, 2006). They argue that the components of one’s profile, for example blogs and photo albums, can be thought of as elements of an ongoing conversation. Social interaction also changes because the simultaneous private and public nature of profiles is not consistent with traditional (i.e., offline) understanding of communication and self presentation.

Creating an interesting profile gives someone status within a social networking site. It enables active connections with friends. It also brings up the challenge of negotiating connections with an unknown audience. Donath and boyd (2004) describe a case where a teacher was approached by her students, who asked her to “friend” them. While she was comfortable with the nature of her own profile, upon consideration, she had concerns about some of the risqué elements in her friends’ profiles. This left her in an awkward social position – uncomfortable with turning down students, and uncomfortable with sharing the private details of her out of school social network.

Social status is a function of many factors, and these can be seen in the construction of profiles. Members of social networking sites work to display many layers of their social status, from the quality of ones’ social network to the “tastefulness” of ones’ cultural preferences. An intensive analysis of over 120,000 profiles on MySpace found that expression of identity through profiles is made up of four general “taste”

statements. These statements convey prestige, differentiation, authenticity, and theatrical persona (Liu, 2007).

An important factor related to the conflict between public and private is how members communicate context as they present themselves. Offline, “friend” relationships have many levels. People develop relationships with work colleagues, neighbors, school friends and family. Within these relationships there are also degrees of closeness. On social networking sites, the friend status is binary: friend or not. Since the friend status is the primary technical boundary used to control access to information, members have to consider that the information they intend to share only with close friends is likely to leak into other contexts. While on the surface members seem blasé about unknown others viewing their profile, there are two people that members greatly fear will view their profile: “boss and mother,” (boyd, 2006a).

boyd explores how technical features of social networking sites impact social interaction in (boyd, 2006b) and (boyd, 2007). Specifically, social networking sites enable profiles to be searched. They also allow profiles to persist, as well as be copied. By enabling search, this gives anyone with access to the site the potential to find you. This means members can not accurately define the potential audience for their profile. The consequences of a persistent digital identity mean that actions taken in the heat of the moment can remain visible well after tempers have cooled down. The ability of profiles to be copied can undermine trust in someone’s identity.

In addition, friending is a different process online compared to developing relationships offline. Acknowledging an online friend takes one click. Once the friend status is established, that connection will remain unless there is an explosive end to the

relationship. In addition, friending is another means of self expression. As more music and film celebrities develop profiles, members add them as friends as a way of specifying their tastes in music. The use of profiles for self expression was also found in a study conducted by Dwyer (Dwyer, 2007).

The migration of social networking to mobile devices is breaking down the barriers between offline and online social spaces. A year long ethnographic study of the use of Dodgeball, a mobile social networking service, found that the use of Dodgeball influences the way subjects behaved in public spaces and how they conducted social relationships. This study also found that due to the close relationship between early adopters and the designers of Dodgeball, there was a great deal of synergy between how the technology was used, and how it evolved over time. It presents a clear example of technology changing use, and use changing technology (Humphreys, 2007). This suggests that socio-technical theory can be used to explain use of these systems.

The performance aspect of profiles, driven by the need for self-expression as well as social competitiveness, can encourage active public sharing of information. The more you share, the more attention can get. However, all this shared information can be easily accessed by other parties. Liu and Maes found that it is relatively simple to harvest information from a profile and use it to generate recommendations (Liu & Maes, 2005). This raises privacy concerns, because this information can be used for other purposes besides recommendations, such as marketing or profiling of individuals by law enforcement.

2.7 Web Crawl Studies of Social Networking Sites

A web crawl is a program that is able to read all of the content on a web site and return that content in the form of a text file. Once the text file has been obtained, a program can be executed that will parse out relevant information and make it available for analysis. This technique has been applied by a number of researchers to examine the general use of Facebook by members of a specific university community. The school communities that have been studied include Carnegie Mellon University (Gross & Acquisti, 2005), Massachusetts Institute of Technology, Michigan State University (Lampe, Ellison, & Steinfield, 2007), and the University of North Carolina at Chapel Hill (Stutzman, 2006).

Gross and Acquisti collected data from the Carnegie Mellon Facebook site in June 2005. By searching for all “female” profiles, and then all “male” profiles, they were able to collect the profile IDs of 4540 members of Facebook at Carnegie Mellon.

From their dataset, Gross and Acquisti carried out the following analysis. They found that most of the profiles belonged to undergraduates (73.7%). The remaining profiles belonged to alumni (18.8%), graduate students (5.9%), staff (.8%), and faculty (.4%). Overall, 60.4% of the profiles were male, and 39.2% were female. This gender distribution is consistent with the population as a whole at that university.

Next, the authors analyzed what information the profiles contained. They found 90.8% include a profile image, 87.8% reveal their birth date, 39.9% list a phone number, and 50.8% list their current residence. The majority also list the relationship status, dating preferences (male or female), political views, and various interests. A web crawl study conducted at Michigan State University found that the amount of information displayed in the profile was weakly associated with the number of friends listed. This was

particularly true with respect to listing of high school, favorite music, AIM screen name, and birthday (Lampe, Ellison, & Steinfield, 2006).

The Carnegie Mellon study did not find that much difference in terms of what information is provided when comparing male to female profiles. The only significant difference was the phone number. More males than female users shared their phone number (47.1% versus 28.9%).

Stutzman conducted a study of first year students at the University of North Carolina, Chapel Hill (Stutzman, 2006). Stutzman carried out a longitudinal study in the fall of 2005, looking at adoption rates. He found that by the first day of school, over 85% of the freshmen class had an account and had established a profile on Facebook. Stutzman found the greatest months of profile creation happened in June in July, shortly after freshmen orientation events. The connection is that freshmen would obtain their school email address at these events, and this allowed them to create a profile on Facebook.

By tracking the profiles through the semester, Stutzman was able to measure the growth in the social networks of freshmen. The typical freshman showed a mean of 46 friends in early September, and by the end of the semester that number had risen to 111. Stutzman found that, as in the Carnegie Mellon study, students presented a lot of potentially sensitive information in their profiles. Stutzman found that more than three quarters of students displayed their birthday, hometown, sexual orientation, relationship status, and political orientation.

Two students at the Massachusetts Institute of Technology, Harvey Jones and Jose Hiram Soltren, created a script to collect profiles from Facebook (H. Jones &

Soltren, 2005). They used this script to collect profile information from the following schools: Harvard, New York University, Massachusetts Institute of Technology, and the University of Oklahoma. In total, they obtained 70,311 profiles.

As found in the study conducted at North Carolina, freshmen signed up for Facebook as soon as they obtained their school email address, which was typically in July or August before beginning their freshman year. The Jones-Soltren study found that freshmen, and also undergraduates in general, were more likely to disclose more information than graduate students or alumni. Freshmen and undergraduates are eager to expand their social networks, and the benefits of more exposure from disclosing information outweighs privacy risks. As students get older, and especially as they get ready to begin a career, then privacy risks have greater weight.

Because this study looked at four schools, there is the opportunity to compare patterns of disclosure between schools. For example, Harvard had the lowest percentage of visible profiles (66%), with Massachusetts Institute of Technology having the highest (79%). 91% of Oklahoma first year students share their major, compared to 64% at Harvard. This suggests that cultural differences at schools are expressed in the Facebook population as well.

2.8 Privacy and Social Networking Sites

The privacy implications of the use of social networking sites are substantial. In general, the level of anxiety about privacy online is quite high, but its relationship to behavior is muddled. A study by (Acquisti & Gross, 2006) indicates people make decisions on whether to reveal information online in unpredictable ways.

Members of social networking sites have publicly expressed a blasé attitude with respect to privacy. Alice Mathias, a recent college graduate describes her feelings about Facebook in an op-ed column in *The New York Times* this way: “My generation has long been bizarrely comfortable with being looked at, and as performers on the Facebook stage, we upload pictures of ourselves cooking dinner for our parents or doing keg stands at last night's party; we are reckless with our personal information,” (Mathias, 2007).

However, this lack of concern does not apply to all aspects of online privacy. When privacy issues have the potential for embarrassment or may trigger unintended consequences, Facebook members do express concern. As Mathias explains:

There is one area of privacy that we won't surrender: the secrecy of how and whom we search. A friend of mine was recently in a panic over rumors of a hacker application that would allow Facebook users to see who's been visiting their profiles. She'd spent the day ogling a love interest's page and was horrified at the idea that he knew she'd been looking at him. But there's no way Facebook would allow such a program to exist: the site is popular largely because it enables us to indulge our gazes anonymously. (We might feel invulnerable in the spotlight, but we don't want to be caught sitting in someone else's audience.) If our ability to privately search is ever jeopardized, Facebook will turn into a ghost town.

People have become comfortable with using credit cards, rarely change permission levels and make their calendar public to co-workers to enable collaboration. Yet surveys indicate concern is increasing. Jonathan Grudin suggests this concern is caused by a condition he calls digital immortality.

Why then the uneasiness, the widespread attention to privacy? It may reflect an awareness at some level of something more fundamental than privacy being challenged: the steady erosion of clearly situated action. We are losing control and knowledge of the consequences of our actions, because if what we do is represented digitally, it can *appear anywhere at any time in the future* [emphasis added]. We no longer control access to anything we disclose, (Grudin, 2001).

With respect to the privacy of information on social networking sites, there are increased reports of the unintended consequences of disclosure. A “hack” that allowed anyone to view the private messages of a MySpace account was posted on the Internet, resulting in the publication of personal messages between Ashley and Jessica Simpson, two sister celebrities, discussing intimate topics (BestWeekEver, 2006).

Employers are searching these sites for background information on applicants. University and high school administrators use these sites to monitor student behavior. One episode had dire consequences for the students involved. Two members of Louisiana State University’s swim team were dismissed from the squad and stripped of their scholarships after creating a Facebook group, called the “Fantastic Four Coaches,” and complaining about poor coaching at last year’s Southeastern Conference championships (Read, 2006).

Social networking sites thrive on interaction fed by sharing of personal experiences and insights. However, unlike telling stories in a neighborhood pub, the information shared within social networking sites can take on a life of its own. A great deal of the public concern and academic research with regard to social networking sites has focused on the privacy implications of their use. This issue is described in the next section.

2.9 Privacy Issues and Internet Use

Privacy has been a difficult concept to define because it has social and cultural contexts that have developed over thousands of years (Lessig, 1998). Tavani (Tavani, 2000) describes three types of privacy:

- Accessibility privacy – freedom from intrusion
- Decisional privacy – freedom from interference in your personal choices, for example reproductive rights
- Informational privacy – person’s ability to manage the sharing and exchange of their personal information

Within the computing research community informational privacy has received the most attention. This is because so much of our personal information is now managed by computers. For example, Minch identifies privacy as the ability to control access to information, describing it as the “extent to which persons can control how information about them is: (1) collected; (2) retained and/or maintained; (3) used; and (4) communicated, disclosed or shared,” (Minch, 2004).

For online privacy management, the above definition of the information privacy perspective is the functional definition of privacy that has informed the current design of privacy management systems.

2.9.1 Development of Internet Privacy Scale

Buchanan, Paine and Joinson have conducted research in order to create validated scales that measure online privacy concern. The authors developed three scales that measure privacy attitudes (privacy concern) and behaviors (general caution and technical protection). The scales were validated in a series of three studies (Buchanan, Paine, Joinson, & Reips, 2007).

Although other privacy scales exist (specifically Westin), none were focused on the nature of privacy with respect to the Internet. Following a literature review of privacy research, the authors created a set of 82 questions, focusing in on a number of dimensions. Questions related to informational privacy (e.g., “Are you concerned that

you are asked for too much personal information when you register or make online purchases?”), accessibility (e.g., “Are you concerned that information about you could be found on an old computer?”), physical privacy (e.g., “Are you concerned about people viewing your screen over your shoulder when you are online?”), expressive privacy (e.g., “Are you concerned that an email you send someone may be inappropriately forwarded to others?”), and possible benefits of surrendering privacy (e.g., “How acceptable is it that personal information provided online can be used to speed up log in / purchases?”; “How acceptable is it that law enforcement agencies track users of websites to track criminals?”). Questions addressed actions taken to protect privacy (e.g., “Do you clear your Internet browser history regularly?”) and privacy attitudes (e.g., “Are you concerned who might access your medical records electronically?”).

These 82 privacy related questions were tested in an online survey completed by 515 subjects. Analysis of the results indicated that a three factor solution. The first factor included questions regarding general caution and concern with the protection of privacy (attitudes). The second factor includes questions that reflect the use of technology to take steps to protect privacy and prevent intrusion (behavior). The third factor includes questions that relate specifically to Internet privacy concern (attitudes). A subset of these questions will be used in this study.

In order to test the external validity of these scales, the questions were repeated in a study that also included other privacy measures, specifically the Westin privacy questionnaire (1996) and the Internet Users Information Privacy Concerns scale (Malhotra, Kim, & Agarwal, 2004).

The results for the new scale measuring Internet Privacy Concern was compared to these established scales. With the exception of the relationships between the Westin Privacy score and Privacy Behavior: General Caution, all other correlations were positive and significant. This provides external validity to the three Internet privacy scales.

2.9.2 Informational Privacy Research

Smith, Milberg, and Burke (Smith et al., 1996) published the results of an information privacy scale in MIS Quarterly. Their goal was to develop an instrument to identify and measure the primary dimensions of an individual's concern regarding organizational privacy practice.

In order to develop their scale the authors began with an examination of privacy literature. They next carried out experience surveys and conducted focus groups. The results of these steps were reviewed by expert judges. This resulted in a 15-item scale with four subscales. The instrument was repeatedly tested across several heterogeneous populations, and the results show a high degree of confidence in the scales' validity, reliability, and generalizability.

Smith et al. identify four subscales within concern for information privacy:

- Collection – concern regarding the increasing amount of personal information being collected
- Errors – concern that errors and mistakes can end up in databases and remain and be difficult to remove
- Unauthorized Secondary Use – concern that personal information collected for one purpose may be applied to a different purpose without the individual's knowledge or consent
- Improper Access – concern that private information is not secure, and may be accessed by unauthorized persons.

The themes of informational privacy can be summarized by the following theories. Fried's control theory of privacy means you have privacy only if you have control over the information about yourself. The limitation theory described by Allen defines privacy as the ability to limit access to your personal information depending on the context. The control/restricted access theory by Moor defines privacy as the protection against intrusion, interference, and information access by others (Lawler & Molluzzo, 2005).

The Westin model of privacy is perhaps the most widely used in all of privacy research. Yet its construct validity for complex computing systems seems to be suspect. The Westin model is based on how subjects reply to three questions:

- "Consumers have lost all control over how personal information is collected and used by companies."
- "Most businesses handle the personal information they collect about consumers in a proper and confidential way."
- "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today," (Westin, 1996)

Westin's method takes the answers on these three questions and divides subjects into three categories: privacy fundamentalists (very high privacy concern), the pragmatic majority (a middle group with balance privacy attitudes), and marginally concerned (little or no concern).

2.9.3 Informational Privacy Within Social Networking Sites

The research on informational privacy constructs has been extensive and influential. However, the definition of privacy within the informational research community is not compatible with the nature of online interaction, especially as it is carried out within

social networking sites. Social networking sites can consist of millions of members. How practical is it for members to consider how they want to manage the availability of their profile to people they do not know and may never encounter?

In addition, the focus on individual control of privacy does not take into account the privacy concerns of the network itself. Within social networking sites, privacy functions center on the individual. These sites need to consider network effects, and the impact of privacy breeches on the extended group. Within social networking sites, there are private data, public data, group data, and community data. Within a college's network on Facebook, for example, access to any profile within that network is the default privacy setting. Even if members are aware of this access, the access to the network itself by someone outside the school is an additional privacy threat for the group as a whole. All that is needed to access a school network is a valid email address, or a relatively easy hack of another member's logon information. For example, alumni at most schools can obtain a college email address. They may be acting in fact as law enforcement personnel or potential employers, gaining through their own account default access to a school's entire network. All the focus is on the privacy of the individual, without any rigorous methods to assure the privacy of the group (Backstrom, Huttenlocher, Kleinberg, & Lan, 2006).

Another limitation of the information privacy perspective is that it does not take into account expectations of privacy that arise in instances of self disclosure from one individual to another. According to the Communications Privacy Management Theory, privacy management involves a fluid definition and evolution of privacy boundaries between and among people. When a person discloses information from one person to

another, there is a clear expectation that both parties have a responsibility to maintain the privacy of that shared information (Petronio, 2002). The information privacy perspective does not look at two privacy expectations, only one way privacy expectations.

2.10 Privacy Implications

A number of researchers have studied the use of social networking sites with the aim of determining the scope of information that members are willing to reveal. Gross and Acquisti, as discussed in Section 2.7, conducted a study at Carnegie Mellon University, extracting 4540 profiles, “virtually the entire CMU Facebook population at the time of the study,” (Gross & Acquisti, 2005, p. 78).

The vast majority of profiles included personal information directly related to identity. The study found that 90.8% of profiles contain an image (photograph), 87.8% of users reveal their birth date (a key piece of information for identity theft), 39.9% list a phone number (including 28.8% of profiles that contain a cell phone number), and 50.8% list their current residence.

The majority of users also disclose their dating preferences (male or female), current relationship status (single, married, or in a relationship), political views (from “very liberal” to “very conservative”), and various interests (including music, books, and movies). A large percentage of users who self-identify as “in a relationship” (62.9%) include a link to their partner’s Facebook profile.

While all this information does raise privacy concerns, the question that needs to be asked is why are millions of people revealing all this information? The first public phone book appeared in 1880 (Coughlan, 2006). How is a profile different from a listing

in a public phone book? When many people can find references to themselves or others through Google anyway, how does including this information in a social networking sites change their privacy status?

Even after removing privacy concerns from the equation, there must be a positive benefit to the individual who creates and manages their profile, otherwise they wouldn't do it in the first place. What these surveys do not uncover is what benefits or value do subjects derive from creating a profile and including personal information? Does the revelation of more personal information improve their enjoyment and perceived usefulness of the site?

What risks does the subject trigger by revealing this personal information? What benefits do they obtain? Millions of people would not fill out these profiles without an expectation of a benefit. What is their expected benefit? How do they balance privacy tradeoffs against that benefit?

2.10.1 Privacy Risks From Information Disclosure

Gross and Acquisti conducted an analysis of privacy risks associated with the use of Facebook, then conducted an analysis of profiles within their dataset to determine who was particularly vulnerable to these threats.

With the information that a large number of students provide in their Facebook profile, it is quite easy to determine the physical location of students for large portions of the day. This can be deduced from either a student's class schedule or their dorm address. The study found 15.7% of female students and 21.2% of male students provide this information, making them vulnerable to real world stalking.

A larger proportion is vulnerable to cyber stalking through the use of AIM (AOL instant messenger). AIM allows users to add “buddies” without the knowledge or permission of the other party. Once added to a buddy list, a cyber stalker can keep track of when the other person is online. More than 77% of the profiles downloaded from CMU contain an AIM screen name.

A more subtle threat has to do with a technique known as re-identification, that can be used to link browsing activities for data mining purposes or to uncover sensitive medical information (Rosenblum, 2007). This is a threat, because a previous study showed that a large proportion of the US population can be re-identified using a combination of 5-digit ZIP code, gender, and date of birth. Overall, 45.8% of the members captured in the CMU dataset reveal their birthday, gender, and current residence, making them vulnerable to re-identification.

Re-identification also poses a risk with respect to identity theft. Including one’s birth date, hometown, current residence, and current phone number can enable a hack that can reveal one’s social security number. The first three numbers of a social security number indicate where that number was created. The digits come from the ZIP code in the mailing address of the application. The next two digits are group identifiers, and the final four are progressive serial numbers, (Gross & Acquisti, 2005).

Once a person’s hometown is known, it can be possible to determine the first three digits of their social security number. When that person’s birth date is also known, an attacker with access to the birth dates of others can pin down the range of possible values for the two digit group identifiers. The last four digits can be obtained through

social engineering, as they have become a semi-standard “pin” for many identity based transactions.

Based on a similar web crawl of four institutions, Jones and Soltren (H. Jones & Soltren, 2005) carry out a threat analysis. Noting that they were able to use accounts at four institutions to data mine tens of thousands of profiles in a week, they conclude that commercial data mining is not only possible, it is easy to do.

Another threat from Facebook that Jones and Soltren found is related to database reverse engineering. For example, you can use Facebook’s search tool to find members interested in “getting drunk,” or “smoking pot.” An advanced search of the NJIT and New York, NY networks found over 500 people otherwise unknown to the author interested in sex, 22 people interested in getting drunk, and six interested in smoking pot (including two members who graduated in 2007 from Catholic high schools).

Privacy risks within social networking sites were discussed in an article published in IEEE Security and Privacy (Rosenblum, 2007). For students who spend four years using social networking sites to document wild outings, boorish behavior, and insensitive or racist remarks, the idea of a prospective employer viewing one’s profile is quite frightening. As described above, access to these networks is quite porous, and it is naïve to assume that a profile public to some people is private to everyone else. Companies now use search engines and also access social networking sites to conduct background checks on prospective employees. This is especially valuable because federal fair hiring practices have restrictions on what questions can be asked in a job interview. As one hiring officer explained, “You really do get a lot of information you can’t ask for in the job interview, but you go on the Web and it is all there,” *ibid*, p. 46. As companies seek

to choose employees based as much on their values as their raw abilities, reviewing these sites is a way to determine if there is “something about their lifestyles that we might find questionable, or that we might find would go against the core values of our corporation,” *ibid.*

The implications of Internet information playing a role in the hiring process has been incorporated into a Harvard Business Review case study entitled “We Googled You,” (Coutu, Joerres, Fertik, Palfrey Jr., & boyd, 2007). This case study presents the hypothetical case of a recent Chinese American college graduate, Mimi Brewster, applying for a job at a luxury goods provider who hopes to grow its market in China. While Mimi speaks Chinese fluently, a search of the Internet finds that she played an active role in protests of China’s treatment of a dissident journalist. This case illustrates the dilemma faced by companies that use the Internet to investigate candidates. The company in question here faces one risk by passing on an otherwise excellent candidate, and a different risk by hiring someone who has publicly protested the actions of the Chinese government.

2.10.2 Use of Privacy Settings to Restrict Access

Gross and Acquisti were also interested in finding out if Facebook members from CMU made any changes to the default privacy settings. As a default, your name can be searched for by anyone on Facebook. You can change this on your privacy settings to restrict who will find you by entering your name. For example, you can restrict the ability to find you via a search on your name to just people who attend your school. But doing an analysis of data obtained via a web crawl, Gross and Acquisti found that only 1.2% of users (18 female, 45 male) had made the search function more restrictive.

Gross and Acquisti also analyzed how many CMU members restrict who at CMU can see their full profile. To do this, they established an account at other schools, and used accounts with varying degrees of connection with the rest of the CMU network to infer how individual users had selected their privacy preferences (this once again makes it clear that it is quite easy to establish accounts at other networks).

By default, your profile is searchable by everyone on Facebook. For example, you can search for any members who are fans of the singer Regina Spektor. Gross and Acquisti found that 1.2% of users (18 female and 45 male) had changed this to restrict searches to only those within the CMU network.

By default, your profile is visible to anyone in your school, whether you know them or not. Only three users (0.06%) in total had restricted access to their full profile for CMU students they did not know. Gross and Acquisti were quite blunt in their assessment: “We can conclude that only a vanishingly small number of users change the (permissive) default privacy preferences,” p. 77.

2.11 Attitudes Regarding Privacy

A study was conducted as a follow up to Gross and Acquisti’s analysis of the use of social networking sites at CMU. This study aimed to determine if there was a relationship between privacy concerns, and behavior with respect to privacy protection (Acquisti & Gross, 2006). A representative sample of CMU students was polled to determine their privacy attitudes, and their level of awareness as to privacy options available on Facebook.

First, it is important to note the strong penetration of Facebook use in this population. From the random sample that completed the study, 91.2% were current Facebook members. Therefore the privacy implications of Facebook use are especially relevant for this population.

This study found there was strong evidence of an attitude / behavior disconnect when it comes to privacy. Privacy concerns are a weak predictor of membership in Facebook. Individuals with high levels of privacy concern still join the network and reveal much personal information. For example, for those who expressed the highest level of concern about a stranger knowing of their class schedule and where they lived, 22% provided at least their address, and 40% provided their class schedule. Although the majority of Facebook members claim to know ways to control their profile's visibility and whether other members can search their profile, a significant minority are unaware of those options.

A study was conducted to compare attitudes regarding privacy and trust between two social networking sites (Dwyer, Hiltz, & Passerini, 2007). The same survey was administered separately to members of both sites. A total of 226 subjects participated, 132 from Facebook and 94 from MySpace. Privacy concern was measured using a subset of the Internet privacy concern scale described in (Buchanan et al., 2007). Five items were included, and the results had a Cronbach's alpha value of .886. No significant difference was found in the level of privacy concern for Facebook versus MySpace. Facebook members expressed significantly higher trust in the site, and its members. Facebook members were significantly more willing to include information, especially contact information, in their profile.

Despite high levels of distrust in the site and its members, MySpace members report much more activity using the site to meet new people, for example 40% reported meeting a MySpace friend face to face. This demonstrates again the attitude / behavior disconnect found in the Acquisti and Gross study (2006).

It appears that members may have a misplaced trust in the nature of these online social networks. For example, Facebook requires new members to have a valid email address if they want to join a college's Facebook network. This increases the expectation that all of the other information has somehow been validated as well. In most online social networks, security, access control, and privacy are weak by design. The presence of readily accessible information takes on a network effect. The more public information that is available, then the easier it will be for people to connect with others. And it follows that the easier it is for people to find connections with others, the higher the utility of the network to the users themselves and the commercial venture supporting it.

Therefore, the culture and the settings of these sites encourage members to provide vast amounts of personal information, which can then be searched by other members looking for points of contact. Despite the fact that Facebook offers granular and powerful privacy controls, its default settings are very permeable. By default a member's profile is searchable by any other member on Facebook, and is fully readable by any other member in the same school or geographic network. In addition, external access by non-students or other non-affiliated persons to a college's Facebook network is so easy that the network is effectively an open community, and its data is effectively public (Gross & Acquisti, 2005).

Consider the web crawl study conducted by Jones and Soltren, two MIT undergraduates (2005). They wrote a short Perl script, and used it to access and download over 70,000 profiles from the networks of four universities. Since they only had accounts on one university (MIT), it appears they used a friend's user name and password to collect profiles from the other schools. It appears to take only access to one profile to compromise the privacy of a school's entire network.

2.12 Discussion of Privacy and Social Networking Sites

Susan Barnes has written an essay that analyzes the public versus public boundaries of "social media spaces," (Barnes, 2006). An example of the fuzzy nature of these boundaries is evident when teenagers freely disclose information but are surprised when parents and school administrators read their profiles. Most current public efforts to curb the use of these sites deal with efforts to protect children from predators. Barnes argues the greater risk lies in the potential misuse of information. She argues that social, legal and technical solutions are needed to address the privacy paradox.

In an article intended to advise educators as to how they should participate in social networking sites, danah boyd discusses the differences between mediated public spaces like social networking sites, and unmediated public spaces that exist in physical space (boyd, 2007).

Mediated public spaces have the following functional characteristics:

- They are searchable
- Information persists in these spaces beyond the life of an encounter

- Information can be replicated or copied. This means a conversation can be copied from one context to another. It also makes it difficult to determine validity
- These spaces are public to unknown and unknowable audiences.

The presence of persistent, searchable, mediated public spaces changes all the rules about public social interaction. For one thing, it is quite difficult to interpret context in a mediated space. People learn to associate contexts of behavior to physical settings through socialization. “We know that the way we can act at the beach is different to how we can act in public lectures. I welcome anyone to show up to a lecture hall wearing a bathing suit, lay down a towel, and proceed to rub oil all over themselves,” *ibid*.

More than any other segment of the population, teenagers are grappling with the consequences of mediated public spaces. Their strategies take the following forms:

- They resumé-ify their profiles, pitching their self presentation to those who have power over their future. This is an adult-approved approach, but one that is disconnected from teens' social dynamics, that prioritizes socialization over adult acceptance.
- They include false names and information in their profile. This is also encouraged by adults, without thought as to what it means to suggest lying to solve social woes. However, it provides only weak protection, because motivated searchers can find someone through their friends.
- They demand adults understand that these sites are “*my* space” and subject to their own norms and standards.

This leads to an interesting ethical issue in modern life: “Just because it’s possible to get access to information, is it always OK to do so?,” *ibid*. Many parents argue that if it is public, they have a right to see it. However, there is evidence that social norms are beginning to evolve that respect this permeable boundary. A group of faculty members on Facebook have proposed the following as guidelines for Facebook use:

- Not friending students unless they request the connection.
- Accepting friend requests from all students (unless the instructor makes the decision not to friend students at all).
- Not looking at student profiles unless the faculty member has been friended by the student and even then using Facebook information judiciously and for educational purposes.

These analyses show that although the use of social networking sites is a new phenomenon, it is beginning to challenge established patterns of social interactions. In particular, the “always public” nature of these sites has brought up ethical issues for those whose interests intersect with its members. Parents, faculty members, and potential employers must learn how to navigate permeable digital boundaries.

2.13 Summary

The widespread use of social networking sites is a very new phenomenon. The first peer reviewed articles describing these sites were published in 2004. There has been little time to study the nature of the use of these sites in depth. This can be seen in the nature of the majority of studies to date, which are largely descriptive. These include ethnographic studies (most specifically boyd), and web crawler studies.

Even though the academic study of social networking sites is very recent, the study of the interaction between technology and society has been a significant focus of prior information systems research. There is already evidence that the use of these sites has changed the way its members develop and maintain relationships. boyd, through her early ethnographic studies of Friendster, describes how the creation of a profile as well as the visible presentation of one’s social network can be understood as a type of performance. This can encourage unfettered self expression, despite it being clear that the

actual audience for one's profile is unknown and unknowable. So not only does the use of technology bring about changes in the socialization process, but it also appears to amplify privacy issues.

This suggests that a deeper understanding of the impact of social networking sites can result from a more rigorous analysis of its socio-technical components. The next chapter explores prior research that is relevant to the interaction of social elements and technology, with the aim of applying it to findings that arise from the use of social networking sites.

CHAPTER 3

THEORETICAL FOUNDATION

There is a lack of theory that can explain the difference between success and failure by social networking sites, or provide advice to developers (Shneiderman, 2007). What theories are relevant to the usage and acceptance of social networking sites? For this chapter, prior research has been selected that explains complex interactions within socio-technical information systems. In the next sections the following research streams will be summarized: structuration theory and its application to information systems, the Adaptive Structuration Theory, the Fit Appropriation Model, and socio-technical systems theory.

3.1 Structuration Theory and Information Systems

Giddens' theory of structuration is the basis for research in information systems that address **appropriation**, or how people adopt and adapt technology to the tasks they need to complete (Dourish, 2003). The theory of structuration is based on "the duality of structure." What Giddens means by the duality of structure is that "the rules and resources drawn upon in the production and re-production of social action are at the same time the means of system reproduction," (Giddens, 1984, p. 19).

For Giddens, this duality explains the recursive nature of social structure. Human agents both draw on structure to guide their actions, and through their actions reinforce structure. Giddens argues that social structures fall into one of three dimensions: structures of signification (meaning or cognition), structures of domination (power and resource allocation), and structures of legitimation (sanctions and norms).

Giddens introduces the concept of **reflexivity**, which he defines as the innate capacity of humans to routinely observe and understand what they are doing while they are doing it (Giddens, 1984, p. 2). Reflexivity is based on the continuous monitoring of behavior, which “human beings display and *expect others to display* [emphasis added],” p. 6. In this regard, Giddens acknowledges the work of Erving Goffman, who carried out detailed ethnographic studies of impression management and self presentation (1959).

Giddens defines the domain of social sciences as “social practices ordered across time and space,” and argues that reflexivity is a key driver of “the recursive ordering of social practices,” (1984, p. 3).

Reflexive knowledge provides human agents with **mutual knowledge** that is drawn on to permit the re-creation of social structures, rituals, and organizational behavior.

According to Giddens, human agency consists of three interrelated processes:

- reflexive monitoring
- rationalization (discursive knowledge, or explanations human agents are able to express
- motivation – practical knowledge that human agents are usually not able to express

Of particular interest to information systems researchers is the belief by Giddens that social structures do not have a separate objective existence – they only exist as traces in the heads of human agents who use their practical knowledge of social structures to “‘go on’ within the routines of social life,” (Giddens, 1984, p. 4).

Nevertheless, these structures can be quite powerful. Consider for example wedding or burial rites that have survived for thousands of years. However, since these

ritual structures exist as social knowledge, it means that when they are enacted they are interpreted by a human agent. The interpreted nature of structure plus the reflexive character of human agents provides the potential both for structures to persist and for structures to evolve. It is this characteristic of Giddens' theory that appeals to information systems researchers, because it can explain both why things persist and why things can change (M. Jones, 1997).

The core of structuration theory is based on these points:

- Social practices, i.e., activity by human agents, are the foundation of the constitution of both individuals and society. This emphasis moves the focus of social theory away from (a) the individual actions and experiences of an individual actor (the subjective perspective) and (b) also away from the existence and requirements of an independent social structure.
- Human agents are knowledgeable and are able to exercise their powers to accomplish a social practice. People often know what they can do in their daily interactions, and given the right circumstances, are able to do it.
- These social practices are routinized and recursive, i.e., they exist across space and time. People draw on structural properties (which Giddens calls rules and procedures) which are the institutionalized properties of society, in order to construct the visible social practices that make up society.

Structure is both the medium and outcome of the process of "structuration."

Structure is revealed through the activity of human agents. It does not have an independent existence, although human agents draw on their understanding of structural properties when engaging in social activity. This production and reproduction of structure allows social practices to persist across time and space (Brooks, 1997, p. 137).

According to Giddens and the work of Erving Goffman, it is a fundamental instinct for humans to closely observe and monitor the behavior of others in a social setting. Goffman argues that people are intuitively aware of when and how they are observed in a social context (Goffman, 1959). Goffman's work involves a detailed study

of how people labor to craft their public persona in order to create and maintain social status. Goffman labeled this behavior as impression management.

Goffman also describes methods people employ to break through impression management. He discussed the case of the “unobserved observer” – how people use opportunities to see an unedited performance as a chance to expose the real person. The following section describes an episode of indirect observation (a crofter is a subsistence farmer):

In Shetland Isle one crofter’s wife, in serving native dishes to a visitor from the mainland of Britain, would listen with a polite smile to his claims of liking what he was eating; at the same time she would take note of the rapidity with which the visitor lifted his fork or his spoon to his mouth, the eagerness with which he passed food into his mouth, and the gusto expressed in chewing his food, using these signs as a check on the stated feelings of the eater. The same woman, in order to discover what one acquaintance (A) ‘actually’ thought of another acquaintance (B), would wait until B was in the presence of A but engaged in conversation with still another person C. She would then covertly examine the facial expressions of A as he regarded B in conversation with C. Not being in conversation with B, and not being directly observed by him, A would sometimes relax usual constraints and tactful deceptions, and freely express what he was ‘actually’ feeling about B. This Shetlander, in short, would observe the unobserved observer. (p.7)

Bloggers have reported situations where one member of a split up couple can track their former partner’s activity by monitoring their availability on instant messenger. This is possible because many users of instant messenger are logged on all day, so when a screen name “goes idle,” it means the person is away from their computer.

Here is a posting from oblivio.com:

E reported over dinner (excellent new Italian place on Vanderbilt) that it’s over between her and J....E said that her instant messaging program lets her know when J’s computer has been idle more than a certain number of minutes, this being information she uses in her speculations about whether J is talking to, emailing, or having sex with the other woman.

I suggested the obvious: Delete him from the program.

She responded with the obvious: This is her only remaining connection to him, (Barrish, 2003).

The viewing of profiles on social network sites is a way to gain insight into the personality of another person. However, this act of online observation is neither transient nor embedded in a context. So therefore the simple act of looking at a new acquaintance's profile has the potential to signal unintended messages.

People often have strong reactions when they realize their digital trail has the potential to be misinterpreted. A Friendster member had been using the site to learn more about her new classmates. After Friendster implemented a profile tracker, she was aghast to realize that whenever she viewed someone else's profile, that someone could see her looking: "I felt totally exposed without my permission ... I was horrified at the thought that this guy or other people ... would think I was stalking them or was insecure or needy for friendship," (Mintz, 2005).

The proliferation of social technologies has greatly increased our ability to become the unobserved observer. Are there ethical consequences to this increased power? How should these consequences be considered in system design?

Goffman argues that the key driver for an individual crafting impression management is the nature of the audience viewing that performance. While it is possible for one's actions to be observed by an unknown audience in a face to face setting, that audience is bounded by the limits of time and space. With respect to Internet based communications, in the case of blogs, instant messenger, and social network sites, the boundaries of the potential audience cannot be determined. This undermines subtle social calculations that take place as information is shared. This may help to explain some of the

risky revelations that take place on social network sites. Members effectively pretend their audience is only their friends, and choose not to restrict their presentations to comply with a hypothetical audience.

Goffman's discussion of the important role of observation in social interaction explains why there are such complexities when it comes to unraveling the impact of technology that reports on member activity. Social interaction, according to Goffman, is a complex dance. One partner's steps and moves are consciously designed to impact social impressions while the other partner is engaged in deflecting the intended effect and uncovering the deeper motivation.

3.2 The Adaptive Structuration Theory

Structuration theory is an important social theory within information systems research. The structuration perspective has largely been applied to Group Support Systems (Orlikowski 1992; DeSanctis and Poole 1994; Dennis, Wixom et al. 2001; Hettinga 2002; Dennis and Garfield 2003). However, it has also been applied to CT scan technology (Barley, 1986), collaboration tools within a virtual team (Majchrzak, Rice, Malhotra, & King, 2000), mobile personal devices (Wiredu, 2007), Computer Aided Design (Brooks, 1997), and software process improvement (Allison & Merali, 2007). The structuration perspective is also prominent in the computer supported cooperative work research community, where there is a focus on appropriation (Bansler & Havn, 2006; Dourish, 2003).

The work of the sociologist Anthony Giddens has been used extensively in the analysis of information systems (Giddens, 1979, 1984). Adaptive Structuration Theory is

an extension of Anthony Giddens' structuration theory (DeSanctis & Poole, 1994, p. 122). Adaptive Structuration Theory focuses on the evolution of groups and organizations in the wake of what DeSanctis and Poole describe as “*advanced information technologies*: electronic messaging systems, executive information systems, collaborative systems, group decision support systems, and other technologies,” (DeSanctis & Poole, 1994, p. 125). Although DeSanctis and Poole apply Adaptive Structuration Theory to small group interaction in the context of group decision support systems, they state that the concepts and relationships that make up Adaptive Structuration Theory can be applied to other advanced technologies in other contexts (DeSanctis & Poole, 1991).

DeSanctis and Poole present Adaptive Structuration Theory as a theoretical approach that can anticipate the changes that advanced information technologies bring to organizations and the workplace. They believe that the effects of advanced technologies are less a result of the nature of the technologies than of how they are used (Poole & DeSanctis, 2004).

DeSanctis and Poole apply Adaptive Structuration Theory to construct a sociotechnical explanation of technology impacts that models technology use as an evolving social practice (DeSanctis & Poole, 1994). Adaptive Structuration Theory builds on structuration theory, and explains use in terms of technology structures and their interaction with social structures that emerge as people use the technology. Adaptive Structuration Theory, in the context of GDSS, describes a process whereby a GDSS offers a set of structures to a group, but it is the process the group goes through as it uses those structures for its own ends that matters. As a group adapts a technology, it

in effect *re-structures* that technology, as the technology becomes enmeshed in the group's decision processes and outcomes.

This idea that technology itself is changed through use is called *appropriation*, as understood and described by Karl Marx (Ollman, 1971). "Appropriation is the process by which users invoke available GDSS structures in their actions and thereby provide meaning to them," (DeSanctis & Poole, 1991, p.547). In their description of Adaptive Structuration Theory, DeSanctis and Poole provide a detailed taxonomy of appropriation moves.

The term appropriation has been used in information systems research to describe the process by which people adopt and adapt information technologies to the tasks they carry out. Adaptive Structuration Theory extends both appropriation (DeSanctis & Poole, 1994) and structuration by analyzing appropriation through the lens of structuration (Poole & DeSanctis, 1989).

DeSanctis and Poole build on the concept of appropriation borrowed from 19th century philosophers Hegel and Marx (Poole & DeSanctis, 1989). Hegel and Marx were concerned with human interaction with technology, specifically how humans learned to control the natural world, and how this in turn shaped human society (Ollman, 1971). According to Marx, to appropriate an object was to use it constructively, to make it part of one's life, for better or worse (Poole & DeSanctis, 1989). The progress of society can therefore be understood as the development of more advanced and successful forms of appropriation.

According to this perspective, every impact of a technology depends on an appropriation of that technology (Ollman, 1971). In appropriating an object, the user

realizes that object. How an object is used then becomes the basis for any human understanding of that object. “This implies that the realization of any object itself can change as people change their mode of using it,” (Poole & DeSanctis, 1989, p. 2). The understanding of appropriation as a constructive process that shapes both the subject (the user) and the object (the technology) is a basic element of Adaptive Structuration Theory.

DeSanctis and Poole also build on the work of Orlikowski (Orlikowski and Robey 1991; Orlikowski 1992; Orlikowski 1993; Orlikowski 2000), who applies structuration to a definition of technology. Orlikowski describes technology as both a structure that is created by human agents who are system designers, and a structure that is appropriated by human agents who are system users. There is an interplay or “duality” of structure whereby the design structures of advanced information technologies feed into the structures that emerge as people begin to use these technologies.

The study of information technology and organizational change has been undertaken from two perspectives: from the perspective of technical factors, and from the perspective of social factors. Research in the technical perspective includes decision theory (Keen, 1981; Keen & Morton, 1978) and task technology fit (Goodhue, 1995). Both these theories treat technology as an independent variable that can be manipulated to achieve the desired productivity outcomes.

A weakness of the technical perspective, called the *decision-making school* by DeSanctis and Poole, is that it views the impact of technology as a deterministic force, whereas empirical research has produced mixed results. Studies revealed variations in attitudes or patterns of use of the same technology design across groups (Kerr and Hiltz

1982; Barley 1986; Hiltz and Johnson 1990; Orlikowski 1992), which implies unknown confounds influencing the adoption of a technology system.

A less deterministic perspective sees the use of technology as an opportunity for change, rather than a causal agent of change (Orlikowski, 1992). This perspective gives greater weight to the influence of social factors, so that the creation, design, and use of advanced technologies are intimately tied to the structure and path of the social order. In this perspective, labeled as the *institutional school* by DeSanctis and Poole, technology does not determine behavior; rather, people propagate social structures of technology using resources, interpretive schemes, and norms rooted in the larger institutional context (Orlikowski, 1992). Given this social process perspective, it follows that studies of technologies of organizational change must focus on interaction and capture historical processes as these social practices evolve. Technology is described as interpretively flexible, and so analysis requires peering beneath the surface layer of technology's role in organizational change to uncover the deeper meanings brought to technology by social systems.

DeSanctis and Poole in Adaptive Structuration Theory seek to reconcile the decision and institutional perspectives. This combined perspective is called the *social technology* perspective, and it advocates a "soft determinism" in its explanations of technology adaptations. Sociotechnical systems theory argues that the nature of advanced information technologies impacts depends upon how well both social and technology structures are optimized. Technology adaptation is understood to be a process of organizational change.

Adaptive Structuration Theory extends prior structuration models of technology-triggered change by acknowledging the influence of both technology and social processes. Adaptive Structuration Theory attempts to explain the structure of advanced technology systems and the evolution of social interaction as these technologies are used. The goal of Adaptive Structuration Theory is to confront “structuring’s central paradox: identical technologies can occasion similar dynamics and yet lead to different structural outcomes,” (Barley, 1986, p. 105).

DeSanctis and Poole focus on advanced information systems as social structures, specifically focusing on the interaction of groups and organizations with information technology. Adaptive Structuration Theory criticizes the techno-centric and deterministic view of technology use and instead emphasizes the social aspects by stressing the reciprocal pressure of social and technical context.

Groups and organizations using information technology for their work dynamically create and evolve perceptions about the role and utility of the technology, and how to best adapt it to their activities. These perceptions are examples of reflexive behavior, as described by Giddens in his description of the continuation and evolution of structures. Because appropriation is a complex and dynamic process, these perceptions can vary widely from one group to another. These perceptions also influence the way technology is used and mediate its impact on group outcomes. Hence, social forces drive the use of technology. Adaptive Structuration Theory focuses on the actual use of technology, rather than on intended use by its developers.

Adaptive Structuration Theory provides a model that describes the interplay between advanced information technologies, social structures, and human interaction.

Building on structuration theory, Adaptive Structuration Theory identifies social structures as the rules and resources provided by technologies and institutions, as the basis for human activity. These social structures both enable and constrain human activity.

DeSanctis and Poole specify that Adaptive Structuration Theory applies to advanced information technologies that mediate coordination among people and interaction. Adaptive Structuration Theory argues that advanced information technologies provide two types of social structures. The first is structural features, which are the resources and functionality provided by the system. For example, in group decision support systems, features can include anonymous recording of ideas, periodic pooling of comments, and voting mechanisms. These functions dictate how information is gathered, manipulated, and otherwise managed by users. Hence, these features bring meaning (what Giddens calls “signification”) and control (“domination,” or power) to group interaction (Dennis et al., 2001).

In addition, the social structures of an advanced information technology also can be described in terms of their *spirit*, which is the general intent with regard to fundamental values and goals, or reasons for a particular choice of system design. For example, the spirit of group decision support systems is to promote more democratic decision processes in order to reach better decisions. If a group decision support system is used to reinforce an autocratic power structure, this can be viewed as contrary to the spirit of the technology (DeSanctis & Poole, 1994, p. 128).

Adaptive Structuration Theory, as described by DeSanctis and Poole, argues that advanced information technologies promote specific social structures based on their

features and spirit. Other sources of social structures come from the task as well as the organizational environment (DeSanctis & Poole, 1994, p. 130).

The act of bringing the rules and resources from an advanced information technology or other structural source into action is termed structuration. Structuration is the process by which social structures are produced and reproduced in social life. When these social structures are brought into action, they may take on new forms. That is, the structures as enacted do not necessarily match the structures that are part of the advanced information technology. Adaptive Structuration Theory defines appropriations as “the immediate, visible actions that evidence deeper structuration processes,” *ibid*.

By examining appropriations, DeSanctis and Poole hope to uncover the exact nature of the relationship between a given resource within a group decision support system, and how it is used, or brought into action. Appropriations cannot be mandated by technology designs. Instead, human agents independently choose how technology structures are used, resulting in varied adoption practices. Human agents have the choice to appropriate technology *faithfully* or *unfaithfully*, meaning consistent with the features and spirit of the technology (DeSanctis & Poole, 1994).

Appropriation is a central component of Adaptive Structuration Theory, presented by DeSanctis and Poole. They describe four aspects of appropriation. The first aspect describes how users may invoke any number of appropriation moves. These can be one of the following:

- The appropriation move directly uses the structure
- The move relates the structure to other structures (related to task or environment)
- The user constrains or interprets the structures as they are used

- The user makes judgments about the structures regarding their usefulness.

The second aspect relates to whether users appropriate the technology faithfully or unfaithfully. The third aspect relates to whether users appropriate the technology for other instrumental uses. And the fourth aspect involves users' attitudes regarding appropriation. These include whether the user is comfortable with the technology, whether the user perceives the technology to be of value, and whether the user is willing to put effort into their use of the system.

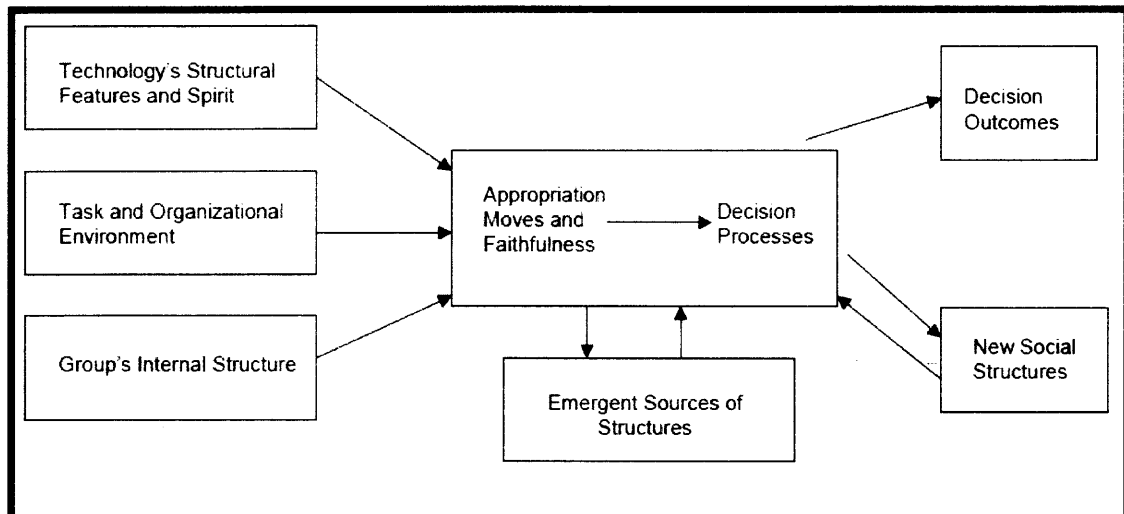


Figure 3.1 Model of Adaptive Structuration Theory, from Majchrzak, 2000.

A model of Adaptive Structuration Theory is presented in Figure 3.1. The process by which technologies are adapted consist of structures, appropriations, and decision outcomes. In the model, three sources of structure form pre-existing conditions that make up the implementation context for technology. Technology provides structures in the form of restrictiveness, sophistication, and comprehensiveness of its features, in addition to its “spirit,” the overall intent of the technology with regard to its values and goals. Task and organizational environment refer to the nature of the task, i.e., its

complexity and interdependence, and the organizational setting, made up of hierarchy, corporate information, and cultural beliefs. The group's structure is made up of the interaction among its members, as well as its decision making processes.

Appropriations are the immediate, visible actions that signal deeper structuration processes. The assessment of appropriation processes is a key component of Adaptive Structuration Theory. The Adaptive Structuration Theory framework documents how technology structures are invoked, or are constrained in use by a specific context. Appropriations can be analyzed for their faithfulness, their instrumental uses, or by users' attitudes.

An important contribution by Adaptive Structuration Theory is the understanding that the faithfulness of an appropriation is an important factor in the overall success of an information system. Chin, Gopal, and Salisbury have developed a scale that measures faithfulness of appropriation (Chin et al., 1997). The questions in the scale collect the perceptions of the user with respect to how they use the technology compared to how they perceive the overall intent (i.e., the spirit) of the technology. The authors first worked to produce an initial set of items. This was followed by instrument testing and refinement. Confirmatory analysis tests were conducted as part of an experiment that had 330 undergrad subjects. The final five item scale has Cronbach's alpha = .94, and also passed several tests for goodness of fit. This scale was subjected to rigorous tests for convergent, discriminant, and nomological validity.

Salisbury, Chin, Gopal, and Newsted worked together to create a scale that captures the consensus of a group with respect to appropriation (2002). DeSanctis and Poole have argued that the success of a group depends not only on the appropriation

process, but also on whether the group has reached an agreement or consensus on that appropriation. For organizational and group settings, consensus on use is thought to be related to performance (Dennis et al., 2001). The consensus scale was tested in a survey of 236 undergraduate students in experiments using GSS technology. The study conducted a comparison of three measurement models of Adaptive Structuration Theory constructs, followed by a causal model analysis of the relationship between consensus of appropriation, faithfulness of appropriation, and satisfaction. The authors found that consensus on appropriation has a significant direct effect on decision scheme satisfaction ($\beta = 0.21$), and faithfulness of appropriation has a significant effect as well ($\beta = 0.31$). Perceived usefulness also has a significant impact ($\beta = 0.34$) on decision scheme satisfaction, but ease of use did not.

3.3 The Fit Appropriation Model

The Fit Appropriation Model as described by Dennis et al. (2001) extends task technology fit theory by combining it with “appropriation” theories, such as Adaptive Structuration Theory. The motivation for combining these approaches is to explain inconsistent results with respect to the impact of group support systems (GSS).

The Fit Appropriation Model begins with the components of task technology fit. Task technology fit theory argues that advanced information systems are more likely to have a positive impact on performance if there is a close alignment between the requirements of the task and the features of the technology (Goodhue, 1995, 1998; Goodhue, Klein, & March, 2000; Goodhue & Thompson, 1995). According to Goodhue, task technology fit will be most appropriately measured by determining the user’s belief

as to how satisfactorily the system meets the requirements of the task, regardless of how they feel about the system (Goodhue, 1998). Furthermore, the links from beliefs of task technology fit will be stronger to performance than “user feelings” (Goodhue, 1995).

The justification for applying an organizational theory such as task technology fit to social networking sites is that task technology fit has already been applied to group support systems, which support social functions. In addition, Media choice theory, especially Media Synchronicity Theory, has been described by Dennis et al. (2001) to be understood as a special case of task technology fit.

Technology gives value by being instrumental in the completion of a task, and this value will be reflected in users evaluation of systems (Goodhue, 1995). Task technology fit builds on utilization theories such as the theory of planned behavior (Ajzen, 1991), the cognitive cost/benefit framework (Payne, Bettman, & Johnson, 1993). These are examples of theories based on technical rationality, as defined by Thompson (1967): “Instrumental action is rooted on the one hand in desired outcomes and on the other hand in beliefs about cause/effect relationships. To the extent that the activities thus dictated by man’s belief are judged to produce the desired outcomes, we can speak of technology, or technical rationality.”

Technologies are viewed as tools used by individuals in carrying out tasks. The task technology fit perspective suggests that a better fit between technology functionalities, task requirements, and individual abilities will lead to “better performance,” i.e., faster or more effective task accomplishment.

According to the cognitive cost benefit framework, individuals weigh benefits, such as impact on correctness, speed, and justification, against costs, such as mental

effort on information acquisition and computation. Related to this theory is rational choice theory, which assumes a rational decision maker with well defined preferences, who can choose among options which have a clearly defined but subjective utility. It also assumes the consumer has the computational ability to calculate the relative values of each option, and select the optimal choice (Bettman, Luce, & Payne, 1988).

This is contrasted with the notion of bounded rationality, which is the notion that decision makers have limitations on their capacity for processing information. These limitations include limited working memory and limited computational ability (Simon, 1955). The notion of bounded rationality, along with limited information processing ability, is consistent with the belief that preferences for options are constructed, not merely revealed. People often do not have well defined preferences. Instead they may construct them on the spot as needed. Thus consumer preference formation may be more like architecture, building some defensible set of values, rather than archeology, uncovering values that are already there (Bettman et al., 1988).

Preferences will not be determined by an invariant process, but from a variety of methods adapted as needed. This implies that choice is therefore quite context dependent. Preferences are also constructed when consumers have multiple and/or conflicting goals. Therefore some accommodation needs to be worked out (Bettman et al., 1988).

An important implication of the constructive nature of preferences is that choices are often highly contingent on a variety of factors characterizing decision problems, individuals, and contexts.

Choice among options can depend on one or a combination of the following goals:

- the goal of minimizing the cognitive effort required to make a decision, i.e., an effort related goal, as described by Simon (1955)
- the goal of minimizing the error with regard to making a poor choice (maximizing the accuracy of the decision, i.e., the rational theory goal)
- minimizing the emotional distress during decision making (the affective goal)
- maximizing the ease of justifying the decision, since decisions are often public and can and will be evaluated (the social goal)

The choice that is made depends on the complexity of the task. Options that are superior on the most prominent attribute are preferred because the use of simple decision processes increases with task complexity.

The model then adds the appropriation construct, which is the process by which people apply and adapt technology to their tasks. DeSanctis and Poole define a “faithful appropriation” as one where the group uses the technology as intended by its designer. An “unfaithful appropriation” is one where the technology is not used in ways intended by the designer (Dennis et al., 2001; Dourish, 2003).

How well the tool fits the task does not matter if the tool is not used properly. Therefore, it is important to look at what support technology provides to guide users. Dennis et al. label this as appropriation support, or the degree of training, facilitation, or software restrictiveness within a system that encourage faithful appropriation, i.e., using the system as intended by its designers. Dourish has described appropriation support as an important consideration in the design of collaborative systems (2003).

For GSS, Dennis et al. identify three ways of providing appropriation support. The first is facilitation, through a group leader or an external facilitator. The second is software restrictiveness, referring to the extent to which a system constrains individual

behavior. For example, for GSS systems, items not related to the group's agenda may be blocked for discussion by the system. The third factor is appropriation training. This involves training in the use of the technology, to reinforce the benefits of using the technology in an appropriate way.

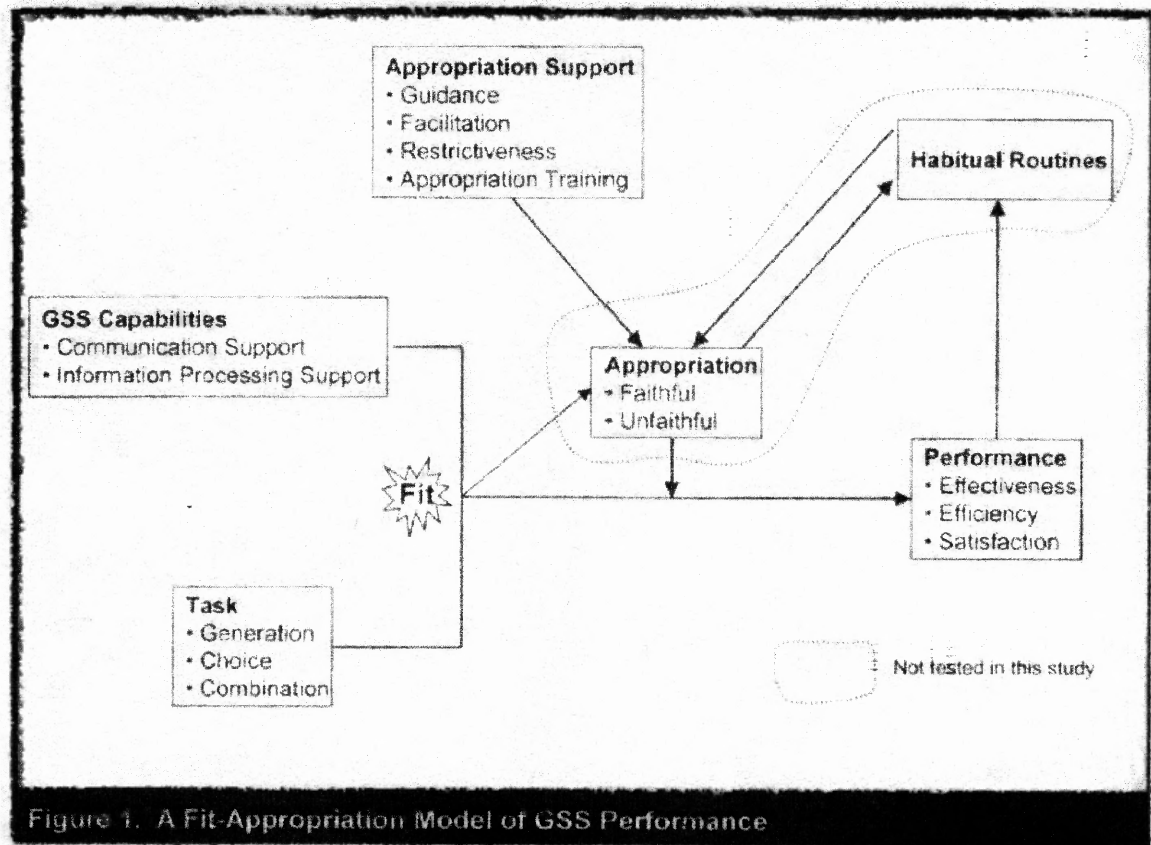


Figure 3.2 Fit Appropriation Model, from Dennis et al., 2001.

Dennis et al. then applied the Fit Appropriation Model to a meta-analysis of GSS studies. This model predicts that when there is task technology fit, the existence of appropriation support will lead to greater performance (such as improved decision quality, more ideas/alternatives, and improved participant satisfaction with the outcome).

Dennis et al.'s meta-analysis found that task technology fit (the match between the requirements of a task and the technology used to carry out that task) explained some

but not all GSS research results. Their results suggest that both task technology fit and appropriation support are factors that can predict outcome.

3.4 Meta-Analysis Results

The Fit Appropriation Model argues that if the use of GSS combines both fit and appropriation support, then performance will be greater than settings without fit or appropriation support. This hypothesis was tested in a meta-analysis of research studies on GSS. Performance was captured through the following measures: decision quality, number of ideas generated, time spent completing task, participant satisfaction with the outcome, and participant satisfaction with the meeting process.

The results of the meta-analysis for GSS studies with task technology fit and appropriation support are the following:

- improved decision quality – not supported
- more ideas – supported
- less time – supported
- improved participant satisfaction with the outcome – not supported
- improved participant satisfaction with the meeting process - supported

The meta analysis provided limited support for the Fit Appropriation Model. For studies with evidence of fit and appropriation support, performance was better in three respects: more ideas were generated, less time was required, and participants had higher satisfaction with the meeting process.

In a follow up to the meta-analysis, Dennis and Garfield conducted a field experiment of six medical project teams (2003). The authors acted as facilitators for the

GSS teams. A goal of this study was to examine more carefully the impact of appropriation support. Half of the teams used a GSS and half used their traditional team processes; data was collected through observations of meetings, interviews, transcripts and a survey.

Some teams found the GSS meeting processes unsatisfactory, and abandoned them. However, they subsequently found traditional methods uncomfortable, and then moved back to include more electronic meeting processes. Within the GSS teams, project leaders faced challenges or abdicated, regular members participated to a greater extent, the project goal emerged from group discussion, and the teams' notes were open and widely distributed. In general, GSS processes were more open and democratic. This is consistent with the spirit of GSS software.

An experiment testing the Fit Appropriation Model is reported in (Fuller & Dennis, 2004). This study found that groups with “low fit” technology, over time, performed as well as those with strong or high fit. However, in this experiment fit is manipulated by giving some technology to one group, and some to another. The perception of fit was not that different between the low fit and high fit groups. The perception of fit was only different in one dimension at T1 (time interval 1). No other differences were found at T2 and T3. This result calls into question the effectiveness of the task fit manipulation.

However, there is an assumption within the term “faithful appropriation” that the intent of the designer is correct. In addition, the Fit Appropriation Model does not represent how use of the system (appropriation) can lead to a change in the technology. This is not consistent with current software development practices. For example, agile

methods emphasize continuous delivery of small increments of functionality based on intense feedback from the users (Boehm, 2002). Models based on appropriation are lacking a feedback cycle because of the presumed validity of the initial design. This limitation will be addressed by adding a feedback cycle, adapted from socio-technical systems theory. The next section will describe Socio-technical Systems Theory and how feedback leads to changes in the system.

3.5 Feedback Within Socio-technical Systems

An understanding of the structure of socio-technical systems theory, particularly feedback loops, helps explain how patterns of usage influence the development of a system. According to Thomas P. Hughes, large technological systems are complex, messy problem solving systems with ill-defined boundaries (1989).

Technological systems are both socially constructed, and also help shape social structures. These systems consist of components, which are social structures, and artifacts, which are technical elements that contribute directly or through other components to a common system goal.

The relationship between artifact and social structure can also be seen in the impact of new communications technologies, such as e-mail, cell phones, and the internet, on the organizational structure of companies. For example, the type of communication technology has been found to affect the structure and success of virtual teams (Cramton 2001; Hinds and Bailey 2003; Coppola, Hiltz et al. 2004).

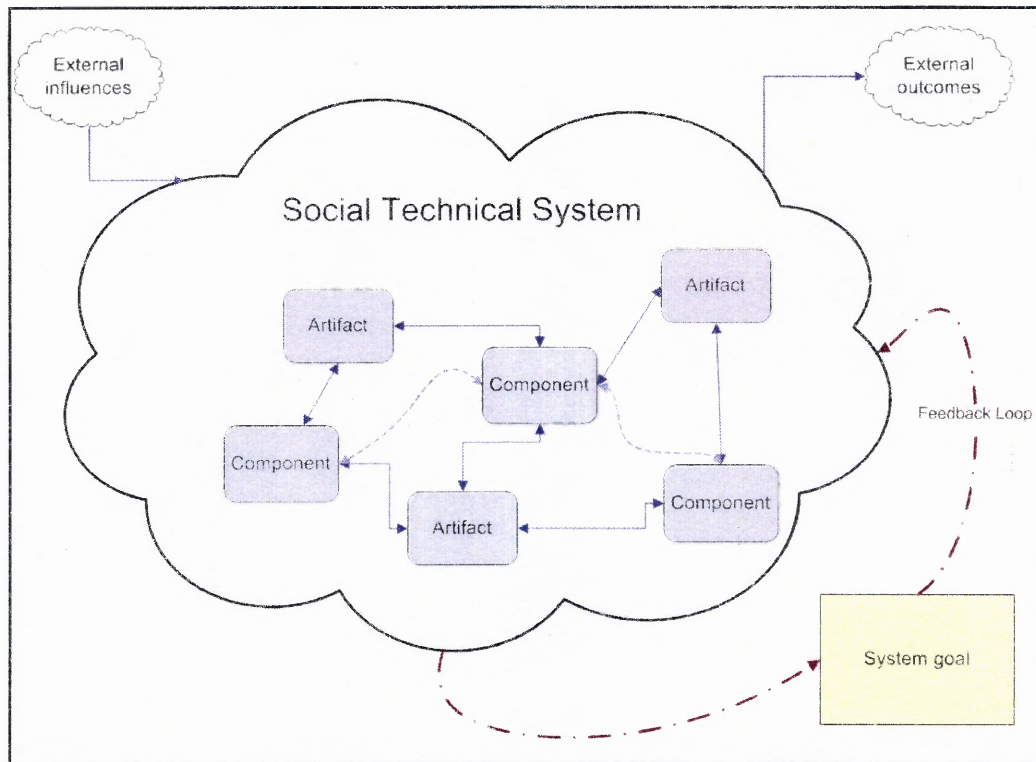


Figure 3.3 The structure of a socio-technical system, based on Hughes, 1989.

Figure 3.3 is a graphical representation of Hughes's description of social technical systems. The system's boundary is depicted with an irregular shape, representing the blurred borders of social technical systems. Within the system are components and artifacts that interact.

An important part of this theory relevant to the use of social networking sites is the feedback loop, represented in Figure 3.3 as a dashed line. Hughes maintains that people within a technological system have a critical role, which is to complete the feedback loop by perceiving the gap between system performance and system goals. Hughes argues that it is only through this feedback loop that errors are caught and corrected, leading to improvement in system performance.

This feedback mechanism continues throughout the life of the system. System builders design artifacts and components in order to fulfill the system goal. People using the system compare the actual performance to its goal, and this feedback leads to adjustments in the artifacts and components of this system. This cycle continues, as the system expands in size and complexity.

3.6 Socio-technical Systems Theory and Information Systems

Research into the management of information systems benefited from an appreciation of both the social and technical components of new computing systems that were implemented into organizations. The socio-technical perspective was applied to information systems by several IS researchers.

An influential paper on information systems that applies the socio-technical systems perspective is the classic article “Information Systems and Organizational Change,” by Peter Keen, (1981). Keen uses Leavitt’s diagram of organizations, which describes systems made up of the following components: task, technology, structure and people. As each of these components changes, the other components are said to adjust in order to maintain system equilibrium. This makes it unlikely for dramatic change to occur within an organization. Keen also uses socio-technical systems theory to discount “economic rationality,” suggesting that change can only occur by engaging actors in a political process.

A paper by Lyytinen, Mathiassen, and Ropponen provide an analysis of risk management through a socio-technical perspective (2000). This paper argues that rather than following a rational decision process that considers both the upside and the

downside to a risk, software managers are concerned with eliminating the possibility of a poor performance. Success is not measured as the best possible outcome, but as any outcome that avoids bad outcomes (p. 235). Risk management suffers from both cognitive limits as well as management styles that progressively prune off options rather than considering the full distribution of possibilities. Managers, in effect, operate to maintain system equilibrium.

The role of the feedback cycle is an important component in socio-technical systems theory. There is evidence of frequent feedback between members of social networking sites and their designers, resulting in changes to these sites. In some cases technology updates can be rejected, requiring revised functionality. The Facebook “news feed” incident is an illustration of functional changes that needed to be revised in response to feedback from members.

In 2006 Facebook introduced a “news feed” feature. The Facebook news feed is a log of members’ daily activity on the site. The news feed is prominently displayed on each member’s profile, and distributed to everyone within a member’s social network. So if Alice posts a comment on one of Bob’s pictures, all of her friends are informed that she did so. This act was in a sense public because anyone could happen upon the comment if they were looking at Bob’s pictures. However, the news feed broadcasts everything you do to all of your “friends,” greatly increasing the visibility of actions.

While Facebook’s designers intended to facilitate social connections, members perceived it as an invasion of privacy and loss of control of their personal information. Within days, over 700,000 members expressed their concern by joining a group “Students Against Facebook News Feed.” In response to vocal protests and media attention, the

founder of Facebook, Mark Zuckerman, explained the purpose behind the news feed: “This is information people used to dig for on a daily basis, nicely reorganized and summarized so people can learn about the people they care about.” Members were unswayed. Angry Facebook members had made their unhappiness felt, and the site was changed to add privacy controls to the distribution of news feed information (Schneier, 2006).

The news feed example illustrates how quickly members of social networking sites can express their unhappiness, triggering functional changes. The news feed is an example of strong negative feedback that resulted in a change to the site.

3.7 Summary

Social theories are an important part of information systems research, and are important in understanding the nature of social networking sites. Socio-technical systems theory describes how artifacts (technology) and components (social structures) interact and influence each other. This can be observed in social networking sites. The way the members use the sites has influenced the structure of the technology. And the effectiveness of these sites’ communication modes has allowed members to expand their social network and change the way they maintain relationships.

Structuration theory has been very influential within information systems research. It provides a non-deterministic approach that explains the interaction between technology and social structures. This has led to two information systems specific theory, adaptive structuration theory, and the Fit Appropriation Model. These two

theories focus on the appropriation process, which involves both the nature of the spirit of the technology, combined with the experiences, values, and social context of users.

The next chapter describes current privacy management functions in two social networking sites, Facebook and MySpace. In addition, the limitations of privacy management are discussed, and behavior surrounding online privacy is explained by applying Adaptive Structuration Theory.

CHAPTER 4

THE SPIRIT OF PRIVACY MANAGEMENT WITHIN SOCIAL NETWORKING SITES

As introduced by DeSanctis and Poole (DeSanctis & Poole, 1994), spirit is the overall design philosophy that guides the functional composition and integration of an advanced information system. The spirit both guides the developer of a system as they construct and connect the components, as well as the users of the system as they adapt and appropriate the functionality made available to them.

In order to develop a deeper understanding of the use of privacy management with social software, it is useful to analyze the spirit that guides the implementation of privacy management within social networking sites. The following sections analyze and compare privacy management functions within Facebook and MySpace, with the objective of identifying the nature of the spirit of privacy management within these two social networking sites.

4.1 The “Spirit” of Facebook and MySpace

How do these sites define themselves? What can be said about the spirit of Facebook and MySpace? On its member login page, Facebook describes itself as “a **social utility** that **connects you** with the people around you.” Specifically, Facebook is intended to be used to maintain social contact with friends and family, re-connect with old friends and classmates, share photos and videos, and engage in online discussions of interests and hobbies (Facebook, 2008). In addition, Facebook emphasizes that control over privacy is an explicit part of the experience on the site, listing privacy control as a function right on

its front banner page. The official description of the site states that “at Facebook, we believe that people should have control over how they share their information and who can see it. People can only see the profiles of confirmed friends and the people in their networks. You can use our privacy settings at any time to control who can see what on Facebook.”

Facebook has an extensive privacy policy and terms of use agreement. The goal of the privacy policy is help members make informed decisions about the privacy levels of the information they decide to share. As stated in Facebook, its “Privacy Policy is designed to help you understand how we collect and use the personal information you decide to share, and help you make informed decisions when using Facebook,” (Facebook, 2006).

Under the terms of use, your account can be closed on Facebook if you are found to have created a false persona, or are impersonating someone else. The idea is to encourage the creation of authentic profiles. Facebook has in place functionality that restricts or terminates accounts that engage in frequent unsolicited messages (i.e., spam). In summary, the spirit of Facebook is reflected in its goal of creating a safe online social space where people can feel comfortable sharing and interacting with other members, while not being bothered by disturbing online behavior. The spirit of Facebook’s privacy management is that its privacy settings are designed with the intent that members can make reasonable and informed decisions about the way they manage their privacy.

On the banner front page of MySpace, the site is described as “an online community that lets you meet your friends’ friends,” (MySpace, 2006). MySpace describes itself as a community where your can share photos, journals, and interests

within a growing network. It is a place for “Single people who want to meet other Singles” and “Matchmakers who want to connect their friends with other friends.”

The spirit of MySpace focuses on making connections with new friends and new potential romantic partners. Privacy is not specifically mentioned as a goal of the site, in contrast to Facebook. The focus of MySpace is on the development of new connections. As part of this focus, it has a more liberal policy with respect to the use of the site for publicity and notifications. The terms of use say that “The MySpace Services are for the personal use of Members and may be used for promotional purposes as well.” This has made MySpace very popular with aspiring musicians, comedians, film makers, and other creative artists.

The privacy settings of MySpace are focused on setting up controls for communication settings, almost like a spam filtering mechanism. The spirit of the privacy management is primarily concerned with setting up controls over who can send you messages. You even have the option to block messages from people you do not know, but allow messages from bands. This illustrates how the spirit of fostering creative connections is implemented in the privacy settings.

4.2 Privacy Support Within Social Networking Sites

On a functional level, privacy management tools on social networking sites control specifically who can view a person’s online profile. The profile may have several components: contact information, descriptive information, photographs, a blog, and a public comment space. The privacy management settings built into social networking sites allow individual members to specify who may view all or segments of their profile.

Privacy management is implemented in a manner similar to role authentication methods used in other information systems. Other members are identified in their role as friend, or not. A friend is granted full access, and “not friend” is restricted. Privacy management settings determine the degree to which a person’s profile and its components are visible to other members of the social networking site.

4.3 Privacy Management on Facebook

Facebook has consistently used its privacy management features as part of its marketing appeal. When Facebook was created, it required new members to provide valid email addresses from an established institution of higher education, such as Harvard or New York University. Although the site is no longer restricted to just college students, it does still require a valid email address from an institution in order to join that school’s network.

Facebook enforces privacy by dividing groups into networks, related to schools, institutions, or regions. There is no global network access available at Facebook. In other words, no privacy setting is supported that would allow you to make your profile visible to everyone at Facebook. This is an example of software restrictiveness being used to enforce privacy.



Figure 4.1 GUI for privacy management on Facebook.

As a member of Facebook, you have the opportunity to join networks associated with a school as long as you have an email address from that institution. The same is true of joining a network associated with an organization. In other words, if you want to join the IBM network, you need to provide an IBM email address. This is a basic level of authentication that helps to validate who resides in certain networks.

You also have the option to join one region, which is organized around a city such as Newark or geographic location such as North Jersey. There is no authentication used

to control who may enter a regional network. However, you are restricted to belonging to only one regional network at a time.

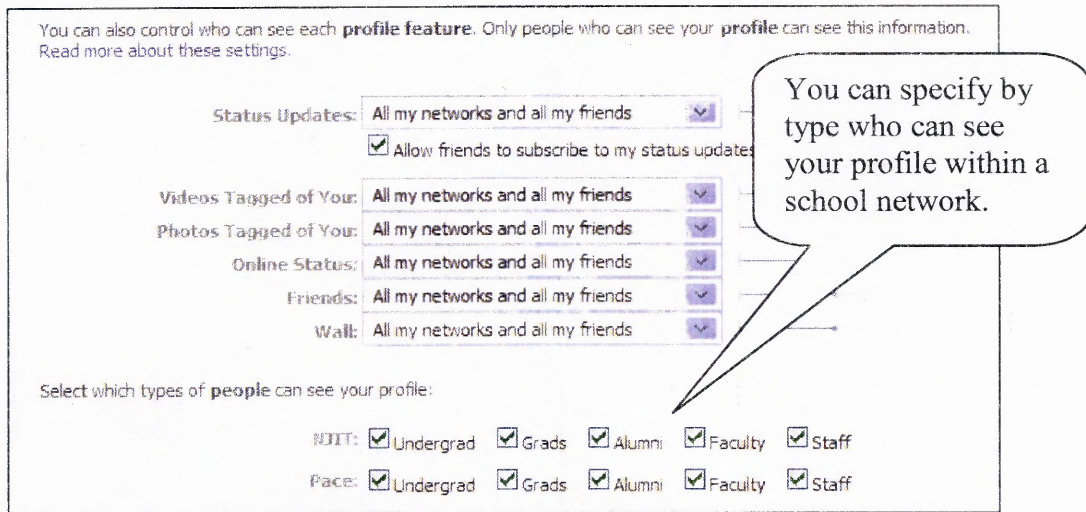



Figure 4.2 Facebook offers granular privacy control.

Privacy options are organized in a set of hierarchical menus that can be directly accessed from any page on the site. Navigation to the privacy management tools is always simple because a link is found in a consistent place on every page. Privacy management is divided into sections (see Figure 4.1). The consequences of changing privacy settings are clarified through the use of sliders that represent the level of privacy protection selected. If the slider is all the way to the right, then privacy settings are as loose as possible; if the slider is all the way to the left, then the privacy settings are as restrictive as possible.


Facebook allows granular control over who can view profiles from a specific network. For example, you may belong to a school's network, but you can restrict your settings so that your profile is only visible to other students. You can also make your profile visible, but only allow friends to see the videos you post on the site (see Figure 4.2).

Contact Information


You can control who can see your contact information — your **friends** can always see your contact information, and you can allow **all your networks** or **some of your networks** to see your contact information. Only people who can see your **profile** can see your contact information.

IM Screen Name: Some of my networks and all my friends 


☒ NJIT
☒ Pace
☐ New York, NY

Mobile Phone: Some of my networks and all my friends 


☒ NJIT
☒ Pace
☐ New York, NY

Land Phone: Some of my networks and all my friends 

☒ NJIT
☒ Pace
☐ New York, NY

Mailbox: Some of my networks and all my friends 

☒ NJIT
☒ Pace
☐ New York, NY

Current Address: Some of my networks and all my friends 


☒ NJIT
☒ Pace
☐ New York, NY

Figure 4.3 Facebook supports control over access to contact information.

Facebook has invested heavily in features that make privacy management more flexible and accessible. It has continually worked on privacy and made changes and improvements over time to increase the functionality of privacy management settings. As described in the next section, compared to MySpace the level of privacy management available on Facebook is much more sophisticated.

4.4 Privacy Management on MySpace

Concern for privacy has never been an emphasis on MySpace. Privacy settings are either non-existent or simplistic. Navigation to privacy settings is not intuitive. There are no direct links from the profile page to privacy settings. Instead, members must first click on Account Settings in order to access privacy sub-menus. In addition, the Account Settings link is only accessible from the home page, not from any other section of the site. So members have to first navigate back to home, then go to Account Settings, then link to privacy. Contrast this with Facebook, which has a link to privacy settings in the same section of every page on the site.


Settings: Privacy

[View My Profile](#)
[Edit Profile](#)

[Account](#) | [Password](#) | [Privacy](#) | [Spam](#) | [Notifications](#) | [Mobile](#) | [Calendar](#) | [Miscellaneous](#)

General Privacy:

Online Now: ☒ Show people when I am online

Birthday: ☐ Show my birthday to my friends


Profile Viewable By: ☒ Everyone
☐ Everyone 18 and over
☐ My friends only

Photos: ☒ Allow my photos to be shared/emailed

Block Users By Age: ☒ Allow users under 18 to contact me

Block Users: Block individual users by clicking "Block User" on their profile.
[\[View list\]](#)

[Save All Changes](#)

Online Now: When you are on MySpace, an  **Online Now!** icon will appear on your profile and wherever your name appears to let others know you are online.

Profile Viewable By: Only the people you select will be able to view your full profile and photos. Everyone else will only see your name, photo, location, and contact table.

Photos: Emailed photos contain a link to your photo on MySpace, but will be viewable according to your profile and album privacy settings.

Block Users: Blocked users will not be able to send you friend requests or messages.

Figure 4.4 Privacy management in MySpace.

Once privacy settings are reached in MySpace, they are very minimal in comparison to Facebook. If you refer to Figure 4.4, you can see a screen shot of the privacy settings for MySpace. Members have few options in terms of restricting access. They can select whether to reveal their online status. Profile visibility is either to everyone, everyone 18 and over, and friends only. By custom in the site, the vast majority of members choose the “Everyone” setting, which means their MySpace profile is as public as a web page.

MySpace includes controls over photos, but the wording is ambiguous. By allowing photos to be shared/mailed, what does that allow exactly? It does not control viewing pictures, only whether they can be transmitted to someone else. Users can be blocked by age, or by name. There are no options to allow a limited profile, or block sections of profiles from certain types of members.

Additional privacy controls are found in another sub-menu that is labeled “Spam,” (see Figure 4.5). These settings control the ability of others to send you messages, invitations, and friend requests. The fact that these controls are included in settings marked Spam is an indication of difficulties MySpace has had in limiting the site to just social interactions between friends. The fact that bands, filmmakers, and comedians are recognized as separate categories of members is an indication of the type of artistic and creative community that MySpace has attracted. It also shows that aspiring artists have used MySpace as an inexpensive publicity mechanism for their upcoming performances. In any case, using privacy settings as a control mechanism for Spam is an illustration of problems in the overall implementation of privacy management in MySpace.

Settings: Spam

[View My Profile](#)
[Edit Profile](#)

[Account](#) | [Password](#) | [Privacy](#) | [Spam](#) | [Notifications](#) | [Mobile](#) | [Calendar](#) | [Miscellaneous](#)

Spam Presets

Overall Level :

Low Medium High Custom

Save All Changes

Communications Settings

Messages :

☒ Allow non-friends to send me messages
☐ Require CAPTCHA for non-friends to send me messages

Friend Requests :

☐ Require last name or email address
☐ Require CAPTCHA
☒ Allow bands to send friend requests
☒ Allow filmmakers to send friend requests
☒ Allow comedians to send friend requests

Comments :

☐ Require approval before comments are posted
☐ Require CAPTCHA to add comments
☐ Only friends can add comments to my blog

Group Invitations :

☒ Allow anyone to send me invitations
☐ No one can send me invitations
☐ Allow only my friends and:

☐ Regular MySpace Users
☐ Bands
☐ Filmmakers
☐ Comedians

Event Invitations :

☐ Allow anyone to send me invitations
☐ No one can send me invitations
☒ Allow only my friends and:

☐ Regular MySpace Users
☒ Bands
☐ Filmmakers
☐ Comedians

Figure 4.5 Options to control spam in MySpace.

Figure 4.6 presents a graphical representation of the differences in terms of typical privacy settings in Facebook compared to MySpace. For Facebook (the figure on the left), the typical profile privacy setting is visible to friends and members of a school or organizational network, and partially visible to members of a regional network. Typically contact information is not visible to a regional network (see Figure 4.6).

Profiles are not visible to members outside one's networks, and the only way to become visible to someone in a different network is by becoming a friend.

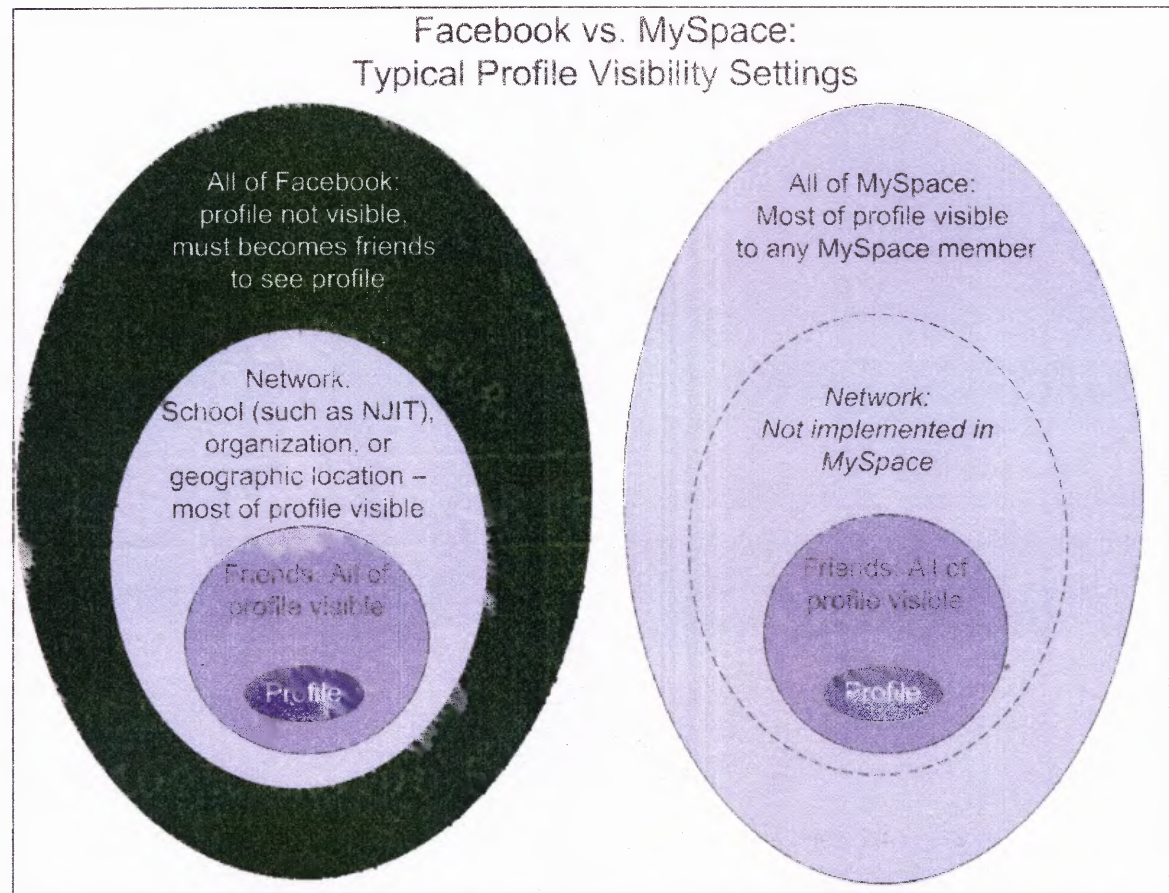


Figure 4.6 Privacy settings control the visibility of profiles.

For MySpace, the vast majority of profiles are public to everyone, which makes them as public as a web site. MySpace does not define networks or use them to manage visibility. People are either visible to just their friends, or to all of MySpace. Members have limited ability to set restrictions on non-friends. For example, MySpace has a setting that allows only friends to post public comments or post bulletins. From the comparison in Figure 4.6, it is clear that profile visibility is much less restricted in MySpace compared to Facebook.

4.5 Complexities of Privacy Management

Privacy management online presents many levels of complexity to members of social networking sites. Privacy itself is a complex social concept that has undergone extensive changes over the centuries, and is interpreted differently based on cultural and personal perspectives (Lessig, 1998). Research has found that privacy is a multi-dimensional construct (Smith et al., 1996).

In addition, privacy management online is cognitively complex. This is because the disclosure implications of pieces of information must be considered across both time and space. In addition, settings control information access by category, not by each piece of information added to a profile. You can set up restrictions for all photos, all videos, all blog entries, and so forth. This lets you control access to all video entries, but not just one out of your selection. Since limiting everything in a category is usually overkill, members may not bother. In addition, you may forget that you restricted access to photos, but did not do anything about videos. You may end up posting an embarrassing video thinking it is visible only to your friends, and then find out your school's administrators have seen it.

An illustration of the cognitive complexities that arise from privacy management is the case of Caroline Giuliani, whose father Rudy ran president in 2008 Republican primaries. Like most other college freshmen, she had a Facebook profile, and joined the network of Harvard University where she is a student. It became public in August 2007 that she had joined a Facebook group in support of Barack Obama, a Democratic candidate for president. This quickly became the talk of blogs and the online media, especially since it was public knowledge that Caroline was estranged from her father and

had refused to appear publicly with him at campaign events. Within 24 hours of the revelation, Caroline had dropped her membership in Facebook. In this case, although her profile was private, her membership in a Facebook group was public to any other Facebook member. It is confusing when the same piece of information – her membership in the Barak Obama group – can have different levels of information visibility. After her membership in the Barak Obama group became public, the option she selected for protecting the rest of her privacy was to drop out of Facebook completely (Caldwell, 2007).

Even if privacy settings are used and match the information requirements of members, they can be broken through hacks or by other security breeches. A hack that became publicly available on the Internet was used to read the private messages of two sister celebrities, resulting in the publication of their personal and private messages to each other discussing intimate topics (BestWeekEver, 2006). This adds to the difficulty of managing online privacy.

4.6 Problems with Privacy Management

While privacy has many different philosophical interpretations (Lawler & Molluzzo, 2005), the one perspective that typically guides online privacy management is the information privacy perspective (Tavani, 2000). Privacy management in social networking sites is largely based on this information privacy interpretation. This perspective defines members' privacy as their ability to control access to personal information. The code that implements this perspective treats each piece of information as an atomic element. This implementation of privacy management must address access

to N pieces of information by N potential recipients. If this is not complex enough, unknown recipients from the future must also be considered in this privacy calculus. This results in an $N * N$ problem, defined in computer science as a wicked or intractable problem (Ackerman, 2000).

This approach is flawed on many levels. It is onerous for both members and systems designers. If members actually had to consider the privacy levels of every action they take on a social networking site, they would never have time to do anything else. For designers, it requires an infinite space on the interface for privacy settings, along with infinite storage space for saving those settings. In addition, privacy is a form of risk, and this approach treats the privacy implications of all information as if they had the same degree of risk. It also assumes that risk is the same across social boundaries, and that it remains static going forward.

4.7 Appropriation of Privacy Management

A comparison of the motivation of members who create an online profile versus the nature of privacy management in social networking sites shows them to be in direct conflict. Social networking sites work hard to create tools that support the ability to express oneself through a profile. This results in more active engagement with the site and its members. However, privacy management depends on sharing less information with a smaller audience.

Research on knowledge contribution within online communities has addressed a construct referred to as perceived identity verification. This is the degree to which a person feels that other members of an online community can identify them. A study

found there is a positive correlation between willingness to share knowledge and perceived identity verification. Perceived identity verification is also correlated with overall member satisfaction with an online community (Ma & Agarwal, 2007). These results should not be surprising, because higher engagement in a community offline is also correlated with greater contributions and greater overall satisfaction (Putnam, 2000).

The goal of online self presentation within social networking sites is to create a rich, authentic profile that keeps friends up to date on your activities and presents an interesting personality to potential new friends. Privacy management consists of a collection of settings that either restrict what information is available or restrict the scope of the audience. It does not seem possible to present a rich, authentic digital profile while carrying out a faithful appropriation of privacy management. This is because of the following issues:

- Privacy management works by limiting information, especially that which is potentially sensitive. This results in a profile that looks more like a resume than something that would spark the interest of others (boyd, 2007).
- Young consumers value honesty and authenticity, and can easily spot insincerity. They have become jaded by intense marketing and spin doctors, and value something that is “real,” (Atal & Wilson, 2007).
- Privacy management works by limiting the potential audience for your profile. This not only protects privacy, but it also cuts off the opportunity to develop new relationships, or rekindle distant ones. This is the equivalent of hiding your lamp under a bushel.²

By this analysis, there is a conflict between the goals of creating an interesting profile and practicing faithful privacy management. Insight into the nature of this conflict, as well as how members resolve it, can be addressed by approaching this as an

² “No one lights a lamp and hides it in a jar or puts it under a bed,” Luke 8:16

appropriation issue. By studying the process by which members adapt and adopt privacy management, new insights can emerge as to what methods are employed to resolve this conflict. In this case, signs of unfaithful appropriation may not be symptoms of misuse; instead they may be symptoms of members' grappling with difficulties in protecting their information with tools that have the potential to restrict their ability to present a faithful profile.

There exists a fundamental mismatch between online privacy needs and privacy management functionality that can hopefully be explained more clearly by application of the appropriation perspective. The next chapter introduces a new conceptual model that uses appropriation and the Adaptive Structuration Theory in order to present a richer understanding of the design and use of social networking sites.

CHAPTER 5

THE SOCIAL SOFTWARE PERFORMANCE MODEL

5.1 Research Questions

On the surface, the use of privacy management structures by members of social networking sites seems at best naïve, and at worst quite dangerous. Studies by Gross and Acquisti (2005 and 2006) found that “a vanishingly small percentage” of members of social networking sites make any revision to the default privacy settings. Two MIT undergraduates demonstrated they could write a fairly simple Perl script that could copy the profiles of over 70,000 Facebook members (H. Jones & Soltren, 2005). Researchers have also shown that the content of profiles is easily accessed and can be used for data mining (Liu & Maes, 2005).

Many examples of information systems research describe instances of user behavior that at first do not make sense. If behavior at first does not seem rational, then deeper explanations must be sought. The research tradition of interpretativism argues that social phenomena cannot be explained in isolation. Specifically, the approach named **hermeneutics** argues that in order to grasp the meaning of an action or statement, you must first place it within the context of the situation or world-view from which it originates (Lee, 1997).

Applying the hermeneutic perspective to privacy management means more effort must be given to understand the context of use. This is a very tall order, and this dissertation cannot hope to fully tackle that task. However, a much richer understanding of privacy management will evolve from an in depth analysis of the appropriation of privacy management that takes place on social networking sites.

One important change as noted by boyd and Heer (2006) is the blurring of boundaries between public and private. The simultaneous public and private nature of the profile and social interaction creates a high degree of cognitive complexity. This makes it difficult for users to identify the potential audience for “performance,” to use the term as coined by Goffman (1959). What conflicts does this raise, and how do these conflicts influence usage and design?

A key part of social networking sites is the opportunity to create a persistent digital identity that can connect you to existing and new friends. The development of a persistent digital identity is both a chance for self expression and a dangerous opportunity for privacy invasion. How can these conflicts be resolved? This involves both understanding positive and creative forces-- identity as performance -- as well as issues of risk with respect to privacy, security and restrictiveness.

How do individuals appropriate technology in order to present attractive self presentations and protect privacy? To what extent are these two tasks in conflict? How is this conflict resolved? How do human agents appropriate digital self presentation in the face of varying levels of privacy support? These appropriation strategies have not been defined or explored. As shown in studies of email (Marcus, 1994), the use of computer mediated communication can affect social structure in unpredictable ways. The structuration perspective sees technology as an opportunity for structuring (Barley, 1986). What does the structuration perspective tell us about the use of social networking sites?

5.2 Foundations of Conceptual Model

This chapter describes the Social Software Performance Model, which combines several theoretical frameworks in order to more accurately describe and predict the structure and use of social networking sites. The model outlines the process by which social software is developed, implemented, evaluated, and revised. Because social software is an example of a socio-technical system, both task requirements and social requirements must be actively addressed by designers (Ackerman, 2000). While the model describes a general evaluation of social software, only a specific section of this model will be studied in depth. The section selected for more intensive study will be centered around appropriation, and specifically appropriation of privacy management.

This model is largely built on the Fit Appropriation Model (Dennis et al., 2001). The Fit Appropriation Model is a useful starting point because it divides system functionality into two parts: one focused on supporting the task, and the other focused on supporting the social processes involved in completing the task. The part of the system that specifically supports appropriation is named by Dennis et al. as appropriation support.

Separating appropriation support from the task model allows designers and researchers to focus on the components that address social requirements, and helps determine how effective that support really is. Following the language of the Fit Appropriation Model, successful appropriation support would result in a faithful appropriation of the technology.

The Social Software Performance Model is shown in Figure 5.1. It includes the same basic components as the Fit Appropriation Model, but also adds a feedback loop,

connecting performance, through habitual routines, to system design processes. The Fit Appropriation Model does not specifically address feedback, or processes by which issues related to appropriation and evaluation can result in changes to the system.

This feedback loop is added because the rapid evolution of social networking sites makes it clear that a feedback loop is in place. There are many instances in the short history of social networking sites that emphasize the importance of following the feedback from evaluation of task technology fit, performance and patterns of appropriation, back to the design process.

5.3 The Social Software Performance Model

The Social Software Performance Model combines the perspectives of task technology fit, appropriation (from Adaptive Structuration Theory), and the feedback cycle from socio-technical systems theory. Task technology fit theory argues that fit is a predictor of performance (Goodhue & Thompson, 1995). Fit is the degree to which system functionality fully supports the needs of a specific task. Task technology fit research also indicates that individual factors influence fit as well. This is represented in the Social Software Performance Model, where you can see that fit is connected by incoming arrows with task requirements, social software functionality, and individual factors. There is also see an out bound arrow from Fit to Performance, predicting that fit will influence performance.

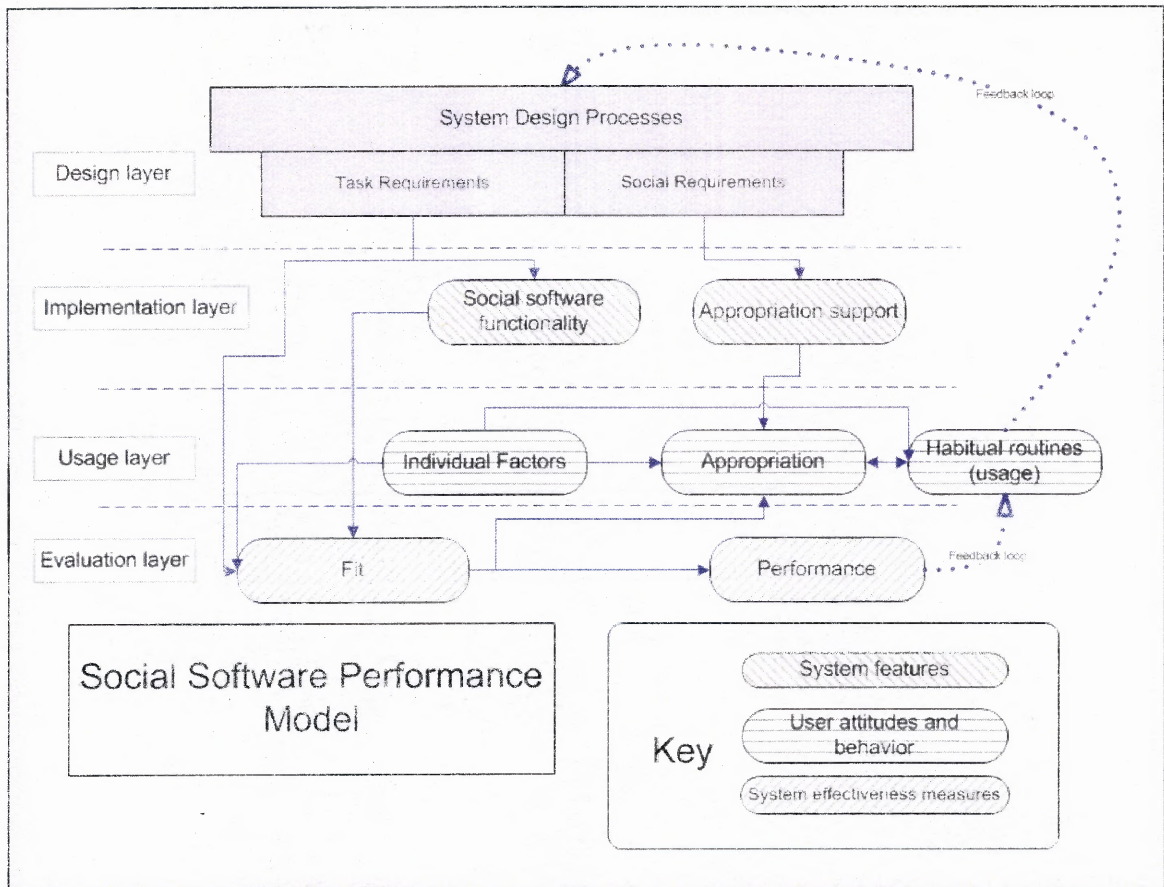


Figure 5.1 Conceptual Model: Social Software Performance Model.

Continuing the basic structure of the Fit Appropriation Model, the Social Software Performance Model as makes appropriation a central part of the model. As Dennis et al. (2001) argue, appropriation support is related to appropriation, as is fit, as well as habitual routines (usage). An addition to the Fit Appropriation Model is the link from Individual Factors to appropriation. Because appropriation was at first studied in group support systems, individual factors were not emphasized. In the case of social software, the manner in which members use these sites is an individual process. Therefore individual factors must be considered in presenting a predictive model of appropriation.

The feedback loop connects performance to usage, and finally back to design. It is represented as a dotted line, so as to not imply that feedback will happen in predictable or consistent ways. The feedback loop begins from performance because in socio-technical systems theory, the ability of a system to meet its overall goals and objectives is the starting point for feedback that regulates the system structure (Hughes, 1989).

The Social Software Performance Model has an additional structuring mechanism that divides the model into four layers. These layers roughly correlate to the process by which software is designed, implemented, used, and evaluated. The four layers in the Social Software Performance Model are made up of design processes, system features, user behavior, and system effectiveness measures. Each of these layers is labeled in the key provided (see Figure 5.1).

Design processes influence the building of basic system functionality, appropriation support, and the development of the task requirements for social interaction. The general task requirements for social software include the following:

- self presentation – individuals must be able to present a portrayal of themselves, in order to communicate news to friends, and stimulate interest from others who are seeking new relationships
- relationship initiation – members must be able to learn about others, making initial contact, sharing common experiences/interests, and then perhaps initiating a stronger relationship
- management of ongoing relationships – members must be able to contact others, learn about their activities, and make available information about their activities.

It is especially important that designers of social software take special effort to define social requirements (Whitworth & de Moor, 2004). Social requirements include privacy and setting expectations and standards for member behavior and site usage. For example, many sites allow other users to report inappropriate content (such as

pornography). Once content has been flagged as inappropriate that content can be removed or restricted in some way.

The next section of the model is the implementation layer. This contains actual functions as implemented in hardware and software. These functions have been built based on an understanding of the task model. In order to support social interaction, social networking sites typically provide the following functional components:

- digital self representation through profiles
- communication tools for both synchronous and asynchronous contact
- linked, visual representation of ego-centric social networks.

This model can be adapted to other examples of social software. Depending on the nature of social interaction being supported, related or similar functionality will be implemented.

Also within the implementation layer is appropriation support, the goal of which is to encourage faithful appropriation. Encouragement of pro-social rather than anti-social behavior is an important requirement for social software systems (Whitworth & de Moor, 2004). In the case of social networking sites, appropriation support involves functionality that encourages the development of social relationships, and discourages acts that break down social relationships. Appropriation support in these sites can include the following:

- reputation management – providing reporting mechanisms for undesired behavior
- restrictive features – defining what type of information is searchable
- privacy controls – allowing customized settings for each member

The next section of the model, the usage layer, represents how members use the site, as well as individual factors that influence use. Individual factors have been found to be a factor in the UTAUT model of technology acceptance (Venkatesh, Morris, Davis, & Davis, 2003). Individual factors also influence task technology fit (Goodhue & Thompson, 1995). This layer also includes habitual routines. This represents how members use the site, and how frequently they return.

The final section of the model, the evaluation layer, contains system effectiveness measures. These measures are fit and performance. Fit, in this model, is defined as the ability of the functionality of social networking sites to support the task model for social interaction. Performance is defined as perceived efficiency, effectiveness, and satisfaction with use of the site.

5.4 Empirical Test of a Portion of the Social Software Performance Model

Since the full Social Software Performance Model has not been tested, a prudent approach is to take a section and carry out research to validate a portion of the model. The section that has been selected for further empirical test revolves around appropriation. This section has been selected because, as argued in the previous chapter, the appropriation perspective is expected to lead to a deeper understanding of the use of privacy management on social networking sites.

This is an important topic for several reasons. First, there are many similarities between issues of privacy management and the problems with privacy that are common within many Web 2.0 applications. Secondly, looking more closely at privacy appropriation can flesh out in more detail the nature of the perceived conflict between

fully engaged personal expression and problems with privacy. This has the potential to lead to new understandings of the nature of online privacy.

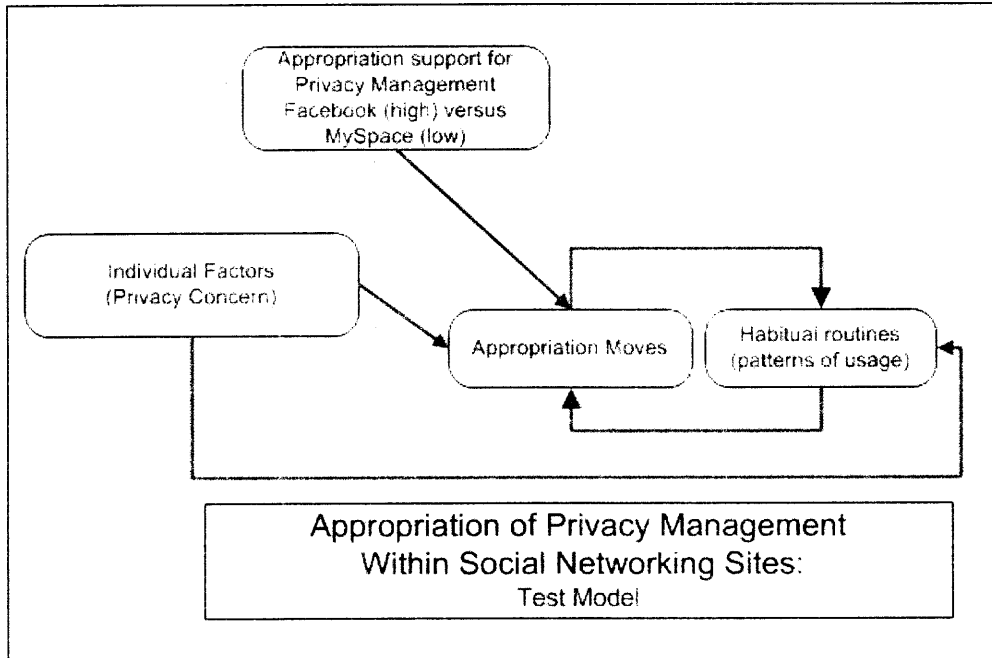


Figure 5.2 Components of model to be tested.

The components to be tested are presented in Figure 5.2. The main dependent variable is appropriation moves. Factors that are expected to influence appropriation moves include individual factors (specifically privacy concern), appropriation support, and habitual routines. Each of these variables will be described in more detail in the next section.

5.5 Appropriation and Appropriation Moves

Appropriation is the process by which people apply and adapt technology to their tasks. Using the terminology of Adaptive Structuration Theory (DeSanctis & Poole, 1991; DeSanctis & Poole, 1994), users faithfully appropriate the technology when they use it in

compliance with what DeSanctis and Poole call the spirit of the technology. The spirit is the general values for the technology. If the technology is used in a manner not consistent with its spirit, this is referred to as unfaithful appropriation (Dennis et al., 2001).

DeSanctis and Poole developed 9 types and 30 sub-types that define possible “appropriation moves.” These moves describe ways that individuals can appropriate technology. These types capture how people directly use or appropriate technology, how they “make sense” out of the technology, how they relate the technology to other structures available to them, and how they misappropriate the technology.

For this research, these sub-types have been used to identify appropriation moves related to the use of privacy structures within social networking sites. One type of appropriation move identified by DeSanctis and Poole is a direct appropriation move, where a user actively makes use of a structure. For this study, direct appropriation moves include the extent to which members are familiar with privacy settings, and the extent to which members report actual use privacy settings. The specific appropriation moves developed for this study will be described in Chapter 6.

An example of an unfaithful appropriation is what DeSanctis and Poole call a paradox, which is a combination of contrary structures with no acknowledgement that they are contradictory. In the case of social networking sites, an example of this would be related to control over whether others can find out if you have viewed their profile. For example, if members indicate they would be interested in knowing who has viewed their profile, while at the same time prohibiting others from seeing the profiles they view, this would be an example of a paradox.

5.6 Appropriation Support

Appropriation support is the design of components for a social technical system with the intent to influence appropriation, or patterns of use (Dennis et al., 2001). In GSS literature, this is referred to as process support. It includes technology components that encourage those using GSS to take advantage of the existing structures to support more effective group interaction.

For this research, the focus will be on appropriation support for managing privacy within a social networking site. Facebook provides much more privacy appropriation support compared to MySpace. The differences between privacy management on Facebook and MySpace are summarized in Table 5.1. On a fairly consistent basis, the nature of privacy management on Facebook is more developed, nuanced, and supported with an accessible user interface. There are many examples where the design of Facebook supports privacy.

This takes the form of more precise privacy restrictions on Facebook compared to MySpace. For both sites, members create and display a profile. For MySpace, your profile privacy options are either public to all or public to just your friends. For Facebook, the most restricted option is public for just your friends. The next option is public to your friends and your network. A network is a sub-set of Facebook, tied to a school, a work organization, or a location, such as San Diego. You must explicitly join a network. In order to join a network associated with a university you need to have a valid school email address. There is no universal public profile option for Facebook.

Table 5.1 Privacy Management Components

Component	Facebook	MySpace	Comments
What profile privacy settings are available?	Friends and network or just friends	Just friends or public to all	Facebook has more restricted visibility. It is not possible to make your profile visible to all of Facebook.
What is the domain for searches?	Within a specific network, tied to an organization or location	All of MySpace	Domain for search in Facebook is limited by design.
Can you adjust whether your profile can be searched by anyone on the site?	Yes -- can set it to allow only certain network to conduct search on your name	No	You can remove your profile from search options in Facebook. There is no way to remove your profile from search in MySpace.
Allow blocking of individual users?	Yes	Yes	Same in both.
Enable member to limit access by individual user?	Yes	No	Facebook offers more granular control over access to information.
Enable member to control access to parts of profile?	Yes	Partial -- can control access to blog and comments	Control over access to parts of profile is more granular in Facebook.
Supports different privacy levels for specific information based on network, i.e., show contact info to only certain network	Yes	No	Facebook allows you to show a more restricted profile to certain networks. This is not available in MySpace.

The search function in Facebook is more restrictive than MySpace. When searching for a person, you must select a network to search in. Only if the search fails in that network can you search all of Facebook. For MySpace, search is by default for the entire site. You can simply enter a search term from your profile and see links to all profiles that match.

Facebook supports more precise privacy settings on several levels. While both sites allow members to block individuals, Facebook allows you to specify individuals who can only view that limited profile. For example, if you had “friended” a teacher or your parent, you can set exactly what you want them to see. Facebook also has settings for individual components of your profile. For example, you can choose to show your instant messenger screen name to only your friends, while displaying the rest of your profile to your network. MySpace does not support these tiered levels of privacy.

In addition, Facebook uses a visualization tool to present to each member the state of his or her privacy settings. The visualization is a scroll bar that goes from left (most restrictive settings) to right (most open settings). By clicking on the scrollbar, a member can view and adjust their privacy settings for different components of their account.

5.7 Individual Factors and Habitual Routines

The remaining two variables that are included in the predictive model are individual factors (Concern for Internet Privacy) and Habitual Routines, or usage. Concern for privacy measures an individual’s level of concern with regard to privacy on the Internet. Privacy concern has been a long term subject of study (Westin, 1996), and recent findings suggest that overall concern is rising (Buchanan et al., 2007). An existing measure of

Internet privacy concerns has been adapted for use in this research, and has already been tested within several pilot studies, including one described by Dwyer, Hiltz, and Passerini (2007).

Usage refers to the frequency of use. Earlier pilot studies have found that as many as half of all subjects report accessing sites every day. In addition, results from pilot studies suggest there are differences between subjects who use the site every day versus those who use it on an occasional basis. This difference in usage certainly seems relevant to privacy. The more you use a social networking site, the greater the amount of information you are sharing, and the greater your privacy risk.

5.8 Hypotheses and Research Questions

This next section will provide formal definitions of each variable and state the hypotheses that will be tested in the study. A more specific description of how each variable will be operationalized can be found in the next chapter.

5.8.1 VARIABLES

5.8.1.1 Independent Variables.

- **Concern for Internet Privacy:** High versus Low concern. This will be measured by using an adapted version of the Concern for Internet Privacy Scale, (Buchanan et al., 2007) and tested in several pilot studies (Dwyer et al., 2007; Dwyer et al., 2008).
- **Appropriation Support For Privacy Management:** High (Facebook) versus Low (MySpace). This variable indicates the extent to which a sites provides functionality that encourages the use of privacy settings.

5.8.1.2 Intervening Variable.

- **Usage:** This is a measurement of frequency of use, or frequency of access. High usage members will be those who access the site at least once a day. Low usage members will be those who access the site less than once a day.

5.8.1.3 Dependent Variables.

Appropriation Moves: The manner in which a member appropriates or makes use of a privacy structure. This is a composite measure of six defined appropriation moves (described in Chapter 6), based on the definitions from Adaptive Structuration Theory (DeSanctis & Poole, 1994). These measures are organized in the following way:

- faithful appropriations: to what extent do members use privacy settings to manage their privacy in a way that is consistent with the spirit of the a social networking site (three faithful moves).
- unfaithful appropriations: to what extent do members ignore, criticize, or misuse all or most of privacy settings (three ironic moves). Ironic appropriation moves are ones that indicate use of structures in a way that is inconsistent with the spirit of the system.
- self report of unfaithful appropriations: this is a self report on unfaithful appropriations, based on (Chin et al., 1997).

5.8.2 HYPOTHESES

5.8.2.1 Main Effects for Appropriation Support. As described in the Fit Appropriation Model and summarized in Section 3.3, appropriation support is predicted to lead to an increase in faithful appropriation moves, and ultimately an improvement in performance and system success. Extending the Fit Appropriation Model and Adaptive Structuration Theory, it follows that if a social networking site includes a higher level of appropriation support for privacy management, then it members will report a higher level of faithful appropriation of privacy management. This leads to the following:

A social networking site with high appropriation support (Facebook) will encourage more faithful appropriation of privacy management compared to a site with low appropriation support (MySpace).

H1. Members of systems with high levels of appropriation support (Facebook) will have more faithful appropriation of privacy management compared to members of systems with low levels of appropriation support (MySpace).

H2. Members of systems with high levels of appropriation support (Facebook) will have fewer unfaithful (or ironic) appropriation of privacy management compared to members of systems with low levels of appropriation support (MySpace).

H3. Members of systems with high levels of appropriation support (Facebook) will report a higher level of faithful appropriation of privacy management compared to members of systems with low levels of appropriation support (MySpace).

5.8.2.2 Main Effects for Privacy Concern. Task technology fit, as part of the Fit Appropriation Model, includes individual factors as part of the model (Goodhue, 1995). As described above in Section 3.3, task technology fit argues that an individual makes a judgment to use technology based on a cost benefit analysis. It therefore follows that if an individual has a high level of privacy concern, then losing privacy would be a high cost, so therefore there is high benefit in taking active measures to protect privacy.

Following this reasoning, if members of a social networking site have a higher level of concern with respect to Internet privacy, they are more likely to appropriate privacy structures, i.e., use privacy management features. This leads to the following prediction:

High levels of privacy concern will result in more faithful appropriation moves.

H4. Members with high levels of Internet privacy concern will have more faithful appropriation moves compared to members with low levels of privacy concern.

H5. Members with high levels of Internet privacy concern will have fewer ironic appropriation moves compared to members with low levels of privacy concern.

H6. Members with high levels of Internet privacy concern will report a higher level of faithful appropriation compared to members with low levels of privacy concern.

5.8.2.3 Main Effects for General System Usage. Social networking sites support regular social interaction. The more time a member spends using a site, it follows that the more social interaction they engage in within the site, and the more personal information they share with others. As Goffman argues (see Section 3.1), people are instinctively aware of when and how they are observed by others. It is expected that due to this relationship between active use and increased personal disclosure, this will consequently result in a greater awareness of self presentation issues. Therefore it is expected that as members become more and more active, they become more and more aware of the need to safeguard their privacy while participating in social networking sites. This results in the following prediction:

High levels of usage will result in faithful appropriation of privacy management.

H7. Members with high levels of general system usage will have more faithful appropriation moves compared to members with low usage.

H8. Members with high levels of general system usage will have fewer ironic appropriation moves compared to members with low usage.

H9. Members with high levels of general system usage will report a higher level of faithful appropriation compared to members with low usage.

5.8.2.4 Interaction of High Usage and High Privacy Concern. There seems to be a contradiction between using privacy settings and at the same time actively engaging in social networking sites. Most privacy settings require limiting access and sharing less information. What happens when these limitations diminish the ability to gain the most value out of the site?

This contradiction is especially keen among those members who have a high level of privacy concern, and who also are active users of these sites. These members can be said to experience a Privacy Dilemma, defined here as the inherent conflict between frequent use of the site (which increases the possibility of privacy violations) and high Internet privacy concern (which would encourage taking action to protect privacy). This combination may create some level of anxiety about privacy in general. If privacy settings interfere with full engagement, then it remains an open question as to how these users resolve this conflict. Do they favor usage over privacy, or vice versa?

Members who experience this Privacy Dilemma are expected to have more ironic appropriation moves compared to members who do not have this combination. This is because high usage increases the privacy risk. If a member is concerned about privacy and faces increased risk due to higher usage, then that member is more likely to take individual actions to safeguard privacy. These appropriations are expected to be ironic. This is because restrictive privacy settings, as built into these sites, impinge on full social interaction carried out by high use members. These high usage, high privacy concern members are expected to make individual appropriations for privacy management.

Of particular interest to this research is whether members who match the Privacy Dilemma condition show evidence of unusual appropriation moves. There has already been some evidence of this in pilot studies conducted thus far.

That evidence came from a study that included questions about the use of tools within these sites to measure popularity and social status. An example of such a tool is a profile tracker, which shows you a list of other members who have accessed your profile. However, not all members want their viewing behavior made public. To protect privacy, sites can allow members to view profiles anonymously. This creates the possibility of a social condition, referred to here as One Sided Profile Browsing. This occurs when members can learn who views their profile while at the same time restricting information as to what profiles they themselves view.

A pilot study for this research on Facebook and MySpace subjects found that over 40% of the subjects expressed preferences consistent with One Sided Profile Browsing, and significantly more members of MySpace exhibit One Sided Profile Browsing compared to Facebook. In addition, One Sided Profile Browsing was found in more than two thirds of members who match a Privacy Dilemma, defined as an internal conflict caused by high levels of privacy concern combined with frequent usage of these sites. The measures that capture One Sided Profile Browsing are included in this study.

This research will address this type of use as a form of appropriation, albeit an ironic or unfaithful one. Social conditions are thought to trigger an adaptation or appropriation that users take on in the face of conflicting motivations. Faced with such a conflict, users sometimes act to maximize their gains at the expense of others.

An appropriation is said to be ironic or unfaithful if it conflicts with the “spirit” of a system, spirit being the general intent with regard to a system’s fundamental values and goals. One Sided Profile Browsing is an example of an ironic appropriation. The spirit that guides the design of social networking sites is in support of positive social interaction, not interaction that benefits one member over another. This results in the following prediction:

H10. For members with high usage, those members with high Internet privacy concerns will have more ironic appropriation moves compared to members with low Internet privacy concern.

5.9 Open Research Questions

While it is anticipated that there will be some relationship between concern for Internet privacy, appropriation support, and usage, our understanding of the dynamics of these sites is not sufficient enough to predict the nature of those relationships. These will remain as open research questions. What is the effect of high privacy concern on levels of usage? What is the effect of appropriation support for privacy management on levels of usage?

CHAPTER 6

DESIGN OF THE SURVEY INSTRUMENT

The survey instrument was developed over a two year period, and is the culmination of research that included an in-depth qualitative study of the use of social networking sites, and four subsequent survey-based pilot studies.

A qualitative study based on semi-structured interviews of 19 subjects was conducted in January 2006. The results showed there was a high level of enjoyment associated with the use of social networking sites for the vast number of subjects interviewed. A more detailed description of this study is available in (Dwyer, 2007). The subjects expressed great appreciation for the ability to carry out personal self expression in the construction of their profiles. At the same time, the subjects did express concern about privacy and some anxiety about whatever bad characters may be around on these sites. From this early study, the twin themes of creative expression through digital identity construction along with non-specific privacy concern emerged.

This led to research questions that revolved around the effect of privacy concern on use of these sites. This required a reliable measure of privacy concern, as well as measures that capture other attitudes and behavior on the site. A privacy measure based on the work of Smith (1996) was adapted for online privacy and tested in a survey completed by 46 NJIT undergraduates that were members of two classes of Computers and Society. The results of this privacy measure were inconclusive, so that measure was scrapped. However, an open ended question on the benefits of social networking sites contained answers that were consistent with the findings of the January 2006 study. This

led to efforts to measure more carefully how members both use the site and manage their privacy.

Another interesting finding from the January 2006 qualitative study was that the 19 subjects interviewed were active in a variety of social networking sites, including MySpace, Facebook, Hi5, and LiveJournal. This suggests there may be differences between social networking sites that can be measured, and may influence both behavior and performance. Two popular sites, Facebook and MySpace were selected for comparative study. This was done because few if any studies of social networking sites had made any explicit comparison between sites. In addition, differences in terms of emphasis on privacy were quite substantial when comparing Facebook to MySpace. Also these sites are both extremely popular, with millions of members.

Another survey was administered in August of 2006, focused on members of Facebook and MySpace. The total number of subjects was 226, made up of 132 members of Facebook and 94 members of MySpace. It was in this survey that the measure for Internet Privacy Concern was first tested. The questions were found to have a high level of reliability as measured by Cronbach's alpha. The measure was also found to relate to other findings in interesting ways. The results that illustrate the Privacy Dilemma and One Sided Profile Browsing described in the previous chapter were obtained from this study. A more detailed description of this pilot study can be found in (Dwyer et al., 2007).

After the initial development of the Social Software Performance Model, a pilot instrument was constructed to test the measures for appropriation moves. This survey was administered in August 2007 to 51 subjects, made up of 35 Facebook members and

16 MySpace members. It included measures for usage and Internet Privacy concern that had been used in previous pilot studies. The Internet Privacy concern scale showed a high degree of reliability, with a Cronbach's alpha of .824. Over 60% of the subjects reported visiting these sites at least once a day, a result consistent with prior studies. A more detailed description of the results can be found in Appendix C.

6.1 Description of Appropriation of Privacy Management Instrument

The complete version of the Appropriation of Privacy Management Survey instrument is available in Appendix B. Here is an overview of the sections included in the survey and the questions included.

6.1.1 Demographics

- Gender
- Age
- School status (year in school)
- Ethnicity
- Country of citizenship

6.1.2 Usage

- Frequency of Use
- What information is included on the profile, for example real name, home town, email address, and so forth.
- How often they update their profile
- How often they post a message to a friend's wall or public comment space
- Whether their use of social networking sites is more than or less than a year ago

6.2.3 Concern for Internet Privacy

This scale measures to what extent subjects express concern over a number of issues related to privacy on the Internet, including identity theft, whether people on the Internet are not really who they say they are, and whether others could obtain information about their personal activities online. It is adapted from the work of Buchanan et al. (2006), and is tested on a seven point semantic differential scale, anchored by Never (1) to Always (7). The scale includes the following questions:

- In general, how concerned are you about your privacy while you are using the internet?
- Are you concerned about online organizations not being who they say they are?
- Are you concerned about online identity theft?
- Are you concerned about people online not being who they say they are?
- Are you concerned about people you do not know obtaining personal information about you from your online activities?

6.2 Appropriation Moves

The measures for appropriation moves are adapted from Adaptive Structuration Theory, (DeSanctis & Poole, 1994). All measures are designed as seven point semantic differential scales, anchored from Strongly Disagree to Strongly Agree. Three moves are examples of faithful appropriation moves, two moves are examples of unfaithful appropriation moves, and one is a measure of perception of faithfulness.

6.2.1 Faithful Appropriation Moves

Use: This move captures the extent to which members report actual use of privacy settings. Members show evidence of a faithful appropriation by actively and explicitly making use of privacy settings. It includes these questions:

- In order to control who can contact me using [name of social networking site] I have adjusted my privacy settings.
- I have modified the privacy settings for my profile on [name of social networking site].
- I have adapted the privacy settings to control who can view my profile on [name of social networking site].
- I have personalized my privacy settings on [name of social networking site].

Familiarity: This move measures to what extent members report familiarity with privacy settings. Members show evidence of a faithful appropriation by demonstrating knowledge of how to use privacy settings. It has the following questions:

- I am comfortable with my ability to adjust my privacy settings.
- I am confident that I know how to control who is able to see my profile on [name of social networking site].
- I am familiar with my privacy settings on [name of social networking site].
- When I need to modify my privacy settings for [name of social networking site], I am able to do it.

Restricted Scope: This move measures to what extent members restrict their contact within the site to those they already know, rather than exploring new relationships and engaging with new people. This appropriation move involves using part of the structure rather than completely depending on it. They are using the site, but restricting who they communicate with. This is evidence of a faithful appropriation because taking steps to

protect your privacy is consistent with the spirit of the privacy settings. It is made up of the following questions:

- I use [name of social networking site] only to contact people I see in person on a regular basis.
- I don't use [name of social networking site] to make contact with people whom I've never heard of.
- I never accept friend requests from people I have not met in person.
- When using [name of social networking site], I ignore contact from people whom I have not met in person.

6.2.2 Unfaithful (Ironical) Appropriation Moves

Rejection: This construct measures the extent to which members explicitly state they do not use or bother with privacy settings. This appropriation move describes the rejection or negation of privacy structures. This move provides evidence of a unfaithful appropriation by measuring to what extent members disagree or otherwise directly reject appropriation of privacy settings. It includes the following questions:

- I don't know what my privacy settings are on [name of social networking site].
- I don't bother to look at the privacy settings for my profile on [name of social networking site].
- I don't use the privacy settings to control who can access my profile.
- Adjusting the privacy settings for [name of social networking site] is a waste of time.

One Sided Profile Browsing: This move is concerned whether a member want to know who has viewed their profile while at the same time blocking others from knowing what profiles they themselves view. An answer of strongly agree for both questions is an indication of this condition. This appropriation move is an example of a paradox, which

is defined as a combination of contrary structures with no acknowledgement that they are contrary (DeSanctis & Poole, 1994). This move provides evidence of an unfaithful appropriation because members are using a privacy setting to block others from obtaining the same type of information they themselves are eager to obtain. This use of a privacy setting is contrary to the spirit of social networking sites, which is the support of positive social interaction. Therefore this is an example of an unfaithful move. It includes these two questions:

- I would like to know who has viewed my profile on [name of social networking site].
- I would not like other people on [name of social networking site] to know how often I view their profile.

6.2.3 Other Measures

Faithfulness: These questions are adapted from the Scale to Measure Faithfulness of Appropriation (Salisbury, Chin, Gopal and Newsted, 2002). The original scale was developed for electronic meeting systems. It has been rewritten to refer to privacy management within social networking sites. It includes these questions:

- I probably use the privacy settings for [name of social networking site] improperly.
- I failed to use the privacy settings of [name of social networking site] as it should be used.
- I did not use the privacy settings in [name of social networking site] in the most appropriate fashion.
- The founders of [name of social networking site] would disagree with how I use the privacy settings.
- The original founders of [name of social networking site] would view my use of the privacy settings as inappropriate.

Distrust: This construct measures to what extent do members have a bad opinion about other people on the site. This construct measures a criticism that is related to overall dissatisfaction with the social networking site. It also provides evidence of dis-satisfaction with overall privacy management, because a robust set of privacy protection functions would be expected to screen out people who do not seem trustworthy. It is made up of the following questions:

- I don't believe most of the information people put on their profiles on [name of social networking site].
- There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy.
- I believe most of the profiles I view on [name of social networking site] are exaggerated to make the person look more appealing.
- I have been contacted by people through [name of social networking site] whom I did not trust.

These questions were tested in a pilot study conducted in August 2007. The questions listed above were found to add to acceptable levels of reliability and load properly on the factors for each construct. The next chapter describes the methodology for the study and summarizes univariate results.

CHAPTER 7

METHODOLOGY AND UNIVARIATE RESULTS

7.1 Survey Methodology

The survey was administered using the online survey tool Zoomerang (www.zoomerang.com). This site provides tools to support survey creation, implementation, as well as basic data analysis. The survey creation tools within Zoomerang make it fairly simple to roll out an online survey quickly. Subjects were provided a link that connects them to the online survey. Zoomerang has a feature that can lock out duplicate attempts to complete a survey. Zoomerang also provides a file that can be exported and used to carry out statistical analysis using a package such as SPSS or SAS. In addition, the survey can be closed when data collection is complete. This means that subjects can no longer access the survey, but the data is retained at the Zoomerang web site. If necessary, a survey can be re-opened.

The survey consists of 61 questions. Subjects were offered five dollars in compensation for completing the survey. The demographic questions and the usage questions were kept together in the survey. All the measures for the appropriation moves were assigned in random order.

7.2 Identifying the Target Population

The target population for this study is members of the NJIT community who participate in Facebook or MySpace. This includes students, faculty, and alumni. Why select the NJIT community for study? NJIT is a fairly large university community that draws most

of its population from the same region, New Jersey. By drawing subjects from NJIT for Facebook and MySpace, the aim is to minimize potential confounding environmental variables that might occur if the sets of users sampled for the two systems came from very different kinds of populations. By sampling from the same base population, the goal is to avoid confounds arising from variables such as age, ethnic background, or regional differences.

In addition, the privacy structure of Facebook limits access to networks unless you are a member of a community. The primary researcher is a member of the Facebook NJIT community. This allowed independent access to profiles of both respondents and non-respondents. That access was used to assess the validity of self reports by respondents.

As of September 27, 2007, the target population in the NJIT Facebook network was 6,467. This information is available from Facebook. The site tracks the size of each network and makes that information available to its members. Facebook organizes communities around organizations such as universities and colleges. When college students join Facebook, they typically do so using their school e-mail address, which allows them to join a network for a particular school.

For MySpace, the target population is not specifically identified and organized by the functionality of the site. Therefore, it was not as straightforward to determine who is in the target population, or how big it is. The method for identifying and contacting the target population is described in the next section.

7.3 Survey Administration for MySpace

Using the tool Friend Blaster Pro (<http://www.friendblasterpro.com>), the MySpace site was searched for potential subjects that are part of the NJIT community. This was accomplished by first looking for members who mention NJIT in their profile. Additional searches were made for groups on MySpace with an NJIT affiliation. The results from these searches were combined, and duplicates were dropped. This resulted in a target population of 986 members on MySpace with an NJIT affiliation identified through these search mechanisms.

Each MySpace profile is identified in MySpace by a unique profile ID number. This number can be used to both see the member's profile, and send them a message through MySpace. Using these numbers, each of the 986 members were contacted and invited to participate in the survey.

The first invitation attempt was done through the use of a script that automatically generated invitations and sent them to the selected subjects. However, the script (also part of Friend Blaster Pro) worked erratically, so therefore the invitations were re-sent by individually contacting each subject. At least one attempt was made to contact each subject on the list, although 22 subjects blocked messages from unknown MySpace members. Every subject that could be contacted was sent at least one invitation to participate, and 927 out of the 964 received two invitations. The survey was fully completed by 115 MySpace subjects, resulting in a response rate of 11.9%.

7.4 Survey Administration for Facebook

Potential subjects from Facebook were identified by using a search tool that is part of Facebook. This tool returns a random selection of 10 profiles from a target network, in this case the NJIT network. Because Facebook prohibits the use of any automated tools to obtain profile information on their site, and will terminate an account if there is any evidence of the use of an automated tool, the profiles were obtained “by hand,” i.e., by repeatedly selecting the random function and saving the results. As in the case of MySpace, Facebook identifies each profile using a unique Profile ID, which can be used to both view the profile and send messages.

Using this rather laborious process, about 900 profiles were collected. Once duplicates were eliminated, this resulted in a sample frame of 778 potential subjects. Of these, 109 restricted access to their profile to friends only (14%), and 669 (86%) had their profile visible to other members of the NJIT network.

The initial plan was to contact subjects using the messaging function of Facebook. However, after only about 15 invitations had been sent out using this method, a warning was received from Facebook indicating the research invitations sent out had been tagged as spam, and that messaging ability was temporarily suspended in order to protect other members from unwanted spam. Customer service for Facebook was contacted, with an explanation that invitations for participation in research were being distributed, but the response was that this still was considered to be against the terms of use of the site, and made any further use of Facebook messaging to recruit subjects liable to result in the suspension of the primary account being used for the study.

Since contacting these subjects through Facebook was not going to be an option, potential subjects were instead contacted via their NJIT email address. Going through the profiles one at a time, each potential subject was found in the online NJIT email address directory. If that address was available, it was used to send an email invitation to participate in the study. Each subject received two invitations via email to participate in the study. If the email address was found to be invalid or not available, the subject was sent a brief and as un-spam like as possible message via Facebook with information on how to participate in the study. Using these methods, 753 out of the 778 were invited to participate in the study. 107 subjects completed the survey, for a response rate of 14.2%.

7.5 Calculating the Confidence Level

The confidence level is based on the Central Limit Theorem (Rosenthal & Rosnow, 1991). If a population is repeatedly sampled, then the average value of the attribute being measured approaches the true mean of the population. The confidence level describes what percentage of the samples drawn will have a true population value within the level of precision. If the confidence level is 95%, then 95% of the samples drawn will produce means that fall within the true population mean, plus or minus the sampling error.

The level of precision, also referred to as the sampling error, is expressed as a percentage, for example $\pm 5\%$. So if the results in the sample say a value is 40%, then the value in the total population is expected to fall between 35% and 45%.

The target population for Facebook is approximately 6500 and the target population for MySpace was found to be approximately 986, although there is no reliable way to verify this is the true size of the target MySpace population.

With 107 responses from Facebook subjects, this results in a sampling error of $\pm 9.5\%$ and a confidence level of 95%. With 115 responses from the MySpace subjects, this results in a sampling error of $\pm 5.9\%$ and a confidence level of 95%.

7.6 Analysis of Missing Data

The amount of missing data is minimal, amounting to a handful of instances per question. The largest number of missing questions is 10 out of 222, which is 4.5% (for listing whether the subject includes their cell phone number in their profile). The complete results for what data is missing can be found in Appendix A. That is well below the 15 to 20% threshold level described in (Hair, Black, Babin, Anderson, & Tatham, 2006) for either dropping cases or making adjustments. Based on the recommendations of Hair et al, this pattern of missing data can be ignored as minimal or random.

7.7 Demographic Data

The demographic data for the survey is summarized in the Table 7.1. A total of 222 subjects completed a valid response to the survey, 107 completing the Facebook survey and 115 completing the MySpace survey. There are significantly more male (160) than female (62) subjects for this study, which is consistent with the target population of NJIT students, staff and alumni. There is no significant difference in the gender distribution between the Facebook subjects (30 female and 77 male) and the MySpace subjects (32 female and 82 male).

Table 7.1 Summary of Demographic Data

		Facebook	MySpace
Gender			
	Male	77	83
	Female	30	32
Age			
	18-22	56	49
	23-29	43	44
	30-39	6	16
	40+	2	6
School status			
	Freshman	15	5
	Sophomore	13	17
	Junior	9	14
	Senior	21	19
	Masters student	24	16
	PhD student	4	1
	Faculty	1	1
	Staff	1	2
	Not a student	18	39
	No response	1	1
Ethnicity			
	White	50	66
	Asian	31	6
	Hispanic	10	20
	Mixed Race	4	9
	African American	2	4
	Other	7	10
	No response	3	0
Citizenship			
	USA	77	107
	India	10	0
	Other	19	8
	No response	1	0

The ages of the subjects ranged from 18 to 69. The mean value is 24.53, the median is 23, and the mode is 22. There is a small but significant difference in age between the Facebook and MySpace subjects, Facebook age mean is 23.07, MySpace age mean is 25.89, $t\text{-value} = -2.911$, $\text{sig.} = .002$, $df = 220$.

The largest group of subjects is comprised of undergraduates, with 58 from Facebook and 55 from MySpace. This is followed by graduate students (28 Facebook and 17 MySpace), faculty or staff (2 Facebook and 3 MySpace), and 57 indicating they are currently not a student (18 Facebook and 39 MySpace). There is a higher number of non-students that are part of the MySpace population (34%) versus the Facebook population (17%). The differences in school status between the two populations is significant (Pearson Chi-Square = 19.92, $df = 10$, $sig. = 0.029$).

The ethnicity of the subjects is diverse, as is to be expected by the target population of the NJIT community. About 52% of the subjects describe themselves as White, while about 16% describe themselves as Asian, 13% as Hispanic, 6% as mixed race, 3% as African American, with the remaining subjects distributed into 11 other categories.

There is a noticeably higher percentage of Asian Facebook subjects, and a higher percentage of MySpace Hispanic subjects. The differences in ethnicity between these two populations is significant (Pearson Chi-Square 39.78, $df = 17$, $sig. = 0.001$). This result is consistent with other studies comparing the two sites, one based on ethnography (boyd & Ellison, 2007), and one based on survey data (Hargittai, 2007). The vast majority of subjects described themselves as American citizens (179 out of 222).

7.8 Site Usage Data

Site usage data is summarized in Table 7.2. Consistent with pilot studies conducted prior to this study, subjects report quite active use of social networking sites. 45 Facebook and 39 MySpace subjects use the site every day or several times a day, and another 47

Facebook and 47 MySpace subjects use the site at least one a week. Only about 18% (42 out of 222) use the site infrequently (once in a while). There is no significant difference in the frequency of use when comparing Facebook subjects to MySpace subjects.

Table 7.2 Summary of Site Usage Data

		Facebook	MySpace
	Number of subjects	107	115
Usage	(no significant difference)		
	Several times a day	20	14
	Every day	25	25
	Several times a week	31	33
	Once a week	16	14
	Once in a while	14	28
	Never	1	1
Use of other site	Pearson Chi-Square= 27.98, df= 2, p<.00001		
	Active on both sites	31	74
	Have two accounts, but only active on one site	27	13
	Have one account	49	28
Update profile	(no significant difference)		
	Every day	0	1
	Several times a week	5	1
	Once a week	4	0
	Once in a while	80	94
	Never	18	19
Post a public message	Pearson Chi-Square = 10.47, df=4, sig. = .03		
	Every day	3	1
	Several times a week	19	6
	Once a week	13	16
	Once in a while	63	78
	Never	9	14
Use over time	(no significant difference)		
	Same as a year ago	48	52
	Less than a year ago	19	33
	More than a year ago	38	27
	Other	2	3

An interesting finding is the degree to which subjects report active use of both Facebook and MySpace. While 47% (105 out of 222) report they are active on both sites, i.e., visiting the second site more frequently than once a month, MySpace members are

significantly more likely to report active use of both sites (Pearson Chi-Square=27.98, $df=2$, $p<.000001$). 27 Facebook and 13 MySpace members report they have an account on the other site but use it infrequently, and 49 Facebook and 28 MySpace members have only one account. The fact that most of the subjects have experience with both sites has potential to act as a confounding factor when comparing the results for these two sites. The extent to which such multiple memberships occur for the total population of social networking sites is unknown.

Most subjects report they update their profile “once in a while.” This includes 80 Facebook subjects and 94 MySpace subjects. A total of 18 from Facebook and 19 from MySpace report they never update their profile.

More than three quarters of the subjects (78%) report posting messages to a public area on a friend’s profile known in Facebook as “the wall,” and in MySpace as a comments area, “once in a while.” This includes 63 from Facebook and 78 from MySpace; 9 Facebook subjects and 14 MySpace subjects report they never do this. There are significantly more members who post several times a week or more on Facebook compared to MySpace.

About 45% of subjects (48 from Facebook and 52 from MySpace) report use of social networking sites about as frequently as a year ago. 24% (19 from Facebook and 33 from MySpace) report they are using these sites less frequently than a year ago, and 29% report they are using the sites more frequently (38 from Facebook and 27 from MySpace).

Table 7.3 Summary of Information Subjects Include in Their Profile

Included in Profile		Facebook	MySpace
Photograph	(no significant difference)		
	Yes	105	108
	No	2	7
Real name	Pearson Chi-Square = 29.10, df = 1, p<.00001		
	Yes	105	82
	No	2	32
	Missing		1
Hometown	(no significant difference)		
	Yes	93	99
	No	13	16
	Missing	1	
Email address	Pearson Chi-Square = 97.53, df = 1, p<.00001		
	Yes	92	22
	No	14	89
	Missing	1	4
Cell phone number	Pearson Chi-Square = 27.396, df = 1, p<.00001		
	Yes	25	1
	No	77	109
	Missing	5	5
Relationship status	Pearson Chi-Square = 8.397, df = 1, p = .004		
	Yes	80	104
	No	25	11
	Missing	2	0
Sexual orientation	(no significant difference)		
	Yes	87	96
	No	18	18
	Missing	2	1
Instant messenger screen name	Pearson Chi-Square = 28.323, df = 1, p<.00001		
	Yes	65	31
	No	36	80
	Missing	6	4

Data were also collected from subjects as to what information they include in their profile. This data is summarized in Table 7.3. There are marked differences in terms of what information is included, with much more being included by Facebook subjects compared to MySpace subjects. The most striking example is listing of cell phone number on the profile, with only one subject out of 110 MySpace subjects answering yes

to this option compared to 25 out of 102 for Facebook. For results on listing real name, email address, instant messenger screen name, and cell phone number, Facebook members are significantly more likely to include this information. However, MySpace members are significantly more likely to include relationship status in their profile. There is no significant difference between the sites with respect to including a photograph, listing home town or sexual orientation.

7.9 Univariate Results for Independent Variables

There are three main categories for independent variables in this study – level of Appropriation Support ((high for Facebook and low for MySpace), frequency of use, and degree of privacy concern. The results for frequency of use were presented in the preceding section. The next section summarizes the results for measures of Internet Privacy Concern.

Measures for Internet Privacy Concern

The results for the questions on Internet Privacy are summarized in Table 7.4. The results are broken out for Facebook and MySpace, although there is no significant difference in the results. This is consistent with prior pilot studies using this measure to analyze behavior on MySpace and Facebook.

Table 7.4 Summary of Results for Concern for Internet Privacy Construct

Label	Choice (SD to SA)	1	2	3	4	5	6	7
	In general, how concerned are you about your privacy while you are using the internet? Mean = 5.03, S.D. = 1.638							
IP1	Facebook	3	5	9	14	22	28	24
	MySpace	5	8	11	14	29	27	21
	Are you concerned about online organizations not being who they say they are? Mean = 5.47, S.D. = 1.379							
IP2	Facebook	1	2	8	14	21	30	28
	MySpace	1	2	8	12	31	27	34
	Are you concerned about online identity theft? Mean = 5.70, S.D. = 1.347							
IP3	Facebook	1	2	8	11	23	24	35
	MySpace	1	2	3	6	30	27	45
	Are you concerned about people online not being who they say they are? Mean = 5.30, S.D. = 1.508							
IP4	Facebook	1	6	6	14	29	26	23
	MySpace	2	7	4	17	24	27	34
	Are you concerned about people you do not know obtaining personal information about you from your online activities? Mean = 5.47, S.D. = 1.518							
IP5	Facebook	1	2	10	8	32	19	33
	MySpace	3	5	7	10	22	27	40

Also consistent with prior pilot studies is that each question is skewed to the high end. Notice the mean for each question is at least one full point above the midpoint of four out of seven. The highest level of concern is related to concern about identity theft (a mean of 5.7, with a S.D. of 1.347).

When comparing subjects from Facebook versus MySpace, there is no significant difference in terms of either frequency of use or level of privacy concern.

Is there a difference in terms of degree of high use when comparing Facebook to MySpace? As shown in Table 7.5, slightly more Facebook members compared to MySpace members access the site at least once a day, but this is not large enough to indicate a significant difference.

Table 7.5 Level of High Use for Facebook Versus MySpace Members

High Use (at least every day)		Facebook	MySpace	Total
Yes	Count	45	39	84
	%	42.1%	33.9%	37.8%
No	Count	62	76	138
	%	57.9%	66.1%	62.2%
Total	Count	107	115	222
		Pearson Chi_Square = 1.563, sig. = .211		

7.10 Univariate Results for Dependent Variables

The dependent variables for this study are measures related to appropriation of privacy management. There are three faithful appropriation moves (Use, Familiarity, and Restricted Scope), two unfaithful moves (Rejection and One Sided Profile Browsing), one measure of Faithfulness, and one measure of Distrust in other members. In the next sections, the results for the questions that make up these constructs will be presented.

7.10.1 Univariate Results for Use Appropriation Move

Table 7.6 presents a summary of responses for the Use appropriation move. The Use appropriation move includes measures for the level of actual use of privacy management features.

Looking at the means for the measures, the responses show a lukewarm response to the use of privacy management, all around the midpoint of 4. Although there is no significant difference found when comparing MySpace members to Facebook members, there is a pronounced inverted distribution for MySpace members. If you look at Use1, for example, the distribution draws a U shape, with the low point being the mid value of 4 (7 responses), versus 28 for option 1 (do not use) and 19 for option 7 (highest option for

use). You can see a similar pattern for Use3. It seems that MySpace members either love or hate the privacy management, with little middle ground. The same pattern can be found in the Facebook responses, but not to the same extreme level.

Table 7.6 Summary of Responses for Use Appropriation Move

Label	(SD to SA)	1	2	3	4	5	6	7
Use1	In order to control who can contact me using [name of social networking site] I have adjusted my privacy settings. Mean = 3.90, S.D. = 2.237							
	Facebook	19	15	8	13	15	16	20
	MySpace	28	20	13	7	8	19	19
Use2	I have modified the privacy settings for my profile on [name of social networking site]. Mean = 4.52, S.D. = 2.217							
	Facebook	13	13	7	9	14	16	32
	MySpace	20	14	6	11	17	18	28
Use3	I have adapted the privacy settings to control who can view my profile on [name of social networking site]. Mean = 4.0, S.D. = 2.293							
	Facebook	17	14	9	10	15	20	20
	MySpace	35	14	6	8	11	19	21
Use4	I have personalized my privacy settings on [name of social networking site]. Mean = 4.59, S.D. = 2.060							
	Facebook	12	9	6	12	16	22	29
	MySpace	14	15	11	12	20	21	21

7.10.2 Univariate Results for Familiarity Appropriation Move

The Familiarity appropriation move is a measure of the extent to which members say they have knowledge of privacy management features. Table 7.7 summarizes the responses for the measures for this construct.

Table 7.7 Summary of Results for Familiarity Appropriation Move

Label	(SD to SA)	1	2	3	4	5	6	7
Fam1	I am comfortable with my ability to adjust my privacy settings. Mean = 5.51, S.D. = 1.559							
	Facebook** Mean = 5.19, S.D. = 1.666	4	5	9	14	20	27	28
	MySpace** Mean = 5.82, S.D. = 1.393	2	1	5	12	17	29	49
Fam2	I am confident that I know how to control who is able to see my profile on [name of social networking site]. Mean = 4.99, S.D. = 1.829							
	Facebook Mean = 4.79, S.D. = 1.744	4	12	8	16	25	20	21
	MySpace Mean = 5.17, S.D. = 1.894	11	4	5	13	13	36	31
Fam3	I am familiar with my privacy settings on [name of social networking site]. Mean = 4.98, S.D. = 1.751							
	Facebook* Mean = 4.71, S.D. = 1.846	9	8	10	14	19	29	17
	MySpace* Mean = 5.23, S.D. = 1.628	3	7	8	15	22	30	30
Fam4	When I need to modify my privacy settings for [name of social networking site], I am able to do it. Mean = 5.66, S.D. = 1.410							
	Facebook Mean = 5.49, S.D. = 1.408	2	1	6	16	20	30	30
	MySpace Mean = 5.83, S.D. = 1.397	2	4	1	8	23	29	48
	* - $p < .05$, ** - $p < .01$							

The results are divided into responses for Facebook and MySpace. Overall, the means for the Familiarity measures are at least a full point higher than the means for the Use measures. This is logical, because you would expect more subjects would say they were familiar with a certain functionality compared to those who actually use it. The distribution for all the measures is skewed to the high end, with only a handful of subjects selecting the low end options (strongly disagree).

There are significant differences between Facebook and MySpace members for two of the items, Fam1 and Fam3. What is surprising is that difference is in the opposite

of the expected direction. In other words, instead of a higher level of Familiarity in the site with higher appropriation support, it is MySpace that has a higher level of Familiarity, despite a lower level of appropriation support. A more detailed analysis of the implications of these results will be discussed in Chapter Nine.

Table 7.8 Summary of Results for Restricted Scope Appropriation Move

Label	(SD to SA)	1	2	3	4	5	6	7
Scope1	I use [name of social networking site] only to contact people I see in person on a regular basis. Mean = 3.77, S.D. = 1.953							
	Facebook	14	19	23	18	7	15	11
	MySpace	20	17	15	15	17	19	12
Scope2	I don't use [name of social networking site] to make contact with people whom I've never heard of. Mean = 5.05, S.D. = 2.100							
	Facebook* Mean = 5.42, S.D. = 1.948	7	6	8	10	7	21	48
	MySpace* Mean = 4.71, S.D. = 2.186	11	13	17	10	8	14	40
Scope3	I never accept friend requests from people I have not met in person. Mean = 4.65, S.D. = 2.023							
	Facebook	8	16	16	9	10	21	27
	MySpace	10	13	10	9	22	24	26
Scope4	When using [name of social networking site] I ignore contact from people whom I have not met in person. Mean = 4.52, S.D. = 1.944							
	Facebook	5	14	18	9	14	24	22
	MySpace	11	18	12	15	17	14	28
* - $p < .05$, ** - $p < .01$								

7.10.3 Univariate Results for Restricted Scope Appropriation Move

The Restricted Scope move is a measure of the extent to which members of a social networking site make a conscious effort to restrict the scope of their online social network while participating in social networking sites. Table 7.8 presents a summary of the responses to the measures for this construct.

The results for the measures for the Restricted Scope appropriation move show a greater level of variance compared to the Use and Familiarity move. For example, the mean for Scope1 is below the midpoint (3.77), which shows that most responses indicate that subjects use social networking sites to interact with people outside their immediate social circle. The next question, Scope2, has the highest mean of the four, and there is a significant difference in the responses of Facebook subjects versus MySpace subjects. Facebook subjects are significantly more likely to refrain from contacting strangers compared to MySpace members, although if you look at the distribution, the highest choice for both groups is number 7, strongly agree (48 in Facebook and 40 in MySpace). As with the question Use1, the Scope2 responses for MySpace subjects tend towards both extremes (i.e., 1 and 7) and avoid the mid-point.

7.10.4 Univariate Results for Rejection Appropriation Move

The Rejection appropriation move is a measure of to what extent members indicate they do not use or take the time to engage with privacy management features on social networking sites. It is an example of an unfaithful appropriation move, because it indicates the member is not engaged with appropriating the features. The summaries for these Rejection measures are presented in Table 7.9.

The results for the Rejection appropriation move show a marked skew to the low end (towards Strongly Disagree). For example, the mean for the responses for Reject4 is only 2.35, and only 1 Facebook and 3 MySpace subjects selected the highest option of 7 (Strongly Agree). Reject3 has a slightly different pattern, and also the results are significantly higher for MySpace rather than Facebook subjects. For Reject1, Reject2, and Reject4, the mode (most popular response) is 1 for both populations. But for Reject2,

the mode is number 7 for MySpace subjects, although the next highest response is number 1, the opposite end of the scale. This continues the pattern found in other appropriation moves of results for MySpace subjects being skewed to both extremes, with much fewer responses in the middle.

Table 7.9 Summary of Results for Rejection Appropriation Move

Label	(SD to SA)	1	2	3	4	5	6	7
Reject1	I don't know what my privacy settings are on [name of social networking site]. Mean = 2.81, S.D. = 1.996							
	Facebook	35	24	10	8	14	6	10
	MySpace	51	20	9	8	17	2	8
Reject2	I don't bother to look at the privacy settings for my profile on [name of social networking site]. Mean = 3.19, S.D. = 2.093							
	Facebook	27	27	9	11	9	12	12
	MySpace	37	22	12	13	8	11	11
Reject3	I don't use the privacy settings to control who can access my profile. Mean = 3.60, S.D. = 2.251							
	Facebook** Mean = 3.13, S.D. = 1.967	31	19	16	11	15	6	9
	MySpace** Mean = 4.03, S.D. = 2.413	27	15	14	7	7	13	32
Reject4	Adjusting the privacy settings for [name of social networking site] is a waste of time. Mean = 2.35, S.D. = 1.468							
	Facebook	43	28	16	10	7	2	1
	MySpace	37	36	13	18	2	4	3
* - $p < .05$, ** - $p < .01$								

7.10.5 Univariate Results for One Sided Profile Browsing

One Sided Profile Browsing is an appropriation move that combines two perspectives on profile viewing history. One perspective is whether the subject would like to see a list of who has viewed their own profile. The second perspective is whether the subject would be willing to make public their own profile viewing history. So the issue is the dialectic between knowing something about other peoples' behavior and restricting knowledge about one's own behavior. If the subject indicates they have a strong interest in seeing

who has viewed their profile while at the same time restricting others from being able to see when they view a profile, then this is a case of One Sided Profile Browsing. Because it is a representation of strong self interest over fair access for all, then this is an example of an unfaithful appropriation move (labeled as a paradox in the terminology of Adaptive Structuration Theory). Table 7.10 summarizes the responses for the two questions that are combined to determine One Sided Profile Browsing.

Table 7.10 Summary of Results for One Sided Profile Browsing

Label	(SD to SA)	1	2	3	4	5	6	7
OneSided1	I would like to know who has viewed my profile on [name of social networking site]. Mean = 5.35, S.D. = 1.852							
	Facebook	7	7	7	12	19	20	35
	MySpace	8	2	3	17	14	16	54
OneSided2	I would not like other people on [name of social networking site] to know whether I viewed their profile. Mean = 4.54, S.D. = 1.936							
	Facebook	5	8	17	22	7	14	32
	MySpace	13	10	11	36	6	17	22

There is no significant difference found in the answers given by Facebook versus MySpace subjects. The results for the question OneSided1 show a marked skew to the high end, indicating there is a strong interest in learning who has viewed one's profile. This is certainly consistent with Goffman's work on presentation management, which is an intense analysis of the dialogue that takes place between an individual (the performer) while engaging in social interaction (with their audience). Goffman describes a strong human instinct to know how one's performance is being viewed by others (Goffman, 1959).

The question OneSided2 has a different distribution, still skewed to the high end but with a sizable number of subjects right in the middle (22 Facebook and 36 MySpace).

The skew to the high end is a little bit stronger for Facebook subjects compared to MySpace subjects.

In order to determine the One Sided Profile Browsing condition, the results of these two questions are compared in a cross tabulation, to see how many subjects answer strongly positive to both questions. The results of that cross tabulation are presented in Table 7.11.

Table 7.11 Cross Tabulation To Determine One Sided Profile Browsing

		I would not like other people on [name of social networking site] to know whether I viewed their profile.													
		FB	MY	FB	MY	FB	MY	FB	MY	FB	MY	FB	MY	FB	MY
SD to SA		1		2		3		4		5		6		7	
I would like to know who has viewed my profile on [name of social networking site].	1	0	2	0	0	0	1	1	3	1	0	2	1	2	1
	2	0	0	1	1	1	0	1	0	0	0	1	0	3	1
	3	0	1	1	0	2	0	1	0	0	0	1	1	2	1
	4	0	1	1	2	1	1	4	9	0	1	2	0	4	3
	5	3	1	1	0	2	2	4	4	4	1	2	6	2	0
	6	0	2	2	2	7	3	7	6	2	2	1	0	1	1
	7	2	6	2	5	4	4	4	14	0	2	5	9	18	14

The cross tabulation shows that 70 subjects (35 Facebook and 35 MySpace) match the One Sided Profile Browsing Condition, by answering 5 or above to both questions. This represents about 32% of the subjects (just under one in three). Notice also that the highest values in all the cells are seven for both questions, answers given by 18 Facebook and 14 MySpace subjects. This represents about 14% of the subjects (about one out of seven). In contrast, only 10 subjects answered three or below to both questions, about 4% of the subjects.

7.10.6 Univariate Results for Distrust in Other Members

Four measures were included in the survey that measures the level of distrust the subjects express as to the behavior of other members of the site. The results for these four measures are summarized in Table 7.12.

Table 7.12 Summary of Responses for Distrust Measures

Label	(SD to SA)	1	2	3	4	5	6	7
Distrust1	I don't believe most of the information people put on their profiles on [name of social networking site]. Mean = 3.89, S.D. = 1.620							
	Facebook*** Mean = 3.37, S.D. = 1.557	11	24	25	24	11	8	4
	MySpace*** Mean = 4.38, S.D. = 1.531	3	10	19	30	26	13	13
Distrust2	There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy. Mean = 5.22, S.D. = 1.763							
	Facebook*** Mean = 4.38, S.D. = 1.781	4	15	13	31	11	12	20
	MySpace*** Mean = 5.99, S.D. = 1.347	3	0	0	15	14	25	58
Distrust3	I believe most of the profiles I view on [name of social networking site] are exaggerated to make the person look more appealing. Mean = 5.16, S.D. = 1.476							
	Facebook*** Mean = 4.69, S.D. = 1.508	2	5	17	25	23	19	15
	MySpace*** Mean = 5.59, S.D. = 1.307	0	3	6	11	29	29	35
Distrust4	I have been contacted by people through [name of social networking site] whom I did not trust. Mean = 4.35, S.D. = 2.148							
	Facebook*** Mean = 3.19, S.D. = 1.835	21	28	14	16	10	10	6
	MySpace*** Mean = 5.42, S.D. = 1.835	6	5	11	10	11	25	47
	* - $p < .05$, ** - $p < .01$, *** - $p < .001$							

For the Distrust measures, the differences between Facebook and MySpace responses are quite striking. MySpace subjects report a highly significant, substantially greater amount of distrust towards other members of the site. The MySpace scores are at least a full point higher for three out of four scores, and for Distrust4 the difference is

over two full points. The answers from MySpace subjects are quite skewed to the high end. More than half of the MySpace responses (58 out of 115) for Distrust2 are the highest value of seven. For Distrust4, the Facebook answers skew towards the low end, and the MySpace answers skew towards the high end.

Table 7.13 Summary of Results for Unfaithfulness

Label	(SD to SA)	1	2	3	4	5	6	7
Faith1	I probably use the privacy settings for [name of social networking site] improperly. Mean = 2.90, S.D. = 1.808							
	Facebook	28	23	15	15	13	5	8
	MySpace	38	25	14	22	7	3	6
Faith2	I failed to use the privacy settings of [name of social networking site] as they should be used. Mean = 2.67, S.D. = 1.714							
	Facebook	28	31	15	15	6	7	5
	MySpace	45	25	9	18	9	6	2
Faith3	I did not use the privacy settings in [name of social networking site] in the most appropriate fashion. Mean = 3.06, S.D. = 1.726							
	Facebook	22	27	14	20	12	6	6
	MySpace	27	29	15	21	12	8	3
Faith4	The founders of [name of social networking site] would disagree with how I use the privacy settings. Mean = 2.64, S.D. = 1.500							
	Facebook	32	22	8	35	5	3	2
	MySpace	41	23	9	39	1	0	2
Faith5	The original founders of [name of social networking site] would view my use of the privacy settings as inappropriate. Mean = 2.68, S.D. = 1.613							
	Facebook	24	29	13	26	3	5	6
	MySpace	44	23	14	27	1	3	2

7.10.7 Univariate Results for Unfaithfulness Measures

The measures for unfaithfulness are adaptations of a published scale (Chin et al., 1997). All the questions are worded as negatives, so that lower values indicate faithfulness, and the higher values indicate unfaithfulness. The results are summarized in Table 7.13.

The responses to these questions skew very strongly to the low end, which indicates a bias towards faithfulness. Four out of the five means are below 3, and the fifth is just a little bit above three. In contrast to the results on Distrust, both the Facebook and MySpace results skew in the same direction. There are no significant differences found in the answers given by Facebook subjects versus MySpace subjects.

7.10.8 Univariate Results for Value of Privacy Measure

As an additional measure of subjects' attitudes towards privacy, a question related to the importance a subject places on protecting privacy was included in this study. The text of the question is as follows: "Please indicate your opinion as to the overall value you place on the importance of protecting your privacy on [name of social networking site]." It was measured as a seven point semantic differential scale, anchored by "Not valuable or important," (1), to "Extremely valuable and important," (7). The results for this question are summarized in Table 7.14.

Table 7.14 Summary of Responses for Measure of Value in Privacy

		1	2	3	4	5	6	7
Please indicate your opinion as to the overall value you place on the importance of protecting your privacy on [name of social networking site]. Mean = 5.53, S.D. = 1.451								
	Facebook* Mean = 5.77, S.D. = 1.265	0	1	6	10	22	26	40
	MySpace* Mean = 5.30, S.D. = 1.574	2	6	7	18	23	25	34
“Not valuable or important,” (1), to “Extremely valuable and important,” (7)								
* - $p < .05$, ** - $p < .01$								

The responses for this question skew towards the high end, indicating the majority of the subjects consider it important to protect their privacy on these sites. Notice only two MySpace subjects and zero (0) Facebook subjects selected (1), strongly disagree. The mean for all responses is well above five, and Facebook subjects place a significantly higher level of importance on privacy. Several subjects in their free form comments compared privacy issues on Facebook versus MySpace:

- *“I have only recently been using Facebook regularly. I have been using MySpace for about 3 years and my profile was hacked twice. Because of this I keep very little information on MySpace. Facebook seems to be much more acceptable and has less stigma than MySpace. People who refused to use MySpace will readily use Facebook.”*
- *“I was concerned with privacy not on Facebook, but on MySpace. On MySpace I always got spam messages from people I didn't even know, so I changed my privacy settings, so letting only a few people view my MySpace page. I don't really get any spam message from Facebook. And if I did I would change my privacy on Facebook.”*
- *“Sites like MySpace are high-profile with little expenditure on security. Any information submitted to it should be considered public regardless of your privacy settings. The controls on the site are ersatz: they've probably been cracked a million times, and MySpace has sold your information to every [language deleted] on the Internet.”*
- *“I enjoy Facebook, I think that it is a ‘safer’ site in comparison to MySpace.”*

Table 7.15 Summary of Results for Trust in Site

Label	SD to SA	1	2	3	4	5	6	7
Trust1	I trust that [name of social networking site] will not use my personal information for any other purpose. Mean = 4.14, S.D. = 1.962							
	Facebook	10	16	10	19	11	26	14
	MySpace	20	9	16	23	18	13	16
Trust2	I feel that the privacy of my personal information is protected by [name of social networking site]. Mean = 3.95, S.D. = 1.663							
	Facebook* Mean = 4.23, S.D. = 1.564	3	16	15	22	24	19	6
	MySpace* Mean = 3.69, S.D. = 1.714	18	12	21	24	20	17	3
	* - $p < .05$, ** - $p < .01$, *** - $p < .001$							

7.10.9 Univariate Results for Trust in Site

Two questions were included that relate to members' degree of trust in the site. These two questions have been used before in previous pilot studies, and were found to show a higher level of trust in Facebook versus MySpace. The results for these two questions are summarized in Table 7.15. The answers from this study also indicate a higher level of trust in Facebook. Results from the second question, "I feel that the privacy of my personal information is protected by [name of social networking site]," is significant, with a mean of 4.23 for Facebook versus a mean of 3.69 for MySpace ($p < .05$).

CHAPTER 8

SUMMARY OF QUALITATIVE DATA

The survey included open ended questions designed to gather more qualitative information on use. A summary of responses is included below.

8.1 Benefits of Social Networking Use

Subjects were asked the following question: “What is the most positive benefit you get from your use of [name of social networking site]? A total of 207 out of 222 subjects wrote in answers to this question. Members are very enthusiastic about their use of social networking sites. This is apparent both from how often they use them, and also by the comments they make.

When asked to describe the benefits of using social networking sites, many subjects talked about using these sites to stay connected to old friends that may be hard to keep up with or may be far away. They use these sites to quickly and easily manage and maintain contact with friends. Here is a selection of responses:

- *“Networking with long lost friends & family from the past that I have lost touch with.”*
- *“Contacting close/long distant friends.”*
- *“Chatting with friends that I haven’t seen in a while.”*
- *“Being able to keep in contact with people whom I normally do not speak to via telephone.”*
- *“Easy to keep in touch with people I don't get a chance to see often.”*
- *“Being able to contact friends easily who are far away at college.”*

- *"Being able to stay in contact with my friend, in Cuba. He's in the Navy and contacting him by phone is a bit pricey."*
- *"Staying in touch with friends and family."*
- *"I would have to say that the most positive benefit is meeting people in my country that I fell out of touch with even family members and for me that's something positive."*

Subjects described how these sites helped them maintain social contact in the face of other demands:

- *"Staying in contact with people I do not get to see on a regular basis as a result of being so busy."*
- *"In some situations it is the only way to interact with my kids who are in their 20's."*
- *"I am currently in the military, so I move/travel a lot. I left a lot of friends back at home and it allows them to track my progress, message me, and know when I am coming home. Also, I find that people from elementary school are coming out of the woodworks now and it allows for a very comfortable, low stress way of getting back in touch with long lost friends or flames."*
- *"You get to stay more regularly informed of your friends."*
- *"Nice to keep in touch (or at least know what's going on) with my friends from outside my department (which can be hard because my major is time-consuming)."*
- *"You are able to keep contact with friends and relatives that are far away, very easily."*
- *"Let's me talk to people I went to school/worked with but don't see anymore. Once you finish high school everybody goes in different directions so it makes it easier to find your friends and keep contact."*
- *"I am able to keep in touch with friends despite a busy schedule."*

They are also described as being useful for meeting new people and dating:

- *"Social Networking and meeting new friends !!"*
- *"Good network for my social and romantic life."*

- *"To see old friends and pretend to make new ones lol [abbreviation for laugh out loud]."*
- *"Meeting new friends, catching up with old friends I haven't seen in a while, and networking."*

The self-publishing features of these sites are also commented on:

- *"Sharing pictures with friends, meeting old buddies."*
- *"Social networking, ego boost from picture comments."*
- *"I see what my friends are up to by their pictures."*
- *"As a business owner, to show myself out there."*
- *"Self-expression."*
- *"It's like having a personal web page only much less work. Sharing photos, reconnecting with real-life friends, finding new contacts, finding info on all sorts of stuff-bands, retailers, websites, eBay sellers, etc."*

The comments were overwhelmingly positive. Only two subjects included negative comments in this section, answering that they could think of *"Nothing really"* and *"Nothing."* The next question collected answers as to concerns over use.

8.2 Greatest Concern With Regard to Use

Subjects were asked the following question: "What is your greatest concern regarding the [name of social networking site]? A total of 200 out of 222 subjects responded to this question.

Many were concerned about children's use of these sites:

- *"I am ok with the use of MySpace for me, but I am concerned with my younger cousins (13-15) using MySpace, especially with the disturbing people out there. There should be a parent profile that rules over the children's profile to enable monitoring (like Webkin's)."*
- *"Children that are too young getting on it."*

- *“The safety of women and children.”*
- *“Vulnerability of KIDS.”*
- *“Underage kids should be protected and supervised by parents.”*
- *“Young children being exploited by internet stalkers.”*

Some commented on disturbing behavior by other members of the site:

- *“I get lots of messages from what I would consider “creepy” people. Sometimes old men.”*
- *“Some wacko will try to find my children.”*
- *“Most likely stalkers and obsessive people bent on harassment.”*
- *“Personal information used inappropriately and drama coming from those interactions.”*
- *“Weird people online.”*
- *“Online stalkers, etc.”*
- *“People that use MySpace for personal gain or for criminal purposes.”*
- *“Creepy people.”*

Many subjects listed very general concerns, such as privacy or identity theft. Some also expressed concern that future employers would view their profile and use it against them. One subject had a concern that *“a lot of precious time is taken!”* 17 subjects specifically said they had no concerns *“None,” “No ‘great’ concerns.”* Some of the answers were overly-dramatic: *“As a 24 year old guy with no children, I don’t have to be concerned about sexual predators or rapists or anything like that. I know not to make my social security number or credit card numbers available to anyone. I suppose I have no concerns.”*

8.3 Effectiveness of Privacy Management

Subjects were asked the following question: "Please comment on how effective you think the privacy protection is for [name of social networking site]? A total of 202 out of 222 subjects wrote in answers to this question.

Many subjects described the privacy management as effective:

- *"It is fairly effective if you use the privacy settings right. But then again the company has access to whatever you put up there so ultimately it is on you on how much people know about you."*
- *"I use two privacy settings. All comments must be approved by me before they are posted to my page, and I do not accept friend requests from bands. Both of these settings are very effective in decreasing my annoyance level while using MySpace."*
- *"I think the privacy protection is sufficient, and will do well in protecting you if you know how to use it."*
- *"I think the privacy protection is fine. You basically get to choose what information can be viewed by others. As for the registration information. You can only trust and have faith that Facebook is not giving it out to anyone. I think they can be trusted for that."*
- *"I think that the privacy settings are pretty good. If you don't want to show up in search results or have your name displayed, that is an option. Also I like how you can adjust the settings so that only friends can view your profile."*
- *"I think it is effective, but getting several random comments from random people has turned me away from MySpace to Facebook."*
- *"I think it is effective as long as the person sets his/her profile to private, understands what information to put/not put in their profiles and also does not talk or accept people he/she does not know already."*
- *"I think it's adequate. If you set your profile to private, there's little anyone can do to view your info or pictures."*
- *"As long as people are smart about it, it's quite effective."*
- *"6 on a scale of 1-10."*
- *"I think it is pretty effective only because I have not had any problems yet."*

Quite a few thought it was not all that effective:

- *“Not very I suspect it’s a bit of a paper tiger.”*
- *“Not at all, especially with all those applications from third parties everywhere now. They seem to have no qualms giving out private info, not just from Facebook but from other websites as well! (such as the ridiculous ‘recent purchase’ instant update feature gizmo.)”*
- *“It is only effective to those who view your page and aren’t very computer savvy.”*
- *“I really don’t trust the privacy protection in MySpace, hence I don’t disclose any information I don’t want public.”*
- *“I think Facebook should and can do more in that area.”*

And a good number said they had no interest or didn’t really care:

- *“I tend not to think of it much because I don’t really put any ‘private’ information on my page.”*
- *“I have no idea.”*
- *“Don’t care. Don’t have much to hide.”*
- *“Don’t really care - I haven’t had any problems with privacy on Facebook. Plus, I don’t have any sensitive information on my profile.”*
- *“Don’t really matter...it’s the user who has to know what to put and what not to put and how to put it.”*

There were no really enthusiastic endorsements of the privacy management features. Subjects in general thought Facebook did a better job with privacy compared to MySpace. The general consensus was that the privacy settings were “ok” or “adequate.”

8.4 Reports of Personal Experiences With Privacy Issues

An important question with regard to understanding the use of privacy management features is related to subjects’ previous encounters with privacy issues. To what extent

does a subject's prior experience with privacy issues influence their use of privacy management features? In order to answer this, several questions were included in the survey related to whether subjects had a personal experience with respect to privacy problems on these sites. The results of those questions are summarized in Table 8.1.

Table 8.1 Summary of Prior Issues With Privacy

		Facebook	MySpace
Over the past year did you experience any incidents that led you to be concerned about privacy when using [name of social networking site]?			
	Yes	16	26
	No	91	89
(only those who answered "yes" were asked the next two questions).			
Did you review your privacy settings after this incident?			
	Yes	8	12
	No	8	14
Did you make any adjustments or changes to your privacy settings after this incident?			
	Yes	8	11
	No	8	15

The data collected by these questions show that nearly one in five (42 out of 222) subjects reported a problem with privacy over the past year. This number includes 16 Facebook subjects (15.6% of all Facebook subjects) and 26 MySpace subjects (22.6% of all MySpace subjects). Although more MySpace subjects reported incidents, the difference is not significant. Only 20 out of the 42 subjects reported they reviewed their privacy settings after this incident, and only 19 out of 42 reported making adjustments in their privacy settings. It is certainly interesting that less than half of subjects with a direct personal experience with a privacy incident report they reviewed their privacy settings in response. The nature of this low response deserves some closer attention, and will be discussed with respect to overall conclusions for this research.

Although not specifically asked to provide details, many subjects described these incidents:

- *“Constant spam from adult content type accounts has basically driven me away from MySpace and more towards the use of Facebook.”*
- *“I found out my Facebook page was on a suspected sex offender's computer in another state last year (along with many other girls) which made me more cautious of what personal content I put of Facebook. Also, I don't think (this may be ignorance) you can remove your email from your profile page.”*
- *“My 17 year old cousin's MySpace account was hacked into and was filled with pornographic images, comments, and videos.”*
- *“My profile was hacked by the ‘Create Your Own South Park Character’ website. While using this site, I gave up my MySpace password to ‘automatically post to profile.’ Once the South Park site had my password, it was used it to leave many, many advertisements for their site in all my friend's comments. I changed my password & the hacking stopped. Lesson learned.”*
- *“Not really except a person whom I was stalked by before tried to contact me through Facebook again which was scary but that is about it.”*
- *“Not with Facebook, but someone I helped at work tracked me down on MySpace once. That was pretty creepy.”*
- *“Random people that I don't know would message me asking me very personal questions that I did not feel comfortable answering.”*
- *“Yeah the girl who committed suicide because of online bullying. And I knew someone who met up with people she met online, it made me very uncomfortable.”*
- *“Yes, but I've only had one person contact me that I did not know. And rumors just started this month about a guy that apparently hacks into your profile through friend's pages. I find it highly unlikely, and it's nice that after this long on Facebook, it's stayed a secure place. It's so refreshing after MySpace has just turned into a complete spamfest.”*

It is important to note that these subjects were very generous in their willingness to share their thoughts about their use of these sites, as well as their concerns and fears. The subjects are very enthusiastic users, but do recognize there are risks to this use.

Looking at both the qualitative responses and the univariate analysis, the results presented thus far show an interesting but somewhat confusing picture of security,

privacy, distrust and privacy management use on these two sites. The next step in data analysis is to combine variables into summative scales and perform reliability and validity tests for the conditions required for ANOVA and MANOVA analysis. Those results will be presented in the next chapter.

CHAPTER 9

RELIABILITY TESTS AND FACTOR ANALYSIS

9.1 Validity and Reliability

An important part of any research design addresses the validity and reliability of the data collected. If the data collected are not reliable or valid, then no reasonable conclusions can be drawn from the study.

Reliability is the extent to which a measure is expected to yield the same result even if it is administered at different times in different circumstances. It is an indication of a measure's stability or consistency (Rosenthal & Rosnow, 1991). If a measure is a true indicator of a construct, then the results obtained must exhibit a consistency that persists.

The validity of a measure is a determination of whether the measure actually measures what is claimed, and that it is logical to draw conclusions from the results of those measures (Rosenthal & Rosnow, 1991). Problems with validity usually take the form of biases or specific events that call into question whether results are meaningful.

The subjects for this study were selected from a random sample. This can help reduce the risk of selection bias that can come from using a convenience sample. The Facebook and MySpace subjects were selected from the same general population, the NJIT community. This was done to reduce to risk of a bias being introduced by some unknown demographic variable.

Convergent validity is the degree to which two measures of the same construct are correlated. Discriminant validity is an indication of whether measures of different constructs do not show a correlation. Because the appropriation moves measures are

new, it not quite clear as of yet which of these measures will be convergent, and which are expected to be discriminant. For example there are two closely related moves, actual use of privacy management, and familiarity. Should these two measures exhibit discriminant or convergent behavior? This can only be answered by collecting and analyzing results.

The data collected for this study were examined using a process for multi-variate data analysis as recommended by (Hair et al., 2006). These authors recommend the following steps be taken for a multivariate data analysis:

- Examine the data set for missing data and assess its potential impact. As described in Section 7.6, the amount of missing data is minimal and is not an impediment to further analysis.
- Examine the data for outliers and assess their impact. The primary outliers are those subjects whose age lies beyond the normal distribution for the other subjects. In order to determine the impact of these outliers tests will be conducted to control for age.
- Test for reliability (this was done using Cronbach's alpha and factor analysis)
- Test for normality by applying tests for Skewness (peak of curve is too far to the left or right) and Kurtosis (peak is too flat or too extreme). Values beyond ± 1 for both tests indicate that a measure needs to be transformed in order to continue multi-variate analysis.
- Homoscedasticity – this characteristic refers to whether the dependent variable has equal levels of variance across the range of predictor variables. In other words, the dispersion of the dependent variables should be relatively similar for all possible values of the predictor variable. If the dispersion is not equal, that relationship is said to be heteroscedastic.

• The Levene test was applied to test for univariate Homoscedasticity, and the Box-M test was applied to determine multi-variate Homoscedasticity.

9.2 Tests of Reliability and Normal Distribution

Six dependent constructs and one independent construct were tested to determine their reliability and compliance with the normal distribution requirement of ANOVA based multi-variate analysis. The results are summarized in Table 9.1. The following were found to have acceptable level for Cronbach's alpha (.7 or above): the Use appropriation move, the Familiarity appropriation move, the Rejection appropriation move, Concern for Internet privacy, and Faithfulness. Two had alpha levels below .7: Restricted Scope and Distrust. By dropping one measure from the Restricted Scope construct, reliability improved to .778. The reliability could not be improved for the Distrust construct by dropping any measures. The decision was made to retain this construct with all four items and a Cronbach's alpha of .665 because a value of .6 or above is acceptable for an exploratory construct (Nunnally, 1967).

After reliability analysis the remaining indicators were added together to form a summative scale for each of these constructs. Statistical tests were carried out to determine whether these summative scales exhibited a normal distribution. Five out of seven had an acceptable normal distribution, but two did not. These two were the Use appropriation move and the Restricted Scope appropriation move. Following recommendations from (Hair et al., 2006), these two scales were transformed to improve the shape of the distribution. The Use appropriation move was transformed using the LN function (natural log), and Restricted Scope was transformed using Square Root. Both transformed scales have an acceptable normal distribution. The next step to be described is factor analysis to confirm that the measures load as expected on the appropriation construct. This will be described in the next section.

Table 9.1 Summary of Reliability Tests for Research Constructs

Construct	Cronbach's alpha	Normality	Adjustment
Use appropriation move (range 4 to 28)	.907	Kurtosis = -1.323 (not acceptable)	Transform using Ln (natural Log)
Familiarity appropriation move (range 4 to 28)	.771	acceptable	
Restricted Scope appropriation move (range 3 to 21)	.690	Kurtosis = -1.043, (not acceptable) Skewness = -.305 (acceptable)	Scope1 dropped to improve Cronbach's alpha to .778 Transformed with square root to improve Kurtosis to -.438
Rejection appropriation move (range 4 to 28)	.701	acceptable	
Distrust of other members (range 4 to 28)	.665	acceptable	Not able to improve reliability by dropping measures Will keep 4 items, this level of reliability acceptable for new measures (Nunnally, 1967)
Concern for Internet privacy	.862	acceptable	
Faithfulness (range 5 to 35)	.751	acceptable	

9.3 Factor Analysis and Identification of Factors

According to (Hair et al., 2006), the basic assumptions of factor analysis are that an underlying structure does indeed exist, and that there is a minimum sample size of 50 subjects. Both assumptions are met for this data. The assumption of underlying structure is that these variables form measures that capture appropriation moves, as described in

the research model (see Chapter 5). Secondly there are more than enough observations, with 222 total subjects.

Table 9.2 Initial Factor Loading for Research Measures

Indicator	1	2	3	4	5	6	7
Use 4	0.769	-0.028	0.177	0.144	0.208	0.007	-0.065
Use 2	0.762	-0.112	0.255	0.122	0.229	0.213	0.075
Use 3	0.722	-0.137	0.396	0.120	0.157	0.315	0.053
Faithful 2	-0.715	0.265	0.185	0.178	0.020	0.200	0.270
Rejection 3	-0.684	0.150	-0.444	-0.152	-0.116	-0.169	0.080
Use 1	0.677	-0.066	0.377	0.183	0.265	0.242	0.022
Rejection 2	-0.677	0.087	0.161	0.174	-0.008	0.100	0.361
Faithful 1	-0.672	0.314	0.312	0.075	0.016	0.253	0.146
Rejection 1	-0.646	0.182	0.197	-0.020	-0.010	0.196	0.166
Familiar4	0.603	-0.076	-0.332	0.020	-0.125	-0.166	0.400
Faithful 3	-0.569	0.361	0.119	0.177	-0.101	0.147	0.056
Rejection 4	-0.527	-0.039	-0.080	0.092	0.193	0.052	0.122
Familiar 1	0.476	-0.256	-0.269	0.005	0.024	-0.037	0.449
IPScale 2	0.458	0.649	-0.082	0.180	-0.248	0.021	0.038
IPScale 4	0.416	0.635	-0.103	0.143	-0.263	0.075	-0.004
IPScale 3	0.416	0.634	-0.234	0.083	-0.291	0.047	0.054
IPScale 1	0.475	0.590	0.088	0.045	-0.185	-0.053	-0.177
IPScale 5	0.422	0.549	0.014	0.099	-0.256	0.105	0.031
Distrust 2	0.048	0.296	-0.615	-0.048	0.288	0.009	-0.174
Distrust 4	0.115	0.209	-0.535	-0.063	0.441	-0.057	-0.016
Scope 2	0.096	0.260	0.442	-0.605	0.045	-0.119	-0.053
Scope 4	0.077	0.413	0.328	-0.595	0.233	-0.229	0.125
Scope 3	0.029	0.486	0.316	-0.573	0.229	-0.094	0.118
Faithful 4	-0.201	0.190	0.257	0.567	0.297	-0.477	-0.042
Distrust 3	0.021	0.433	-0.283	0.086	0.562	0.164	0.048
Distrust 1	-0.139	0.229	-0.394	-0.053	0.439	0.351	-0.029
Faithful 5	-0.127	0.308	0.293	0.501	0.284	-0.521	0.019
Familiar 2	0.527	-0.118	-0.112	-0.079	0.011	-0.183	0.573
Extraction Method: Principal Component Analysis.							
a	7 components extracted.						

When conducting a factor analysis, important issues to consider are the number of factors extracted, the percentage of variance explained. These are usually apparent in an initial, unrotated solution. Factor loadings of ± 0.30 to ± 0.80 are considered for initial

analysis. Factor loadings should be .50 or above for practical significance, and the goal is factor loadings of $\pm .70$.

Following this process as described in Hair et al. the measures for the seven constructs of interest were examined using Principal Component Analysis. Seven factors were identified, explaining 66.98% of the variance. Table 9.2 presents the initial unrotated factor solution.

The next step is to further clarify the factors by creating a rotated solution. The rotation method used for this study is the Equamax method. This method was found to return the best results for this data set. The Equamax attempts to both simplify the rows and the columns of the solution matrix.

By carrying out various rotation methods, the goal is to simplify the loadings so that each measure loads only on one factor. When a measure does load on more than one factor, it is said to be cross loading and is a candidate for deletion.

When looking at factor loadings, the goal is to identify factor loadings that are statistically significant. With a sample size of about 200 subjects (222), the significance level for factor loadings for this analysis is .40 (Hair et al., 2006).

Based on the criteria described above, Use1 and Familiar3 were dropped as split factors. The measures for the Rejection appropriation move did not load on one factor. Two loaded with three of the items for the Faithfulness construct. In addition the faithfulness construct loaded as two separate factors.

This leads to the rotated solution shown in Table 9.3. The factors were rotated using the Equamax rotation method, and the solution was found in six iterations.

Table 9.3 Rotated Factor Solution

Factor Label	Measure	1	2	3	4	5	6	7
Concern for Internet Privacy	IPScale 2	0.830	0.116	-0.031	0.127	0.067	0.085	0.070
	IPScale 3	0.819	-0.017	-0.070	0.156	0.029	0.159	-0.034
	IPScale 4	0.805	0.112	-0.008	0.070	0.048	0.114	0.009
	IPScale 5	0.726	0.144	-0.024	0.083	0.079	0.027	0.003
	IPScale 1	0.722	0.178	-0.215	-0.074	0.222	-0.005	0.093
Use approp. move	Use 3	0.109	0.866	-0.130	0.174	0.040	-0.107	-0.087
	Use 2	0.110	0.827	-0.215	0.238	0.039	-0.003	-0.043
	Rejection 3	-0.094	-0.805	0.214	-0.093	-0.042	0.184	-0.024
	Use 4	0.184	0.708	-0.364	0.198	0.052	0.031	0.090
Unfaithfulness	Faithful 2	-0.066	-0.237	0.799	-0.210	-0.001	0.036	0.167
	Faithful 1	-0.047	-0.155	0.737	-0.371	0.128	-0.027	0.107
	Rejection 2	-0.177	-0.239	0.714	-0.095	-0.056	-0.070	0.159
	Rejection 1	-0.111	-0.263	0.641	-0.232	0.093	-0.003	0.043
	Faithful 3	0.124	-0.236	0.589	-0.325	-0.014	0.013	0.130
Familiarity approp. move	Familiar 2	0.056	0.189	-0.083	0.798	0.097	-0.019	-0.030
	Familiar4	0.239	0.078	-0.283	0.722	-0.103	0.031	-0.094
	Familiar 1	-0.005	0.153	-0.177	0.678	-0.135	0.054	-0.138
Restricted Scope approp. move	Scope 4	0.056	-0.017	0.002	0.048	0.865	0.054	0.065
	Scope 3	0.110	0.036	0.127	-0.026	0.837	0.114	-0.008
	Scope 2	0.051	0.075	-0.060	-0.129	0.776	-0.173	-0.096
Distrust of other members	Distrust 3	0.121	0.096	0.124	0.001	0.069	0.743	0.163
	Distrust 1	-0.025	0.012	0.184	-0.095	-0.032	0.707	-0.137
	Distrust 4	0.026	-0.145	-0.192	0.186	0.019	0.688	0.056
	Distrust 2	0.167	-0.221	-0.213	-0.006	-0.055	0.676	-0.045
Faithful with system spirit	Faithful 5	0.078	0.004	0.087	-0.041	0.049	0.005	0.887
	Faithful 4	-0.018	0.006	0.093	-0.113	-0.085	0.014	0.868

The results of the factor analysis have led to a reconstruction of some of the constructs under measurement. The Rejection appropriation move is dropped, because its measures have loaded strongly on other constructs. For the Use appropriation move, one initial measure is dropped (Use1) and replaced with Rejection3, which will be reversed to make its scoring consistent with the other measures in the Use appropriation move. The Familiarity move and the Restricted Scope move now have three measures.

The Faithfulness measure has broken into two factors that will be considered separately. The first Faithfulness measure has the first three measures of Faithfulness, and the first two measures of the Rejection construct. The last two measures of the Faithfulness construct load as one factor. They also show an acceptable level of reliability (Cronbach's alpha = .759).

The five item Unfaithfulness construct is a measure of the subject's ignorance and/or lack of engagement with privacy management. It combines the answers to the following items:

- I failed to use the privacy settings of [name of social networking sites] as it should be used.
- I did not use the privacy settings in [name of social networking sites] in the most appropriate fashion.
- I probably use the privacy settings for [name of social networking sites] improperly.
- I don't know what my privacy settings are on [name of social networking site].
- I don't bother to look at the privacy settings for my profile on [name of social networking site].

A two item construct is included that measures the subject's perception of the overall "spirit" of the system design, using the term from Adaptive Structuration Theory.

It consists of the following two questions:

- The founders of [name of social networking sites] would disagree with how I use the privacy settings.
- The original founders of [name of social networking sites] would view my use of the privacy settings as inappropriate.

This leaves use with the following constructs made up of items that do not cross load and have a factor loading of $\pm .50$ or above:

- Concern for Internet Privacy – Independent variable (five items)
- Use appropriation move – Combines three items from the original Use construct with a reversed measure from the Rejection construct (four items)
- Unfaithfulness – the degree of ignorance or indifference with respect to privacy settings. This combines three items from the Faithfulness scale (Chin et al., 1997) and two items from the Rejection construct
- Familiarity appropriation move – the degree to which a subject is familiar with their privacy settings and how to manage them (three items)
- Restricted Scope appropriation move – the degree to which subjects manage their privacy by limiting the scope of their social network (three items)
- Distrust – the degree to which subjects express distrust with other members of the social networking site (four items)
- Faithfulness with System Spirit – these are two items from the original Faithfulness scale that load on another factor. These questions address the degree of faithfulness to the overall system spirit of each site (two items)

9.4 Evaluation of Hypotheses

The next step in the analysis is the consideration of the hypotheses using the most appropriate statistical method. In order to use ANOVA for analysis, the variables need to display homoscedasticity, or a consistent dispersion of variance throughout the range of values under test. This can be determined using Levene's test (Hair et al., 2006). If Levene's test is significant (i.e., $p < .05$), that means the variable does not meet the test for homoscedasticity. In those cases, other methods such as the T test (with no assumption of equal variances) or Chi-Square will be applied.

9.5 Main Effects

Table 9.4 Summary of Hypothesis Tests for H1

H1. Members of Facebook will have more faithful appropriation moves compared to members of MySpace.			
Dependent variable	Statistical test	Results	Conclusion
Use (transformed with Ln)	T test (equal variances not assumed)	T = -2.094, df = 211.762, sig. = .037	H1 is supported for Use appropriation move
Familiarity	ANOVA	F (1, 216) = 7.097, sig. = .008, R-squared = .032	Results are in the opposite of predicted direction, H1 is not supported for Familiarity appropriation move
Restricted Scope (transformed with square root)	ANOVA	F (1, 216) = 1.216, sig. = .271	H1 is not supported for Restricted Scope appropriation move
H1 is partially supported.			

H1: Members of Facebook will report higher levels of faithful appropriation moves compared to members of MySpace.

Partially supported.

H1a. Members of Facebook will report a higher level of Use appropriation moves compared to members of MySpace.

Supported (mean MySpace= 2.58, Facebook = 2.75), significant ($p < .05$)

H1b. Members of Facebook will report a higher level of Familiarity appropriation moves compared to members of MySpace.

Not supported, reverse effect is found (mean MySpace = 6.79, Facebook = 15.44), significant ($p < .01$).

H1c. Members of Facebook will report a higher level of Restricted Scope appropriation moves compared to members of MySpace.

Results are in the predicted direction (mean MySpace = 3.65, Facebook = 3.76), but not significant.

Table 9.5 Summary of Hypothesis Tests for H2

H2. Members of Facebook will have fewer ironic appropriation moves compared to members of MySpace.			
Dependent variable	Statistical test	Results	Conclusion
One Sided Profile Browsing, general condition	Chi-Square	Pearson Chi-Square = .712, df = 2, sig. = .712	H2 is not supported for One Sided Profile Browsing, general condition
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = .919, df = 2, sig. = .338	H2 is not supported for One Sided Profile Browsing, extreme condition
H2 is not supported for ironic appropriation moves.			

H2. Members of Facebook will have fewer ironic appropriation moves compared to members of MySpace.

Not supported.

H2a. Members of Facebook will be less likely to match One Sided Profile Browsing, general condition compared to members of MySpace.

Results are very slightly opposite of the expected direction (33% of Facebook match the condition versus 30.7% of MySpace), no significant differences found.

H2b. Members of Facebook will be less likely to match One Sided Profile Browsing, general condition compared to members of MySpace.

Results are opposite of expected direction (16.8% of Facebook match the condition versus 12.3% of MySpace), no significant differences found.

Table 9.6 Summary of Hypothesis Tests for H3

H3: Members of Facebook will express more positive perceptions of their appropriation and use of Facebook compared to members of MySpace.			
Dependent variable	Statistical test	Results	Conclusion
Faithful With System Spirit	ANOVA	Opposite results are supported (weakly). MySpace members report more faithful appropriation $F(1, 216) = 4.1632$, sig. = .038, R squared = .02	H3 is not supported for Faithful With System Spirit
Unfaithful (ignorance/lack of engagement with privacy settings)	ANOVA	$F(1, 216) = 1.562$, sig. = .213	H3 is not supported for Unfaithful (ignorance/lack of engagement with privacy settings)
H3 is not supported for either variable.			

H3. Members of Facebook will express more positive perceptions of their appropriation of Facebook compared to members of MySpace.

Not supported.

H3a. Members of Facebook will express a higher level of faithfulness with overall system spirit compared to members of MySpace.

Not supported. Results are opposite of the predicted direction, MySpace members report more faithful appropriation, (mean for MySpace = 4.94, Facebook = 5.70) and significant ($p < .05$).

H3b. Members of Facebook will express a lower level of unfaithfulness/ignorance of privacy settings compared to members of MySpace.

Not supported. Results are opposite of predicted direction (mean for MySpace = 13.97, Facebook = 15.34), not significant.

Table 9.7 Summary of Hypothesis Tests for H4

	H4. Members with high levels of Internet privacy concern will have more faithful appropriation moves compared to members with low levels of privacy concern.		
Dependent variable	Statistical test	Results	Conclusion
Use (transformed with Ln)	ANOVA	F (2, 213) = 5.660, sig. = .003, R squared = .051	H4 supported for Use appropriation move.
Familiar	Chi-Square	Pearson Chi-Square = 12.678, df = 4, sig. = .013	H4 supported for Familiar appropriation move.
Restricted Scope (transformed with square root)	ANOVA	F (2, 217) = 3.766, sig. = .025, R squared = .032	H4 supported for Scope appropriation move.
H4 is supported for all measures of faithful appropriation moves.			

H4. Members with high levels of Internet privacy concern will have more faithful appropriation moves compared to members with low levels of privacy concern.

Supported for all three faithful appropriation moves.

H4a. Members with high levels of Internet privacy concern will report a higher level of Use appropriation moves compared to members with low levels of Internet privacy concern.

Supported, significant ($p = .003$), $R^2 = .051$

H4b. Members with high levels of Internet privacy concern will report a higher level of Familiarity appropriation moves compared to members with low levels of Internet privacy concern.

Supported, significant ($p = .013$)

H4c. Members with high levels of Internet privacy concern will report a higher level of Restricted Scope appropriation moves compared to members with low levels of Internet privacy concern.

Supported, significant ($p = .025$), $R^2 = .032$

Table 9.8 Summary of Hypothesis Tests for H5

	H5. Members with high levels of Internet privacy concern will have fewer ironic appropriation moves compared to members with low levels of privacy concern.		
Dependent variable	Statistical test	Results	Conclusion
One Sided Profile Browsing, general condition	Chi-Square	Pearson Chi-Square = .467, df = 2, sig. = .792	H5 is not supported for One Sided Profile Browsing, general condition
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = .924, df = 2, sig. = .630	H5 is not supported for One Sided Profile Browsing, extreme condition
H5 is not supported.			

H5. Members with high levels of Internet privacy concern will have fewer ironic appropriation moves compared to members with low levels of privacy concern.

Not supported.

H5a. Members with high levels of Internet privacy concern will be less likely to match the One Sided Profile Browsing, general condition compared to members with low levels of privacy concern.

Not supported.

H5b. Members with high levels of Internet privacy concern will be less likely to match the One Sided Profile Browsing, extreme condition compared to members with low levels of privacy concern.

Not supported.

Table 9.9 Summary of Hypothesis Tests for H6

H6. Members with high levels of Internet privacy concern will report a higher level of faithful appropriation compared to members with low levels of privacy concern.			
Dependent variable	Statistical test	Results	Conclusion
Faithful With System Spirit	Chi-Square	Pearson's Chi-Square = 1.416, df = 4, sig. = .841	H6 is not supported
Unfaithful (ignorance/lack of engagement with privacy settings)	ANOVA	F (2, 219) = 3.424, sig. = .034, R squared = .031	H6 is supported
H6 is partially supported for the Unfaithful variable.			

H6. Members with high levels of Internet privacy concern will report a higher level of faithful appropriation compared to members with low levels of privacy concern.

Partially supported.

H6a. Members with high levels of Internet privacy concern will report a higher level of Faithfulness with System Spirit compared to members with low levels of privacy concern.

Not supported.

H6b. Members with high levels of Internet privacy concern will report a lower level of Unfaithfulness/Ignorance or lack of engagement with privacy settings compared to members with low levels of privacy concern.

Supported, significant ($p = .034$), $R^2 = .031$.

Table 9.10 Summary of Hypothesis Tests for H7

H7. Members with high levels of usage will have more faithful appropriation moves compared to members with low usage.			
Dependent variable	Statistical test	Results	Conclusion
Use (transformed with Ln)	ANOVA	F (1, 217) = 3.847, sig. = .051, R squared = .018	H7 is not supported (borderline result)
Familiar	ANOVA	F (1, 217) = .435, sig. = .510	H7 is not supported
Scope (transformed with square root)	ANOVA	F (1, 217) = .077, sig. = .782	H7 is not supported
H7 is not supported.			

H7. Members with high levels of usage will have more faithful appropriation moves compared to members with low usage.

Not supported.

H7a. Members with high levels of usage will report a higher level of Use appropriation move compared to members with low levels of usage.

Not supported (significance is borderline, $p = .051$)

H7b. Members with high levels of usage will report a higher level of Familiarity appropriation move compared to members with low levels of usage.

Not supported.

H7b. Members with high levels of usage will report a higher level of Restricted Scope appropriation move compared to members with low levels of usage.

Not supported.

Table 9.11 Summary of Hypothesis Tests for H8

H8. Members with high levels of usage will have fewer ironic appropriation moves compared to members with low usage.			
Dependent variable	Statistical test	Results	Conclusion
One Sided Profile Browsing, general condition	Chi-Square	Pearson's Chi-Square = .758, df = 1, sig. = .384	H8 is not supported
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson's Chi-Square = 2.471, df = 1, sig. = .116	H8 is not supported
H8 is not supported.			

H8. Members with high levels of usage will have fewer ironic appropriation moves compared to members with low usage.

Not supported.

H8a. Members with high levels of usage will be less likely to match One Sided Profile Browsing, general condition compared to members with low usage.

Not supported.

H8b. Members with high levels of usage will be less likely to match One Sided Profile Browsing, extreme condition compared to members with low usage.

Not supported.

Table 9.12 Summary of Hypothesis Tests for H9

H9. Members with high levels of usage will report a higher level of faithful appropriation compared to members with low usage.			
Dependent variable	Statistical test	Results	Conclusion
Faithful With System Spirit	ANOVA	F (1, 218) = .662, sig. = .417	H9 not supported
Unfaithful (ignorance/lack of engagement with privacy settings)	ANOVA	F (1, 218) = 3.912, sig. = .049, R squared = .018	H9 is supported
H9 is partially supported for the Unfaithful variable.			

H9. Members with high levels of usage will report a higher level of faithful appropriation compared to members with low usage.

Partially supported.

H9a. Members with high levels of usage will report a higher level of Faithfulness with System Spirit appropriation compared to members with low usage.

Not supported.

H9b. Members with high levels of usage will report a lower level of Unfaithfulness/Lack of engagement with privacy settings compared to members with low usage.

Supported, significant ($p = .049$), $R^2 = .018$.

Table 9.13 Summary of Hypothesis Tests for H10

	H10. For members with high usage, those members with high Internet privacy concerns will have more ironic appropriation moves compared to members with low Internet privacy concern.		
Dependent variable	Statistical test	Results	Conclusion
Appropriation moves			
Use (transformed with Ln)	Chi-Square	Pearson Chi-Square = 7.644, df = 4, sig. = .106	H10 not supported
Familiar	Chi-Square	Pearson Chi-Square = 14.984, df = 4, sig. = .005	H10 is supported, high use high privacy concern subjects show a lower than expected familiarity with their privacy settings
Restricted Scope (transformed with square root)	ANOVA	(Interaction results) F (2, 212) = 2.272, sig. = .106	H10 is not supported
One Sided Profile Browsing, general condition	ANOVA	(Interaction results) F (2, 214) = .125, sig. = .882	H10 is not supported
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = 1.279, df = 2, sig. = .528	H10 is not supported
Perceptions of appropriation and use			
Faithful With System Spirit	ANOVA	(Interaction results) F (2, 214) = .912, sig. = .474	H10 is not supported
Unfaithful (ignorance/lack of engagement with privacy settings)	ANOVA	(Interaction results) F (2, 214) = .272, sig. = .762	H10 is not supported
For nearly all measures H10 is not supported. H10 is only supported for the Familiar appropriation move.			

H10. For members with high usage, those members with high Internet privacy concerns will have more ironic appropriation moves compared to members with low Internet privacy concern.

Partially supported (for Familiarity appropriation move only).

H10a. For members with high usage, those members with high Internet privacy concerns will show a lower level of Use appropriation moves compared to members with low Internet privacy concern.

Not supported.

H10b. For members with high usage, those members with high Internet privacy concerns will show a lower level of Familiarity appropriation moves compared to members with low Internet privacy concern.

Supported, significant ($p = .005$)

H10c. For members with high usage, those members with high Internet privacy concerns will show a higher level of One Sided Profile Browsing, general condition compared to members with low Internet privacy concern.

Not supported.

H10d. For members with high usage, those members with high Internet privacy concerns will show a lower level of higher level of One Sided Profile Browsing, extreme condition compared to members with low Internet privacy concern.

Not supported.

H10e. For members with high usage, those members with high Internet privacy concerns will show a lower level of Faithfulness with System Spirit compared to members with low Internet privacy concern.

Not supported.

H10f. For members with high usage, those members with high Internet privacy concerns will show a higher level of Unfaithfulness/Lack of Engagement With Privacy Management compared to members with low Internet privacy concern.

Not supported.

9.6 Open Research Questions

While it is anticipated that there will be some relationship between concern for Internet privacy, appropriation support, and usage, current understanding of the dynamics of these sites is not sufficient enough to predict the nature of those relationships. These were tested as open research questions.

What is the effect of high privacy concern on levels of usage? What is the effect of appropriation support for privacy management on levels of usage? Specifically, is there a relationship between demographic categories (such as gender, age, school status, and ethnicity) and appropriation moves? Does their previous experience with issues of online privacy influence their system use and appropriation moves? These questions were tested using ANOVA analysis and summarized in this section.

Table 9.14 Summary of Hypothesis Tests for Outcomes by Gender

Is there a difference with respect to gender and measured outcomes?			
Dependent variable	Statistical test	Results	Conclusion
Appropriation moves			
Use (transformed with Ln)	ANOVA	F (1, 212) = 9.965, sig. = .002, R squared = .045	Females report significantly higher use of privacy settings compared to males
Familiarity	ANOVA	F (1, 212) = .065, sig. = .800	No significant differences found
Restricted Scope (transformed with square root)	Chi-Square	Pearson Chi-Square = 9.419, df = 1, sig. = .009	Females report significantly higher results on scope settings compared to males
One Sided Profile Browsing, general condition	Chi-Square	Pearson Chi-Square = 2.204, df = 1, sig. = .138	No significant differences found
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = .005, df = 1, sig. = .943	No significant differences found
Perceptions of appropriations and use			
Distrust of other members	ANOVA	F (1, 214) = .944, sig. = .332	No significant differences found
Faithful With System Spirit	ANOVA	F (1, 218) = .658, sig. = .418	No significant differences found
Unfaithfulness (ignorance/lack of engagement with privacy settings)	ANOVA	F (1, 218) = 5.747, sig. = .017, R squared = .026	Males report significantly more ignorance/lack of engagement with privacy settings compared to females
Differences in gender were found for Use (Females report higher Use than Males), Restricted Scope (Females report higher levels of Restricted Scope), and for Unfaithfulness (Males report higher levels of Unfaithfulness)			

Comparisons of results by gender are summarized in Table 9.14. Differences in gender were found for the Use appropriation move. Females report significantly higher Use than males. For Restricted Scope, females report significantly higher levels. Males

report significantly higher levels of Unfaithfulness/lack of engagement with privacy settings.

Table 9.15 Summary of Hypothesis Tests for Outcomes by Age

Is there a difference with respect to age and measured outcomes?			
Independent variable: Age 24 and over (median age for subjects is 23)			
Dependent variable	Statistical test	Results	Conclusion
Appropriation moves			
Use (transformed with Ln)	ANOVA	$F(1, 220) = 3.805$, sig. = .052, R squared = .017	Results are borderline not significant, but younger members do report higher levels of use compared to older members.
Familiarity	ANOVA	$F(1, 216) = .759$, sig. = .385	No significant difference found
Restricted Scope (transformed with square root)	ANOVA	$F(1, 216) = .069$, sig. = .793	No significant difference found
One Sided Profile Browsing, general condition	Chi-Square	Pearson Chi-Square = .180, df = 1, sig. = .670	No significant difference found
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = .180, df = 1, sig. = .672	No significant difference found
Perceptions of appropriations and use			
Distrust	ANOVA	$F(1, 214) = .001$, sig. = .971	No significant difference found
Faithful With System Spirit	ANOVA	$F(1, 218) = .337$, sig. = .562	No significant difference found
Unfaithfulness (ignorance/lack of engagement with privacy settings)	ANOVA	$F(1, 218) = .243$, sig. = .622	No significant difference found
No significant differences found between younger and older subjects.			

Table 9.16 Summary of Hypothesis Tests for Outcomes by School Status

	Is there a difference with respect to school status and measured outcomes? Independent variable: Undergraduate (about half the subjects are undergraduates)		
Dependent variable	Statistical test	Results	Conclusion
Appropriation moves			
Use (transformed with Ln)	ANOVA	$F(1, 212) = .262, \text{sig.} = .609$	No significant difference found
Familiarity	ANOVA	$F(1, 216) = .006, \text{sig.} = .939$	No significant difference found
Restricted Scope (transformed with square root)	ANOVA	$F(1, 216) = 2.703, \text{sig.} = .102$	No significant difference found
One Sided Profile Browsing, general condition	Chi-Square	Pearson Chi-Square = .011, $df = 1, \text{sig.} = .916$	No significant difference found
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = .816, $df = 1, \text{sig.} = .366$	No significant difference found
Perceptions of appropriations and use			
Distrust	ANOVA	$F(1, 214) = .038, \text{sig.} = .845$	No significant difference found
Faithful With System Spirit	ANOVA	$F(1, 218) = .725, \text{sig.} = .395$	No significant difference found
Unfaithfulness (ignorance/lack of engagement with privacy settings)	ANOVA	$F(1, 218) = .088, \text{sig.} = .768$	No significant difference found
No significant differences were found comparing undergraduates with other subjects.			

A summary of comparisons based on age is presented in Table 9.15. The population was divided based on the median age of 24. Multiple ANOVA tests were then run for each of the measured outcomes. No significant difference was found for any of the measured outcomes.

Table 9.17 Summary of Hypothesis Tests for Outcomes by Ethnicity

	Is there a difference with respect to ethnicity and measured outcomes? Independent variable: Whether subject is White (about half the subjects are White)		
Dependent variable	Statistical test	Results	Conclusion
Appropriation moves			
Use (transformed with Ln)	Chi-Square	Pearson's Chi-Square = 2.272, df = 2, sig. = .321	No significant difference found
Familiarity	ANOVA	F (1, 216) = .111, sig. = .740	No significant difference found
Restricted Scope (transformed with square root)	ANOVA	F (1, 216) = .526, sig. = .469	No significant difference found
One Sided Profile Browsing, general condition	Chi-Square	Pearson Chi-Square = 1.083, df = 1, sig. = .298	No significant difference found
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = 1.029, df = 1, sig. = .310	No significant difference found
Perceptions of appropriations and use			
Distrust	ANOVA	F (1, 214) = .624, sig. = .431	No significant difference found
Faithful With System Spirit	ANOVA	F (1, 218) = 1.520, sig. = .219	No significant difference found
Unfaithfulness (ignorance/lack of engagement with privacy settings)	ANOVA	F (1, 218) = 1.090, sig. = .298	No significant difference found
No significant differences were found comparing White subjects with non-White subjects.			

Table 9.18 Summary of Hypothesis Tests for Outcomes by Privacy Experience

	Do prior experiences with online privacy influence outcomes? Independent variable: Whether subject is has experiences an issue with online privacy within the last year (42 out of 222 said yes, about 18%)		
Dependent variable	Statistical test	Results	Conclusion
Appropriation moves			
Use (transformed with Ln)	ANOVA	$F(1, 220) = .040, sig. = .843$	No significant difference found
Familiarity	ANOVA	$F(1, 216) = .005, sig. = .945$	No significant difference found
Restricted Scope (transformed with square root)	ANOVA	$F(1, 216) = .110, sig. = .740$	No significant difference found
One Sided Profile Browsing, general condition	Chi-Square	Pearson Chi-Square = 2.261, $df = 1, sig. = .133$	No significant difference found
One Sided Profile Browsing, extreme condition	Chi-Square	Pearson Chi-Square = .001, $df = 1, sig. = .975$	No significant difference found
Perceptions of appropriations and use			
Distrust of Other Members	ANOVA	$F(1, 214) = 9.973, sig. = .002, R\text{ squared} = .045$	Subjects who had experienced a privacy incident had a higher level of distrust compared to subjects who did not.
Faithful With System Spirit	ANOVA	$F(1, 218) = .015, sig. = .904$	No significant difference found
Unfaithfulness (ignorance/lack of engagement with privacy settings)	ANOVA	$F(1, 218) = .090, sig. = .765$	No significant difference found
No significant differences were found for subjects who had experienced a privacy incident with respect to appropriation moves. A significant difference was found with respect to distrust of other members.			

Table 9.16 presents a summary of comparisons based on school status. The population was divided based on school status, those who are currently a student and those who identify themselves as “not a student.” A series of ANOVA tests were conducted for each of the measured outcomes. No significant differences were found for any of the measured outcomes based on school status.

Table 9.17 presents a summary of comparisons based on ethnicity. The population was divided into two groups based on ethnicity, White and non-White subjects. Multiple ANOVA tests were run against each of the measured outcomes. No significant differences were found for any of the measured outcomes based on ethnicity.

Table 9.18 presents a summary of results regarding personal experience with a privacy incident while using a social networking site. Subjects were asked if they had personal experience with a privacy episode within the past year. The answers were used to divide the population into two groups, those who reported a privacy incident ($n=42$) versus those that did not ($n=180$). Multiple ANOVA tests were conducted against each of the measured outcomes. A significant difference was only found in one case, which is the construct measuring Distrust of other members.

Those who reported a prior privacy experience had significantly higher levels of Distrust $F(1, 214) = 9.973$, $\text{sig.} = .002$, with $R^2 = .045$.

Notice there is no significant difference found for constructs such as Use or Familiarity with privacy management. This seems to be a contradictory result. You would expect that a user who reports a privacy episode would also report more Use or more Familiarity. However, this is not the case.

The application of ANOVA and factor analysis to this data set has helped establish constructs and measures that pass reliability tests. However, the basis of ANOVA is a one-to-one comparison of variables. With all the complex interaction that takes place within an online social environment, it becomes very difficult to validate a socio-technical model while keeping within the constraints of regression based analysis. Model based analysis methods, such as structural equation modeling (SEM) or partial least squares (PLS) provide more flexibility with respect to examining the overall validity of a conceptual model. Therefore in the next chapter will describe the testing of this research model using PLS.

CHAPTER 10

PLS ANALYSIS OF FINDINGS

This chapter describes the use of the data analysis tool Smart-PLS (Ringle, Wende, & Will, 2005) to carry out a secondary analysis of the main hypotheses. This chapter describes the validity and reliability requirements for using PLS, and then applies PLS to test the research model.

10.1 Overview of PLS

The construction of predictive models of socio-technical systems requires the ability to manipulate variables within a system framework. This involves modeling multiple relationships and interactions. Multi-variate analysis based on regression and analysis of variance looks at two variables at a time. Because regression is looking at predicting the location of two points on a line, it has limited flexibility for interactive analysis and modeling of socio-technical systems.

Computer modeling methods such as structural equation modeling (SEM) and partial least squares (PLS) provide a process whereby complex relationships within a set of variables can be analyzed and considered (Gefen, Straub, & Boudreau, 2000). These methods allow a system to be defined as a combination of constructs and paths that can depict the model in motion. SEM and PLS evaluate the underlying structural model, along with the measurement model, made up of the path weights between constructs. While these methods use regression as their building block, they do not have the same strict requirements as to the shape of the distribution (Chin, 1998).

In addition, PLS has more flexibility with respect to the underlying structure of constructs. In the terminology of structural equation modeling, constructs are made up of measures, or indicators or items. Indicators are combined to form a latent variable, because the variable of interest is not directly observable (i.e., latent), and must instead be abstractly constructed through combinations of indicators (Petter, Straub, & Rai, 2007).

Latent variables can be constructed in one of two ways. The most common method to date within information systems research is where each item measures the same specific aspect of a construct. Each indicator is considered to be interchangeable, since they are all related to the same thing. This form is called a reflective construct, so that the indicators reflect the construct, not the other way around. Within this research study, Concern for Internet Privacy is an example of a reflective construct. These types of constructs have a long history in social science based research, and their validity and reliability can be defined by well established methods (Petter et al., 2007).

However many variables of interest, especially within socio-technical systems, are not so easily modeled as reflective constructs. For example, factors that comprise a person's teamwork skills can include punctuality, communication skills, and personal flexibility. It does not make sense to combine these as a reflective construct. Another important examples is system usage, which Barki, Titah and Boffo argue cannot be accurately modeled by only including indicators that reflect the same aspect (Barki, Titah, & Boffo, 2007).

In these cases, researchers argue that it is more accurate to create formative constructs. Formative constructs are composites of indicators that form the latent variable. While reflective constructs are unidimensional, this is not the case with

formative constructs. The composite of the indicators are said to cause the formative construct, not the other way around. In addition, removing an indicator from a formative construct reduces the coverage of the construct and may de-stabilize its reliability (Petter et al., 2007).

PLS has the ability to evaluate models that contain formative constructs (Chin, 1998). Petter, Straub and Rai have argued that numerous studies in information systems contain constructs mis-specified as reflective rather than formative, resulting in both Type I and Type II errors (Petter et al., 2007). Therefore, the statistical package Smart-PLS (Ringle et al., 2005) will be used to evaluate this research model due to its ability to handle formative constructs.

Within this research, the construct Faithful Appropriation Moves is an example of a formative construct. As presented in this research study, Faithful Appropriation is a combination of the Use appropriation move, the Familiarity appropriation move, and the Restricted Scope appropriation move. In terms of creating a clearer picture of the use of privacy management with social networking sites, the use of PLS to consider what factors impact faithful appropriation moves is very beneficial.

While PLS does have the benefit of being able to handle formative constructs, the validity of PLS has been called into question by Goodhue, Lewis, and Thompson (Goodhue, Lewis, & Thompson, 2006). Goodhue et al. specifically argue against the claim that PLS provides a way to handle data with small sample sizes, i.e., less than 50. In their analysis, they used a Monte Carlo method to generate data sets with sample sizes of 40, 90, 150 and 200. They then compared the outcomes of regression analysis, SEM,

and PLS. Their results found that PLS did not accurately calculate path weights or significance with small sample sizes.

However, their research did find that PLS is accurate with samples sizes of 150 or more, and is equal or better than SEM when combined with normal theory testing (Goodhue et al., 2006). All of the analysis presented here is based on a sample size of at least 150.

10.2 Establishing Validity and Reliability Using PLS

The use of PLS requires a different set of reliability and validity processes compared to regression based analyses, as described by Chin (1998). These processes include the following:

Average Variance Extracted (AVE)

This statistic is a measure of the amount of variance that a latent variable is able to capture, as compared to the amount of measurement error. This statistic is only relevant for reflective latent variables within a model. It is recommended that AVE exceed .50 for all reflective latent variables within a model (Chin, 1998).

Discriminant Validity

AVE can be used as a measure of discriminant validity for a measurement model through the following process. It is recommended that the AVE of each latent variable should be greater than the square of the correlations among the latent variables. This is a test of the validity of the model because it indicates that more variance is shared between the latent variable and its indicators than another latent variable and its block of indicators. An

equivalent comparison that can be use is between the values in the correlation matrix and the square root of the AVE (Chin, 1998).

Composite Reliability

Composite reliability is a measure of reliability for a given block of indicators. As with AVE, it is only relevant for reflective constructs. In general, Cronbach's alpha serves as a lower bound for Composite Reliability, so values of .70 are considered acceptable (Chin, 1998).

Cross Loadings

An additional test of discriminant validity for reflective constructs can be obtained by examining cross-loadings between indicators and other constructs in the model. In a manner similar to factor analysis, an indicator should not cross load on more than one latent variable, or load higher for another construct than the one that it is assigned to (Chin, 1998).

Model Evaluation (Practical Significance)

The primary output of PLS analysis is a calculation of the R-squares for each dependent construct. The underlying method used by PLS is regression, so that the value of the derived R-squares can be interpreted in a similar manner to regression results. An additional test of the practical significance of a model is to calculate R-square values with and without a specific independent construct, then compare the difference. This process results in the calculation of the effect size (f^2). A resulting f^2 of .02 indicates a low effect, .15 a medium effect, and .35 a large effect (Chin, 1998).

Predictive Relevance

PLS uses a re-sampling method known as blindfolding to evaluate the predictive relevance of a model (Chin, 1998). The blindfolding method systematically omits a portion of actual data from the model, and uses the model to predict what those data points “should” be. Then the predicted data point is compared to the omitted “actual” data point. This process continues until every data point has been omitted, predicted, and compared.

The statistic q^2 is calculated by comparing the sum of the prediction error with the sum of the observed points. If the resulting q^2 statistic is greater than zero (0), this implies the model has predictive relevance, and values below zero (0) indicate a lack of predictive relevance (Chin, 1998).

Redundancy Analysis

When using PLS to evaluate a model with a formative construct, it is recommended to perform a redundancy analysis on the formative construct. This involves the following process. The first step in the analysis is to construct a two block redundancy model. One block is the formative latent variable, and the second block is a reflective version of the same construct. By examining the path weights between the two blocks, the success of the formative variable in predicting R-square values can be evaluated. As a test of convergent validity, a path from the formative construct to the reflective construct of .80 would indicate an adequate sign of convergent validity (Chin, 1998).

10.3 Redundancy Analysis

Using the process described above, the model for this research study was analyzed for its reliability, validity, and predictive relevance. The main dependent construct of interest is Faithful Appropriation Moves. In other words, what factors predict a member's faithful use of privacy management features within a social networking site?

The first step for this analysis is the construction of a redundancy test for the formative construct Faithful Appropriation Moves. This formative construct is made up of three faithful moves: the Use appropriation move, the Familiarity appropriation move, and the Restricted Scope appropriation move.

The redundancy test was used to create a parsimonious formative construct for Faithful Appropriation Moves. Included in the test are three indicators for the Familiarity move, four indicators for the Use move, and three indicators for the Restricted Scope move. The indicators for each of these constructs are the same as the indicators for the multi-variate analysis conducted in Chapter 8. These ten indicators were loaded into a formative block. A second block was constructed of reflective measures of Faithfulness. The indicators for this block come from the five item construct Unfaithfulness. The unfaithfulness indicators were reversed for this analysis to improve the clarity of the model. These two blocks were then connected.

The goal at this stage is to only retain indicators with significant path weights, but also have at least one representative from each appropriation move. It is recommended to drop poor indicators, as long as the behaviors of interest within the multi-dimensional construct are represented (Chin, 1998).

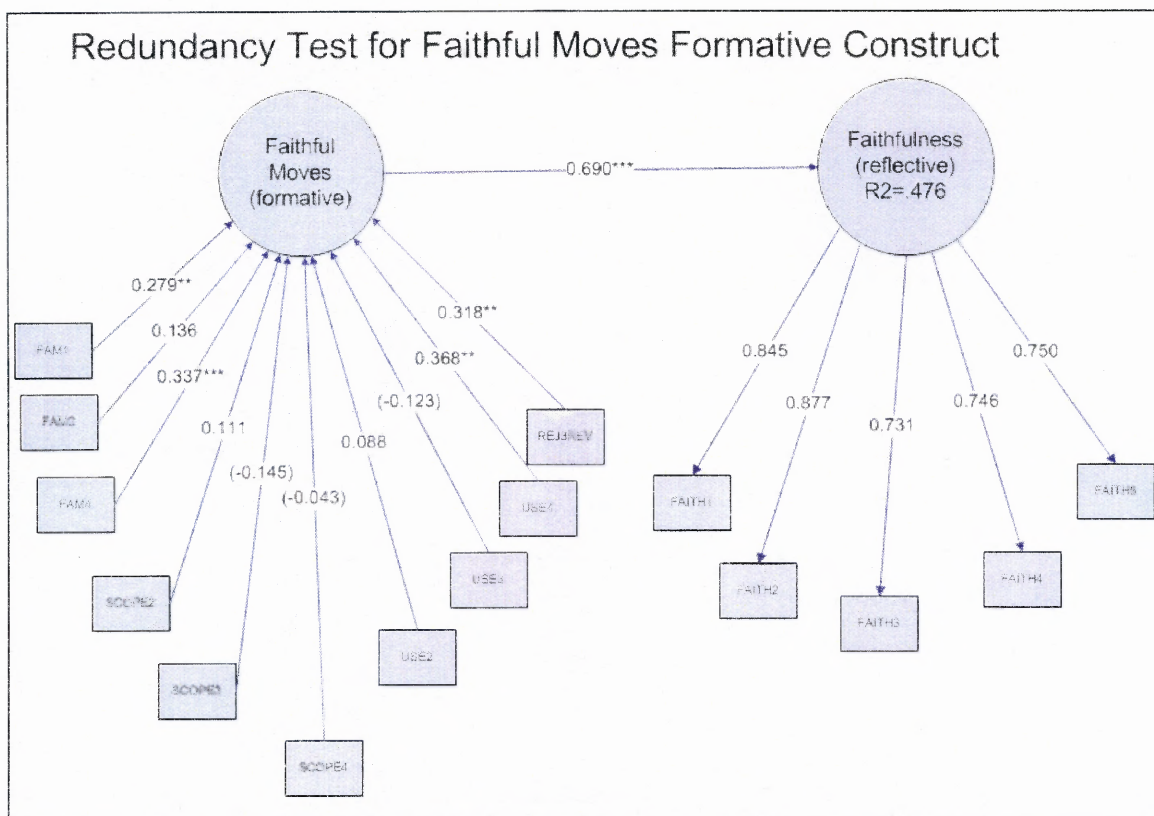


Figure 10.1 Redundancy analysis of Faithful appropriation moves.

As shown in Figure 10.1, the results of this redundancy test show a correlation of 0.690 between the formative construct Faithful Appropriation Moves and the reflective construct Faithfulness. While this is below the recommended level of .80 for redundancy tests, it is acceptable to consider results below this threshold for exploratory research (Chin, 1998). The R-squared for this redundancy analysis is .476. This value provides further support for the validity of this approach, because research on system usage as a formative construct found that R-squared values around .45 to be acceptable (Barki et al., 2007).

The impact of the individual indicators within the redundancy test can be seen by examining the path weights and significance of the components of the formative model. These are listed in Table 10.1. The indicators that have significant path weights are

marked in the table with a heavy border. These indicators are FAM1, FAM4, USE4 and REJ3REV. Their path weights are 0.279, 0.337, 0.368, and 0.318, respectively. The best result for the Restricted Scope move is the indicator SCOPE3, which has a p value of .07 with a path weight of -0.145.

Table 10.1 Summary of Faithful Appropriation Moves Formative Construct

Summary of Indicators for Faithful Appropriation Moves Formative Construct			
Label	Statement	Path Weights	T-Stat
Fam1	I am comfortable with my ability to adjust my privacy settings.	0.279	2.715**
Fam2	I am confident that I know how to control who is able to see my profile on [name of social networking site].	0.136	1.346
Fam4	When I need to modify my privacy settings for [name of social networking site], I am able to do it.	0.337	3.405***
Scope2	I don't use [name of social networking site] to make contact with people whom I've never heard of.	0.111	1.100
Scope3	I never accept friend requests from people I have not met in person.	-0.145	1.362
Scope4	When using [name of social networking site] I ignore contact from people whom I have not met in person.	-0.043	0.358
Use2	I have modified the privacy settings for my profile on [name of social networking site].	0.088	0.536
Use3	I have adapted the privacy settings to control who can view my profile on [name of social networking site].	-0.123	0.794
Use4	I have personalized my privacy settings on [name of social networking site].	0.368	2.888**
Reject3Rev	I don't use the privacy settings to control who can access my profile.	0.318	2.713**
* - $p < .05$ ** - $p < .01$ *** $p < .001$			

The strongest path weight among all the indicators is for FAM4: “When I need to modify my privacy settings for [name of social networking site], I am able to do it.” This implies an individual’s evaluation of their potential ability (i.e., self-efficacy) to adjust their privacy settings has the strongest weight in determining faithfulness. It is also interesting that the indicator SCOPE3 has a negative weight: “I never accept friend requests from people I have not met in person.” This implies that subjects who do not use social networking sites to explore new relationships are less likely match a faithfulness profile, perhaps because they are screening their privacy through their offline interactions.

Two indicators have extremely low path weights, SCOPE4: “When using [name of social networking site] I ignore contact from people whom I have not met in person,” and USE1: “In order to control who can contact me using [name of social networking site] I have adjusted my privacy settings.” This seems to suggest that managing contact from other members of the site is not considered to be related to faithful privacy management. If non-significant items are dropped, but the highest result for the restricted scope move is kept, that leaves the following set of indicators to be used for subsequent analysis: FAM1, FAM4, SCOPE3, USE4, and REJ3REV.

The ability to examine the impact of individual indicators is an advantage of using PLS to carry out an exploratory analysis. Because regression analysis typically involves creating summative scales, the impact of individual indicators can be difficult to trace. Since PLS calculates linear relationships going from one indicator to another, the relative path weight and significant of individual indicators is preserved and made available to the researcher.

Table 10.2 summarizes the results for the five Faithfulness reflective indicators. As explained previously, the results of these items have been reversed to improve the clarity of the model. All the indicators load at .735 or higher. This is consistent with the results of the factor analysis described in chapter 8. These are acceptable loadings for a reflective measure within PLS (Chin, 1998).

Table 10.2 Summary of Indicators for Faithfulness Reflective Construct

Summary of Indicators for Unfaithfulness Reflective Construct			
Label	Statement	Loadings	T-Stat
Faith1	I probably use the privacy settings for [name of social networking site] improperly.	0.847	21.934
Faith2	I failed to use the privacy settings of [name of social networking site] as they should be used.	0.877	44.356
Faith3	I did not use the privacy settings in [name of social networking site] in the most appropriate fashion.	0.735	11.753
Faith4	I don't know what my privacy settings are on [name of social networking site].	0.742	12.701
Faith5	I don't bother to look at the privacy settings for my profile on [name of social networking site].	0.747	13.308
All items significant at .001 level.			

10.4 PLS Analysis of Research Model

Next PLS was used to test the research model described in Chapter 5. The results are shown in Figure 10.2. The three independent variables are System Usage, Attitudes Towards Privacy, and level of Appropriation Support. In addition, an interaction effect was hypothesized between Concern for Internet Privacy and System Usage.

The indicators for this model are as follows. Appropriation Support has a binary indicator for level of appropriation support, with 1 for high (i.e., Facebook) and 0 for low

(i.e., MySpace). System Usage is a formative construct with two indicators. The first is HighUse, a binary indicator, with 1 indicating high use (at least every day) and 0 indicating a lower level of use. The second indicator is UseBoth, with 1 indicating the subjects use both sites at least once a month, and 0 indicating another level of usage.

The Attitudes Towards Privacy Construct contains the five item Internet Privacy Concern Scale (summarized in Section 7.9.1) and an additional indicator related to how much the subjects value their privacy (summarized in Section 7.10.8). Testing of the model found that adding this extra indicator improved the R-squared results, while still meeting the PLS quality criteria.

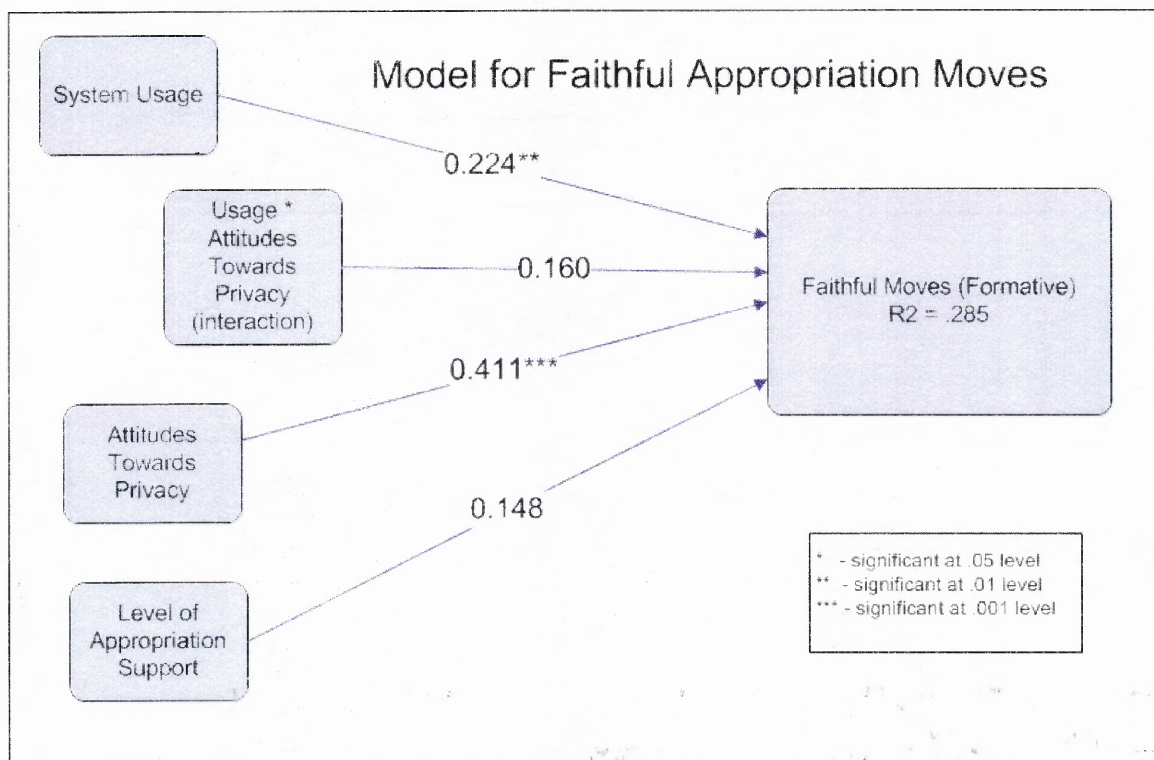


Figure 10.2 PLS evaluation of Faithful Privacy Management model.

In the results presented in Figure 10.2, two paths are significant: from Concern for Internet Privacy and System Usage. The path weight for Attitudes Towards Privacy is 0.411, with a significance level of less than .001. The path weight for System Usage is

0.224, with a significance level of less than .01. The two other paths, Level of Appropriation Support and the interaction effect between System Usage and Concern for Internet Privacy, are not significant.

The R-squared result for this model is 0.285. The AVE for Concern for Internet Privacy is 0.64, well above the recommended threshold of .50. The composite reliability for this construct is .899, also an acceptable value. None of the indicators are cross loading on any other construct. The q^2 value for this model is greater than zero, indicating the model does have predictive relevance.

These results show there is validity and reliability in this model, which explains about 28% of the variance with respect to Faithful appropriation of privacy management. Next the model will be used to test the research hypotheses.

Hypotheses for Faithful Moves

Members of sites with high levels of appropriation support (Facebook) will report higher levels of faithful appropriation moves compared to members of sites with high levels of appropriation support (MySpace).

Not supported. Path weight is in the predicted direction (0.148) but is not significant.

Members with higher levels of usage will report higher levels of faithful appropriation moves compared to members with lower levels of usage.

Supported. Path weight of 0.224 is significant at the .01 level.

Members with higher levels of concern for Internet privacy will report higher levels of faithful appropriation moves compared to members with low levels of concern for Internet privacy.

Supported. Path weight of 0.411 is significant at the .001 level.

For members with high levels of usage, those with high levels of Internet privacy concern will report lower levels of faithful appropriation moves compared to members with lower levels of Internet privacy concern (interaction effect).

Not supported. Path weight is in the opposite of hypothesized direction (0.160) and is not significant.

The next section will present the PLS results for unfaithful moves.

10.5 PLS Analysis For Unfaithful Moves

The research model was tested using PLS with unfaithful appropriation moves. This research study included three measures for unfaithful appropriation moves, which potentially could be combined into a formative construct. This ended up not being possible, because only one of the measures resulted in reliable results. Recall that two versions of profile browsing were tested, One Sided Profile Browsing (general condition), and One Sided Profile Browsing (extreme condition). Recall that around 32 % of the subjects match the One Sided Profile Browsing (general condition), and 14 % match the One Sided Profile Browsing (extreme condition). Please refer to Section 7.10.7 for a full summary of the results.

As presented in Figure 10.3, the model has a very small R-squared value of only .083. It model has only one significant path weight, going from Privacy Attitudes to Unfaithful Moves, with a weight of 0.209 ($p < .01$). However, this result is opposite of the predicted effect. It was hypothesized that high levels of concern about privacy would make a subject less likely to carry out unfaithful moves. It passes all the quality criteria for PLS with respect to values for AVE, composite reliability, and q^2 .

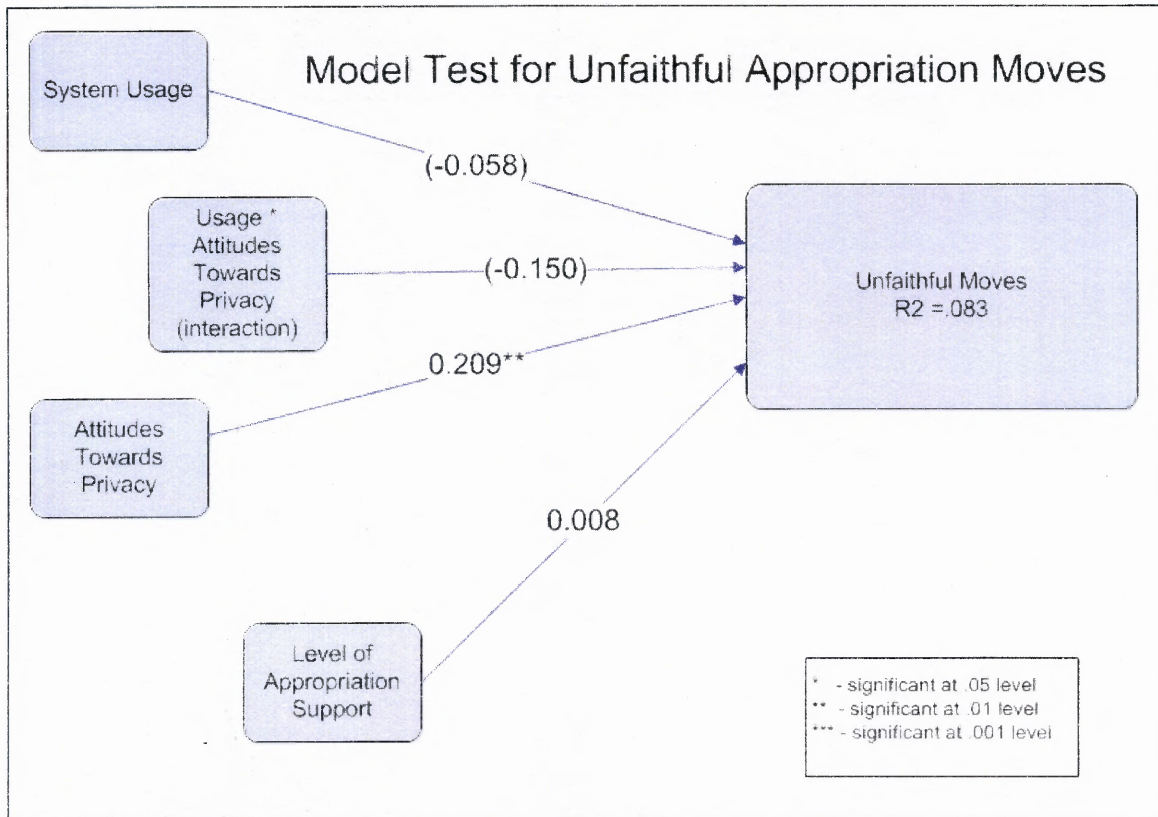


Figure 10.3 PLS analysis of Unfaithful moves.

While One Sided Profile Browsing is an unfaithful move, it does improve the overall privacy of the individual. The factor that raises the issue of unfaithfulness has to do with using privacy management features for individual advantage. So while the predicted direction of the relation between privacy concern and unfaithful moves is a negative path weight, it is not completely illogical that these subjects would be more likely to engage in One Sided Profile Browsing. This illustrates a limitation of the model that must be addressed by determining how to model behavior in situations where individual goals conflict with group goals.

Hypotheses for Unfaithful Moves

Members of sites with high levels of appropriation support will report lower levels of unfaithful appropriation moves compared to members of sites with high levels of appropriation support (MySpace).

Not supported. Path weight is very weakly in the opposite direction (0.008) but is not significant.

Members with higher levels of usage will report lower levels of unfaithful appropriation moves compared to members of sites compared to members with lower levels of usage.

Not supported. Path weight is in the predicted direction (-0.058) but is not significant.

Members with higher levels of concern for Internet privacy will report lower levels of unfaithful appropriation moves compared to members with low levels of concern for Internet privacy.

Not supported. Path weight is in the opposite direction (0.209) and is significant at the .01 level.

For members with high levels of usage, those with high levels of Internet privacy concern will report higher levels of unfaithful appropriation moves compared to members with lower levels of Internet privacy concern (interaction effect).

Not supported. Path weight is in the opposite of hypothesized direction (-0.150) and is not significant.

The next section will present the PLS results for the faithfulness construct.

10.6 PLS Analysis of Faithfulness

The research model was tested against the Faithfulness construct. The model derived an R-squared value of 0.131. There are two significant path weights, from System Usage, with a path weight of 0.126 ($p < .05$) and from Attitudes Towards Privacy, with a path weight of 0.265 ($p < .001$). The model passes all the quality criteria for AVE, composite reliability, and q^2 .

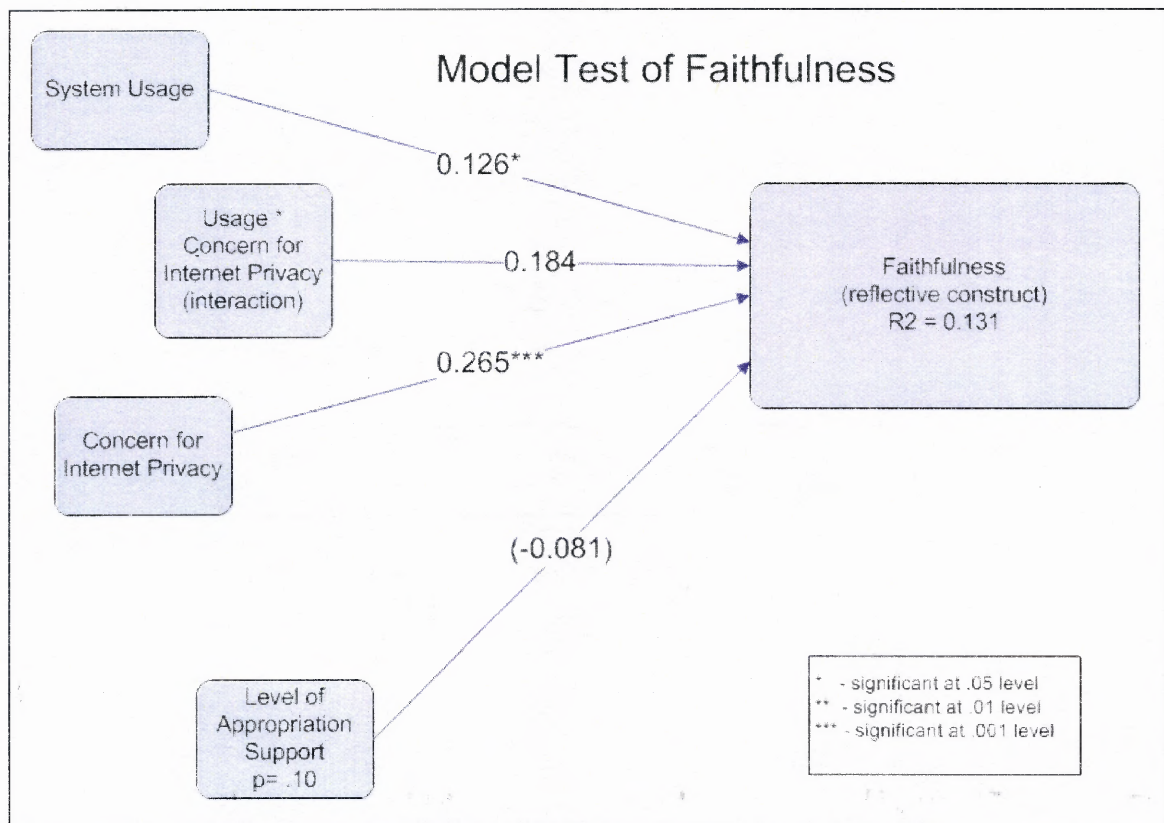


Figure 10.4 Summary of results for Faithfulness.

As described by (Chin, 1998), the validity of a formative construct can be tested by comparing its results with a version of the model with the reflective construct. If you compare Figure 10.2 with Figure 10.4, you can compare the relative weight and significance levels of the two versions. By mapping Faithful moves (formative construct)

with Faithfulness (reflective construct), you will see that the overall pattern of path weights is similar. There are positive significant path weights from both System Usage and Attitudes Towards Privacy. The path weight from the interaction effect also matches, being positive and not significant. The only difference is with appropriation support, which is positive for the formative construct, and negative for the reflective construct.

Hypotheses for Faithfulness

Members of sites with high levels of appropriation support will report higher levels of faithfulness compared to members of sites with high levels of appropriation support (MySpace).

Not supported. Path weight is weakly in the opposite of the predicted direction (0.206) but is not significant ($p=.10$).

Members with higher levels of usage will report higher levels of faithfulness compared to members with lower levels of usage.

Supported. Path weight of 0.126 is significant at the .05 level.

Members with higher levels of concern for Internet privacy will report higher levels of faithfulness compared to members with low levels of concern for Internet privacy.

Supported. Path weight of 0.265 is significant at the .001 level.

For members with high levels of usage, those with high levels of Internet privacy concern will report lower levels of faithful appropriation moves compared to members with lower levels of Internet privacy concern (interaction effect).

Not supported. Path weight is in the opposite of hypothesized direction (0.184) and is not significant.

The next chapter will present an expanded analysis of the results using PLS, and apply results from the qualitative responses in order to explain the findings.

CHAPTER 11

EXPLORATION OF FINDINGS USING PLS AND QUALITATIVE ANALYSIS

11.1 Adding Social Context to The Research Model

In the research model proposed for this study, the independent variable Appropriation Support is a binary indicator that denotes either high (1) or low (0) levels of appropriation support. However, because no other constructs in the model capture perceptions of social interaction, Appropriation Support becomes a stand in for the entire social experience with a social networking site.

What the model calls Appropriation Support is actually a single binary indicator that should be called “Social Networking Site.” Reducing the experience of using a social networking site to a binary variable does not accurately capture the member’s experience. The similar reduction of “technology” to a single indicator has been critiqued by Orlikowski: “By aggregating task, technique, knowledge, and tools into a single construct – technology – interaction among these constituting components and with humans is ignored,” (Orlikowski, 1992).

As Orlikowski explained in her paper, technology cannot be modeled as a monolithic, one-dimensional independent variable. This is also the case with the use of social networking sites. The original research model only has one indicator related to the site, i.e., level of appropriation support. This model is derived from theory that places technology use within an organizational context. While the use of social networking site is not related to organizational issues, it does take place within a social context. So a

more accurate predictive model would need to take into account the impact of social context.

An advantage of the use of PLS as an analysis tool is the ability to easily and flexibly explore alternate combinations of constructs as a way to develop theory (Chin, 1998). This leads to the opportunity to test additional indicators that capture perceptions of social interaction, and determine their relationship to faithful appropriation moves. As an example of this, the model will be revised and tested on the Familiarity appropriation move.

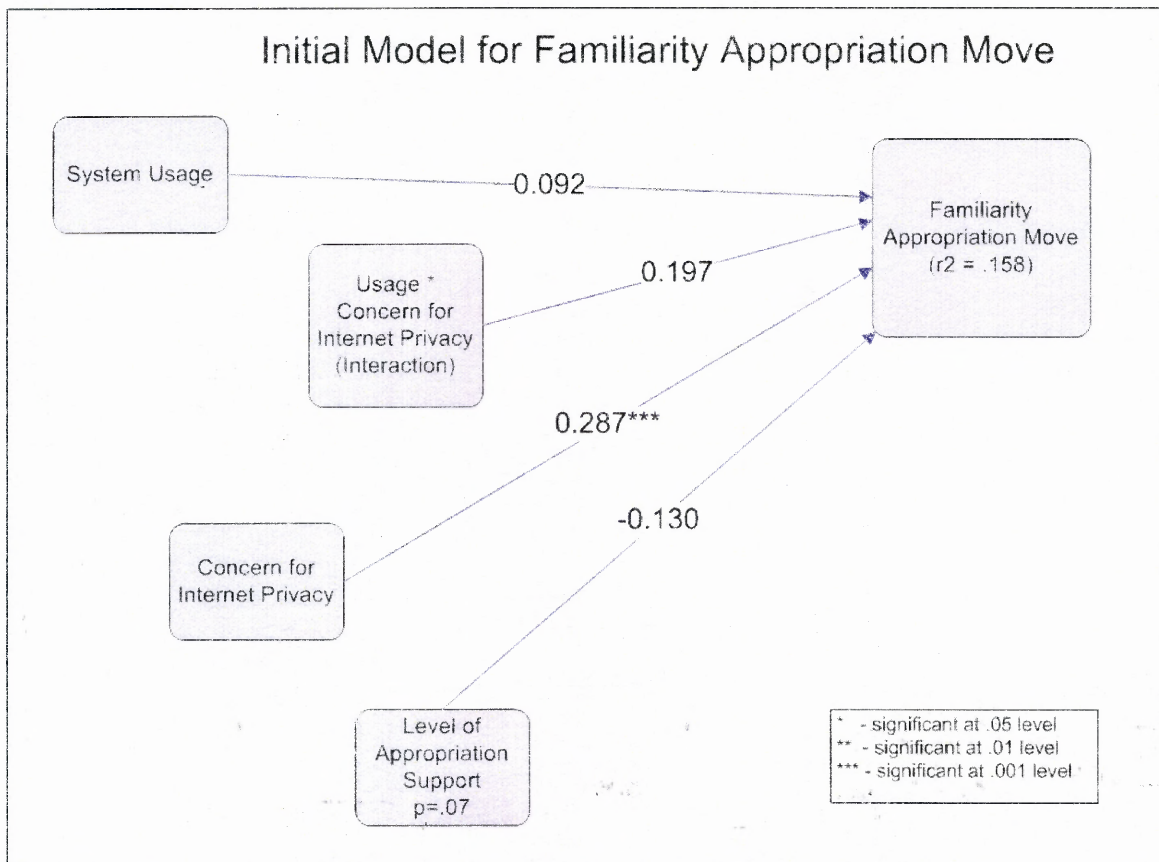


Figure 11.1 Initial model of Familiarity appropriation move.

Figure 11.1 shows the results for the initial model in terms of predicting the Familiarity appropriation move. The R-squared value is .158. There is one significant path, going from Concern for Internet Privacy, with a path weight of .287. The other paths are not significant. However, the path from Level of Appropriation Support is approaching significance, with a very surprising negative path weight. In other words, high levels of appropriation support lead to lower levels of Familiarity. The results obtained through PLS analysis are basically consistent with the findings revealed by the ANOVA analysis in Chapter 8.

11.2 Revisions to the Research Model

In order to represent the impact of social interaction on privacy management, the following indicators and constructs were added to the model. The question “Please indicate your opinion as to the overall value you place on the importance of protecting your privacy on [name of social networking site]” was added to the Concern for Internet Privacy Construct. A summary of results for this indicator can be found in Section 7.10.8.

A reflective construct labeled Distrust in Other Members was added. It includes three questions related to whether members express distrust with respect to other members. The construct was originally conceived of as a dependent variable with four indicators. A summary of results for these indicators can be found in Section 7.10.6. One indicator, Distrust1, was dropped from this analysis due to poor AVE results. A second construct was added, labeled Trust in the Site. This construct has two indicators, which measure the degree to which members trust the site’s intentions to provide privacy protection. A summary of results for these two indicators can be found in Section 7.10.9.

As these trust related constructs were added, interaction effects were tested. A significant interaction effect was found between Appropriation Support and Distrust. When the revised model was tested, it resulted in an increase from one to four significant paths, and an increase in R-squared from .158 to .211, an increase of 33%. The effect size of adding the trust constructs to the model is .067, about midway between a low and medium effect.

The four significant paths are as follows: Attitudes towards privacy has a positive path weight of 0.249 ($p < .001$), Level of Appropriation Support has a negative path weight of -0.179 ($p < .05$), Distrust has a positive path weight of .221 ($p < .001$), and the interaction between Appropriation Support and Distrust has a negative path weight of -0.145 ($p < .05$). The total effects are displayed in the Figure 11.2.

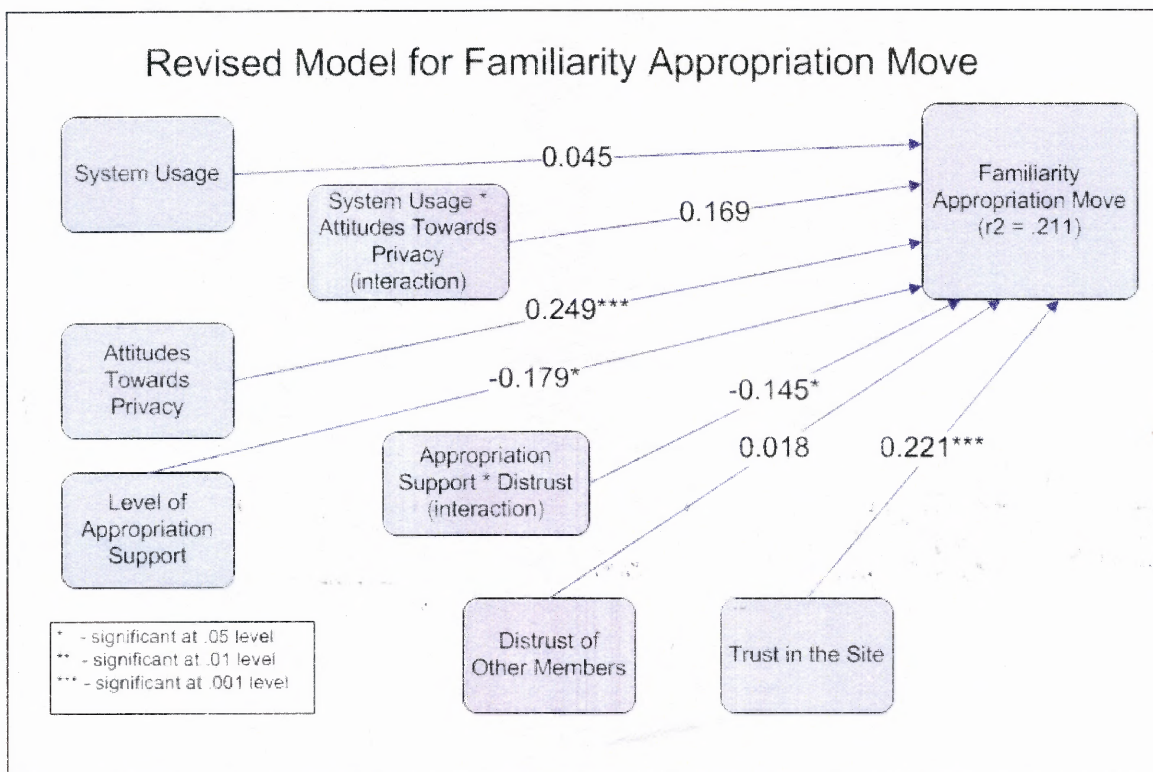


Figure 11.2 Revised Model for Familiarity Appropriation Move, adding two trust related constructs.

11.3 Validity Tests for Revised Model

The quality criteria for the revised model are summarized in Table 11.1. There are four reflective latent variables in this model, the dependent variable, Familiarity, and three independent variables, Attitudes Towards Privacy, Trust in the Site, and Distrust in Other Members. Each latent variable meets or exceeds the AVE threshold value of .50, which is a test of convergent validity. Each latent variable shows a composite reliability of .74 or higher, above the recommended threshold value of .7. Two of the variables, Familiarity and Distrust in Other Members, have a Cronbach's alpha value below .7. However, the measure for composite Reliability is considered to be a better test of reliability for models tested with PLS (Chin, 1998).

Table 11.1 Quality Criteria for Revised Familiarity Model

	AVE	Composite Reliability	R Square	Cronbach's Alpha
Familiarity	0.619	0.829	0.211	0.693
Attitudes Towards Privacy	0.587	0.895		0.861
Trust in the Site	0.792	0.883		0.767
Distrust in Other Members	0.514	0.742		0.643

None of the indicators are cross loading on any other construct. In addition, the test for predictive relevance (q^2) is positive, indicating the model does have predictive relevance.

Table 11.2 Test of Discriminant Validity for Revised Model

Correlation Matrix	Familiarity	Attitudes Towards Privacy	Trust in the Site	Distrust in Other Members
Familiarity	0.787			
Attitudes Towards Privacy	0.279	0.766		
Trust in the Site	0.244	0.146	0.890	
Distrust in Other Members	0.129	0.134	-0.158	0.717

Table 11.2 presents the results for the test of discriminant validity. Discriminant validity in a model is determined by whether the AVE of each construct is greater than the variance shared between the constructs (Chin, 1998). The numbers in bold on the diagonal in the table of is the square root of the AVE of each construct. Since all the correlation values for each construct are less than the square root of its AVE, then the revised model passes this test for discriminant validity.

11.4 Discussion of Revised Model

The negative and significant path weight for Appropriation Support signals that this indicator is being confounded by other conditions. By renaming this indicator as Facebook versus MySpace, rather than appropriation support, the results can be interpreted as follows.

Based on the negative path from Facebook to Familiarity, this says that members of Facebook do not make themselves familiar with privacy settings, as compared to members of MySpace. This can be explained one of two ways:

- The privacy management settings for Facebook are complex and confusing, and members do not feel comfortable using them (a few subjects indicated they found the settings confusing)
- The members of Facebook feel it is a “safe” site, and therefore they can depend on the site to protect their privacy and do not need to go to the effort of managing their privacy settings

Another way of saying this is that the degree of untrustworthy behavior is so pervasive in MySpace that it has driven members to use privacy management features. So the issue is what dangers do you face, rather than how well supported privacy management happens to be. This brings up the question as to why do these subjects

continue to use the site despite high levels of distrust? However, to answer that question, the study would need to include subjects who have left MySpace, and compare their results to those that have stayed. The population of this study is probably over-representative of those who can tolerate discomfort with online social interactions, because those who find that problematic have either left the site or never joined in the first place.

Looking at the path weights of the individual indicators, the interaction effect between Appropriation Support and Distrust with the highest level of significance and path weight is Distrust2, “There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy.” This interaction effect has a path weight of .833 and a T-statistic of 2.997 ($p < .01$).

Table 11.3 Results for the Distrust2 Indicator

Distrust2 There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy.									
	Familiarity Ranked	1	2	3	4	5	6	7	Total
Facebook	Low	1	6	4	11	8	7	9	46
	Medium	3	8	7	15	3	2	8	46
	High	0	1	2	5	0	3	3	14
	Total	4	15	13	31	11	12	20	106
MySpace	Low	2	0	0	7	4	5	18	36
	Medium	0	0	0	5	7	11	23	46
	High	1	0	0	3	3	9	17	33
	Total	3	0	0	15	14	25	58	115

In Table 11.3, the answers of Facebook versus MySpace members for Distrust2 are presented. The results show a stark difference between the two sites. A total of 58 members of MySpace choose the highest value (7), compared to 20 in Facebook. Of the 20 in Facebook who select 7 as their level for Distrust2, nine are in the lowest rank for

Familiarity, eight are in the middle rank, and only three are in the top rank. For the members of MySpace who selected 7 for the Distrust2 indicator, 17 out of 58 are in the highest rank for Familiarity, a much higher percentage (29% for MySpace versus 15% for Facebook).

The pattern is similar for levels 5 and 6 for Distrust2. Combining the results for levels 5, 6, and 7, 55% of Facebook subjects who answer 5, 6, or 7 to Distrust2 are in the lowest rank for Familiarity. This contrasts with MySpace, where only 27% of those who answer 5, 6, or 7 to Distrust2 are also in the lowest rank for Familiarity. The groups are 24 out of 43 for Facebook, versus 27 out of 97 for MySpace.

A more reasonable explanation for these results is that the level of appropriation support is not a driver for the level of Familiarity. Instead, it is the degree to which the behavior of others is perceived as a threat. Based on these results, the existence of untrustworthy profiles on Facebook is not seen as a threat, compared to MySpace. These results serve as an indirect indicator of members' overall perception of the social environment of Facebook versus MySpace. This finding is also confirmed by comments from subjects when comparing Facebook to MySpace:

- *“Facebook is great because it does not have the stigma that MySpace has. Many people who are generally against social websites will use Facebook. Facebook gives you options regarding privacy which make it easy to set up who sees what.”*
- *“I think [Facebook] is pretty good as is. I think it is a safer network than MySpace. MySpace has so many peoples accounts hacked into daily. I have not encountered a problem like this on Facebook.”*
- *“I have more confidence in [Facebook] than with MySpace.”*
- *“It seems to be a lot safer than MySpace (for now at least).”*

In the case of the Familiarity appropriation move, the addition of constructs related to perceptions of social interaction make the behavior within these sites easier to understand and model.

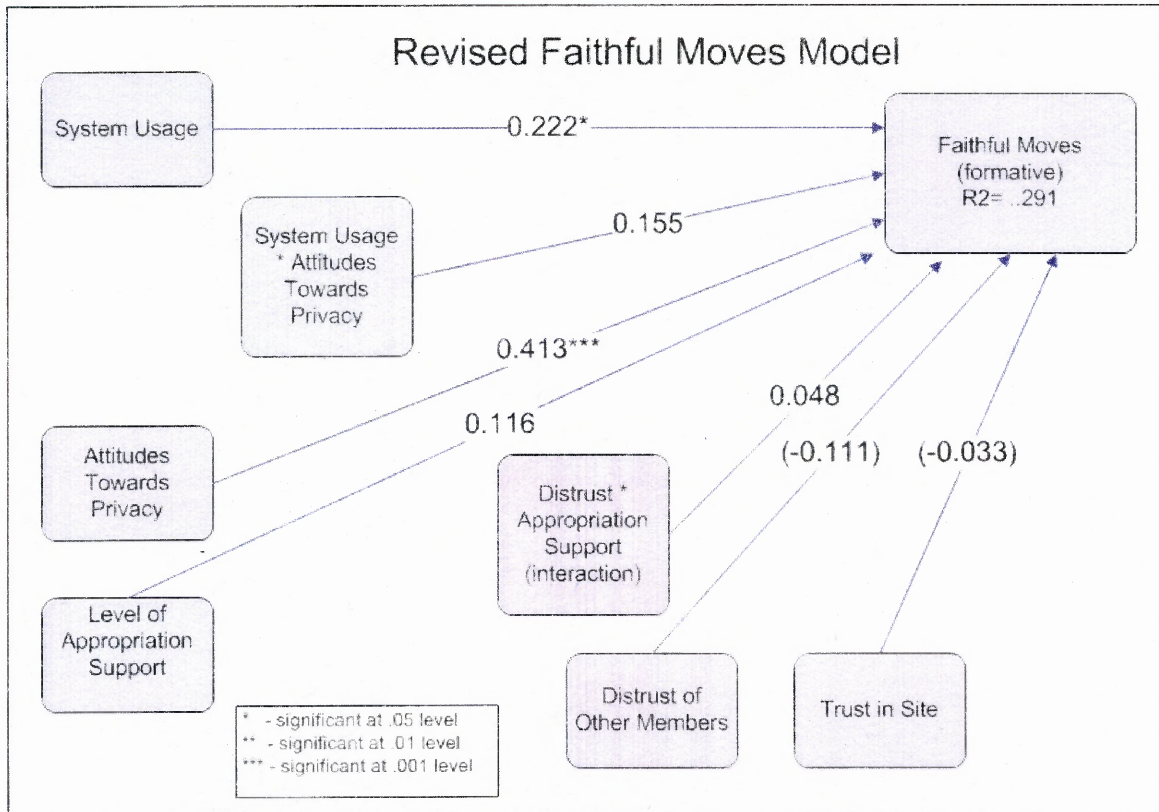


Figure 11.3 Revised model results as applied to Faithful appropriation moves.

However, when this model was applied to Faithful Moves (formative), there was a minimal improvement in R-squared (from .285 to .294). The results are summarized in Figure 11.3. There are only two significant paths, from System Usage, with a path weight of 0.222 ($p < .05$), and from Attitudes Towards Privacy, with a path weight of 0.413 ($p < .001$).

While the revised model passed all the recommended quality tests, the practical significance of adding these trust constructs to the full model is minimal. The findings

with respect to the Familiarity appropriation move shows promise, but clearly more theoretical development for modeling social context within an online community is needed. The next section presents an analysis of qualitative results in order to more clearly explain the findings of this research.

Table 11.4 Quality Measures for Revised Model Applied to Faithful Moves

Construct	AVE	Composite Reliability	R Square	Cronbach's Alpha
Faithful Appropriation Moves			0.294	
Attitudes Towards Privacy	0.590	0.896		0.861
Distrust of Other Members	0.565	0.792		0.643
Trust in Site	0.772	0.869		0.767

The model also indicates predictive relevance, with a q^2 statistic greater than zero. It also passed the test for discriminant validity, with the correlation matrix compared to the square root of the AVE for each construct, as described in Chin (1998). The results of these tests help to establish the credibility of the findings from this research, and justify the revision of the model to include constructs that represent perceptions of social interaction.

11.5 Identification of Privacy Management Strategies

An analysis of the free form responses collected in the survey resulted in the identification of a number of privacy management strategies that do not involve per se the explicit use of the settings made available within these two sites. For example, subjects will act to preserve their privacy by limiting contact information on their profile. This is especially the case for subjects from MySpace.

The most common strategy described can be labeled as “profile self editing,” or in other words self-filtering of information is to be shared. Here are comments that describe this strategy:

- *“I think [the level of privacy protection] is fine. In the end, **your privacy is up to you** [emphasis added]. If you only post what you want people to see, then privacy is not a problem.”*
- *“To be honest, I do not have any concerns. on my profile, I do not put any information about myself that people could use against me.”*
- *“Normally I post very little that will attribute to me with importance, it's usually trivial things and things most people can find out by getting to know me anyways.”*
- *“Its a great site...all social sites are great....its just how u use it. [emphasis added]..and how u choose to expose yourself to the internet.”*
- *“I don't want people knowing stuff about me that I don't want them to know - which is why I limit what I put on there. People should just be more careful [emphasis added].”*

Another strategy described is similar to the structure of secure systems, such as operating systems or defense environments. Secure systems are built with layers of protection. In the case of social networking use, this involves the creation of a “shell” profile with only bare bones contact information and no personal details. Here is how one subject describes this strategy:

“In terms of the questions about privacy, although I display ‘personal’ information, this information is outer cell of information which is insulated from my truly personal information. For instance the phone number listed is an auto-forward number that forwards to my real telephone. This can be disabled or specific calling numbers can be blocked. This allows me to provide contact information but informed that is controlled outside of Facebook. The same is true of my email address which forwards to my ‘real email account’ which is not listed. This provides a layer of insulation between me and others on Facebook while allowing me to use the contact tools for my benefit. Any other personal information listed is information that I would feel comfortable providing or is commonly available elsewhere with little effort.”

The use of a shell profile is evident within the population targeted for the Facebook target population. Of the 778 Facebook profiles identified for this study, 85 were very bare bones, with no picture, no links to friends, and nothing more than a name and perhaps an email address. Some of these are likely to be inactive rather than shell profiles, but Facebook, unlike MySpace, does not display the date of the most recent log in to the site, so it was not possible to determine if these were all inactive sites. However it is likely this set does include shell profiles, because unlike MySpace, Facebook does requires you to set up a profile in order to be able to access any content on the site.

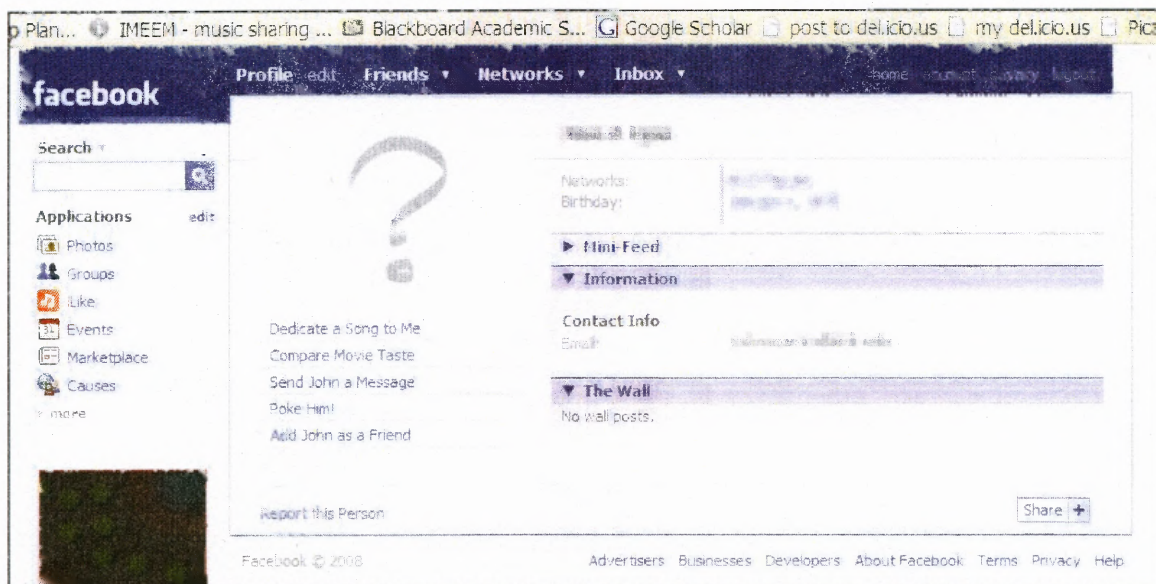


Figure 11.4 Example of a bare bones "shell" profile from Facebook.

The "self-edit" privacy strategy is also in evidence when subjects discuss their responses to privacy episodes. One subject said *"I found out my Facebook page was on a suspected sex offender's computer in another state last year (along with many other girls) which made me more cautious of what personal content I put on Facebook."* She reported that she did review her privacy settings after that incident but did not change them: *"They*

were already pretty high! At least I thought so.” Her primary action in response to this issue was to be more rigorous about what was revealed on her profile: “I removed a lot of personal information that I had put up there... I hadn't even thought of strangers being able to view my page without being my ‘friend’. It made me suspicious of the website.”

However, did this incident make her less active as a member of a social networking site? It seems not, because she reports visiting the site “Several times a week,” and also that her use of social networking sites is about the same as a year ago. In addition, her profile is visible to anyone who is also a member of the NJIT community. Her profile includes her relationship status, including a link to her partner’s page. It also includes 64 pictures, including several of her dressed in a Wonder Woman costume.

Subjects also expressed confusion as to exactly what information should be kept private: *“All the information provided by me for MySpace has been strictly voluntary since the beginning. I also never put any type of information where they can steal my identity such as social security number or any other relevant information. I am not worried about what I insert. Information can be easily taken from a phone book, other internet sites and in other means that are more dangerous than MySpace. Furthermore, I have chosen to write the information I felt was unimportant and that would be available by other means, and therefore I should not be worried. I am more worried about paying bills online than MySpace since I control what I want to insert there.”*

Does this suggest the only private data you may have is your social security number? This comment exposes a lack of precision in subjects’ conceptions of what exactly is private information. This concern over social security numbers was echoed by another subject’s discussion of their credit card information: *“When used properly the*

internet is a very safe place in my opinion. However anytime you enter your full name, address, phone numbers, credit card numbers, or whatever, you better know that you trust the website and that it is the website that it claims to be. If you don't trust in that judgment and still enter your information that's not what I would consider using the internet properly." Another agreed: *"Not really concerned since I haven't shared any info of value on MySpace, such as my phone#, SS#, credit card#, home address, real name, etc. Now if eBay or PayPal got hacked I'd be in big trouble."*

There was additional evidence of confusion as to what information can be made private, and what that really means: *"Also, I don't think (this may be ignorance) you can remove your email from your profile page."* (Not at all true, you can remove your email from your profile page). One Facebook subject said *"The privacy settings are way too complicated. Sometimes I am unsure if I have achieved what I wanted after doing some changes."* Another Facebook member complained that you *"can see far too much information by default on users. When they break up, when they post, etc."*

Especially with Facebook, it can be confusing as to the real visibility of your profile. One subject reported they had little or no privacy concern because *"I don't really have a concern because if I don't accept someone as a friend they can't look at my profile so it doesn't bother me."* Yet this subject's profile is public to members of the NJIT community, and it includes her full birthday, her instant messenger screen name, as well as access to her "wall," messages posted from Facebook members.

Subjects also expressed concern about future employers using the material found on these sites to rule out potential applicants. *"[I am concerned about] Employers getting on to see my profile and judging me based on the profile, which is why I have the privacy*

settings high. But I still have the concern.” Another reported the difficulty of *“keeping it accurate while still keeping it appropriate for future employers to view.”* The subject use of the word accurate relates to a concern for a recognizable profile, a profile that friends won’t perceive to be fake or exaggerated. So the tension here is apparent between personal accuracy and keeping a pristine image for future potential employers.

Another subject echoed a similar tension, saying his greatest concern was being able to *“Have fun, [yet be able to maintain] a professional image outside of the website.”*

Some subjects expressed confusion as to what information in their profile could be misinterpreted: *“I don't think there is much content in my MySpace that could be used against me....although now I'm starting to question that. Thanks! =).”*

Subjects were more likely to criticize the tone of other profiles rather than admit that their own behavior was at all risky. One subject complained about *“The exploitation of women - they practically whore themselves out to many willing strangers. It's unsafe and demeaning.”* There were also comments about *“under aged people saying they are over 21.”* And another subject complained about *“so many young girls letting the entire world see all of their personal information, as well as racy pictures. I don't need to see 14 year old girls in sexy outfits, and this makes an online predator's job much easier.”*

The issue of setting boundaries for acceptable social behavior was expressed in this comment: *“I like it to keep connected with friends, but some people put things up that are private and even illegal - maybe it isn't MySpace's job to censor people - maybe as a society we need to focus more on appropriate boundaries.”*

Subjects also expressed a lack of faith in the ability of privacy management to make a difference: One subject reported their *“17 year old cousin's MySpace account was*

hacked into and was filled with pornographic images, comments, and videos.” However, in response this subject did not even review their own privacy settings because *“It wouldn't make a difference.”* Another subject commented that *“I really don't trust the privacy protection in MySpace, hence I don't disclose any information I don't want public.”*

Consistent with this perspective that demonstrates a lack of faith in privacy management was a set of subjects who reported very high scores for the Familiarity appropriation move along with very low scores for the Use appropriation move. This means they report they are very familiar with privacy management, but do not use it.

Using a filter with the program SPSS, subjects were selected who scored high on the Familiar appropriation move (indicating they are very familiar with privacy management settings) and at the same time low on the Use appropriation move (indicating they do not use the privacy management settings). This resulted in a population of 17 subjects with the following characteristics:

- 2 subjects from Facebook and 15 from MySpace
- 2 Female and 15 Male subjects
- Mean age of 24.47, with a range from 18 to 35 (no significant difference)
- 9 undergraduates, 3 graduate students, and 5 not a student
- A significantly higher level of Distrust ($F=5.901$, $df=1$, $sig. = .016$)
- A significantly lower level of Faithfulness ($F=4.451$, $df = 1$, $sig. = .036$)
- Fairly active visitors to these sites, with 6 accessing the site at least every day, and 12 out of the 17 accessing the sites at least once a week
- 9 out of 17 are active on both sites

- 8 use social networking sites about the same as last year, 5 use the sites less, and 4 use them more frequently
- Higher levels (but not significant) of Internet Privacy concern
- Higher levels (but not significant) of One Sided Profile Browsing
- 3 out of the 17 reported a privacy incident within the past year

There are also subjects who report they chose Facebook over MySpace because of privacy issues. For example, one subject reported that “*Getting several random comments from random people has turned me away from MySpace to Facebook.*” Another said “*It's nice that Facebook [has] stayed a secure place. It's SO refreshing after MySpace has just turned into a complete spamfest.*”

Another element of the responses can be labeled as “Privacy Unconcerned.” These subjects state that if you want privacy then do not use these sites: “*I'm not sure why privacy is such an issue re: MySpace. If maintaining extreme privacy is a big concern to people they shouldn't use MySpace or they could use it without revealing any private information.*” The unspoken assumption for these subjects is that use of these sites waives any expectation of privacy.

11.6 Comparing Default Privacy Levels on Facebook Versus MySpace

An issue revealed through data analysis for this study is the confounding of the impact of technology to provide privacy management with the social experiences on the site.

A second confounding issue relates to default levels of privacy established by both sites. For the study design, the very same questions were asked of subjects for both sites. However, since the baseline privacy level for Facebook is higher than MySpace,

this throws off comparisons of the data. So even if a member of Facebook does not use or adjust their privacy settings, they may still have a higher absolute level of privacy compared to members of MySpace. This is especially apparent when you look at how many Facebook members use their real name compared to MySpace members. More than just a cultural issue of the site, it is a real indicator of the level of trust in Facebook to deliver privacy.

The implication in the research design is that use of privacy management means actively accessing that part of the site and making adjustments and personalizations. This has the result of giving a positive bias to responses from MySpace. So even if a subject chooses Facebook over MySpace due to privacy concerns, unless they actively engage in their privacy settings, their level of use will be below a MySpace member who uses privacy settings to block spam. Determining how to adjust for different default settings greatly complicates the interpretation of these results.

In addition, future work on this subject must explicitly consider the impact of behavior of other members on outcomes. In other words, social context was under represented in the original model. In addition to appropriation support, another issue to be evaluating is what steps these sites take to police the action of other members. Stronger control mechanisms on behavior (as found in Facebook) are also likely to lessen member's need to actively manage their privacy settings.

11.7 Comparing Groups by Use Profile

The results of this study showed that the number of subjects who are active on both sites is quite high. As a way of clarifying the contextual differences between these sites, an

analysis was conducted that split the results into three groups: those who only use Facebook, those who only use MySpace, and those who are active on both sites.

In order to conduct this analysis a new categorical variable was created. The new variable, Use Profile, has three possible values: FB (Facebook only), MY (MySpace only), and BOTH (uses both). Because PLS modeling software is based on regression analysis, this means that categorical values must be converted to dummy variables. The PLS package Smart-PLS was found to have difficulty calculating results for three way dummy variables. Therefore a PLS analysis comparing these groups, along with determining the best method for conducting a three way analysis, will be added to future research. For this condition, the results were analyzed using ANOVA.

The number of subjects for the Use Profile FB (Facebook only) is 76, for MY (MySpace only) it is 41, and for BOTH (uses both sites), n is equal to 105. ANOVA analysis was conducted with Use Profile as the independent variable against the following dependent variables: the Use appropriation move, the Familiarity appropriation move, Restricted Scope appropriation move, Unfaithfulness, Distrust of other members, and One Sided Profile Browsing.

First an analysis was conducted comparing FB only subjects to MY only subjects (subjects who used both were dropped). When comparing FB only to MY only, significant differences are found for the Use appropriation move and for Distrust. Although MY subjects have a slightly higher level for the Familiarity appropriation move compared to FB subjects, the differences are not significant. In addition there is a very strong result for Distrust. The results are summarized in Table 11.5.

Table 11.5 Comparing Groups Based on Use Profile

Comparison of FB versus MY Only						
Dependent Variables	Use Profile	Mean	dF	F	Sig.	Partial Eta Squared
Familiarity appropriation move	FB	15.2632	1	0.276	0.600	0.002
	MY	15.6829				
Restricted Scope appropriation move	FB	3.7354	1	2.114	0.149	0.018
	MY	3.4703				
Use appropriation move	FB	2.6175	1	4.514	0.036	0.038
	MY	2.2534				
Unfaithfulness	FB	15.9868	1	1.844	0.177	0.016
	MY	14.0732				
One Sided Profile Browsing	FB	0.3553	1	1.311	0.255	0.011
	MY	0.2439				
Distrust	FB	15.0526	1	41.039	0.000	0.263
	MY	21.3902				

For the Use appropriation move, FB subjects had a significantly higher result ($F = 4.514$, $\text{sig.} = .03$). However, the effect size is rather weak (Partial Eta Squared = .038). The MY subjects have a significantly higher level of Distrust ($F = 41.039$, $\text{sig.} < .001$), with a medium effect size (Partial Eta Squared = 0.263). Note that the differences for the Familiarity appropriation move are not significant. Compare this outcome with the initial analysis, which found that results for Familiarity were significant in the opposite of the predicted direction (see Section 9.5). These results provide evidence that active memberships on both sites may be confounding results.

A second analysis was conducted comparing all three groups at once. In this case, the only variable that shows significant differences is Distrust. However, both the Use appropriation move and Unfaithfulness have results approaching significance ($p = .092$ and $p = .096$, respectively). The results for all three groups are summarized in Table 11.6.

Table 11.6 Comparing All Groups Based on Use Profile

Use Profile Compared for All Three Groups					
	Use Profile	Mean	F	Sig.	Partial Eta Squared
Familiarity appropriation move	BOTH	16.2952	1.246	0.290	0.011
	FB	15.2632			
	MY	15.6829			
Restricted Scope appropriation move	BOTH	3.5869	1.119	0.329	0.010
	FB	3.7354			
	MY	3.4703			
Use appropriation move	BOTH	2.5792	2.416	0.092	0.022
	FB	2.6175			
	MY	2.2534			
Unfaithfulness	BOTH	13.5905	2.367	0.096	0.021
	FB	15.9868			
	MY	14.0732			
One Sided Profile Browsing	BOTH	0.2952	0.764	0.467	0.007
	FB	0.3553			
	MY	0.2439			
Distrust	BOTH	19.0667	21.568	0.000	0.165
	FB	15.0526			
	MY	21.3902			

When comparing three groups based on Distrust, MY subjects had the highest level, FB subjects had the lowest level, and BOTH subjects were in the middle. This difference was significant ($F = 21.568$, $\text{sig.} < .001$), with a low-medium effect size (Partial Eta Squared = 0.165). Two other measures had results that were approaching significance. For the Use appropriation move, FB subjects had the highest result, MY subjects had the lowest result, and BOTH subjects were in the middle ($F = 2.416$, $\text{sig.} = .092$).

For the Unfaithfulness construct, FB subjects showed the highest level of Unfaithfulness, MY the next highest, with BOTH at the lowest level ($F = 2.367$, $\text{sig.} = 0.096$). Because these questions are reverse scored, these results should be interpreted in

the following way. Subjects who match the BOTH condition express the highest level of faithfulness, and FB subjects express the lowest. Although this result is not significant, these findings suggest there are differences between these three groups of subjects that justify further study.

CHAPTER 12

SUMMARY AND CONCLUSIONS

Millions of people have joined social networking sites, using them to maintain closer contact with far flung friends and family. The nature of this use is often quite poignant. MySpace profiles of soldiers killed in Iraq are frequently preserved by family members as shrines for the dead (Hunt, 2007). Profiles also serve as an outlet for self-expression and personal multi-media publication (Lange, 2007; Liu, 2007).

The general public's embrace of social networking has far outstripped the ability of academic researchers to model and understand the implications of their use. In particular, fundamental social axioms as to the treatment of private information and the boundaries between public and private have been trampled and discarded. Social researchers have tried to explain this behavior by describing a new type of mediated self-presentation labeled as "publicness," (Lange, 2007). Publicness refers to self-presentation using a public forum. Lange found that users crafted their performances for private interchange within the fully public forum of YouTube. Just as people use personal dialects and code words to carry on private conversations in a public space, so a performance within a public mediated space can be crafted in such a way so that it only makes sense for a private audience.

While publicness gives the performer some measure of privacy, it does not offer any protection against mis-interpretations or discovery by completely unintended audiences. Social networking sites have been harshly criticized for their inability to provide rigorous privacy protection, especially for children. These sites want to improve how they protect privacy, but it is not well understood how members use the tools already

in place. This leads to the following research question: how do members of social networking sites use the privacy management features built into the site to protect their privacy?

12.1 Development of The Theoretical Model

Two important ideas were drivers of the research model. One is that managing privacy is cognitively complex, especially within online settings where feedback on self-presentation is absent or diluted. The second is that privacy management within social networking sites could best be understood by looking at user behavior from a socio-technical systems perspective.

A key part of social networking sites is the opportunity to create a persistent digital identity that can connect you to existing and new friends. The development of a persistent digital identity is both a chance for self expression and a dangerous opportunity for privacy invasion. How can these conflicts be resolved? How do social factors and technical design influence the resolution of this conflict? How do individuals appropriate technology in order to present attractive self presentations and protect privacy?

Consideration of these questions led to the development of the Social Software Performance Model, which is an extension of the Fit Appropriation Model (Dennis et al., 2001). A central assumption of this research is that design of effective socio-technical systems requires both understanding how technology supports tasks that complete system goals, and understanding how technology can sustain the social processes involved in completing those tasks.

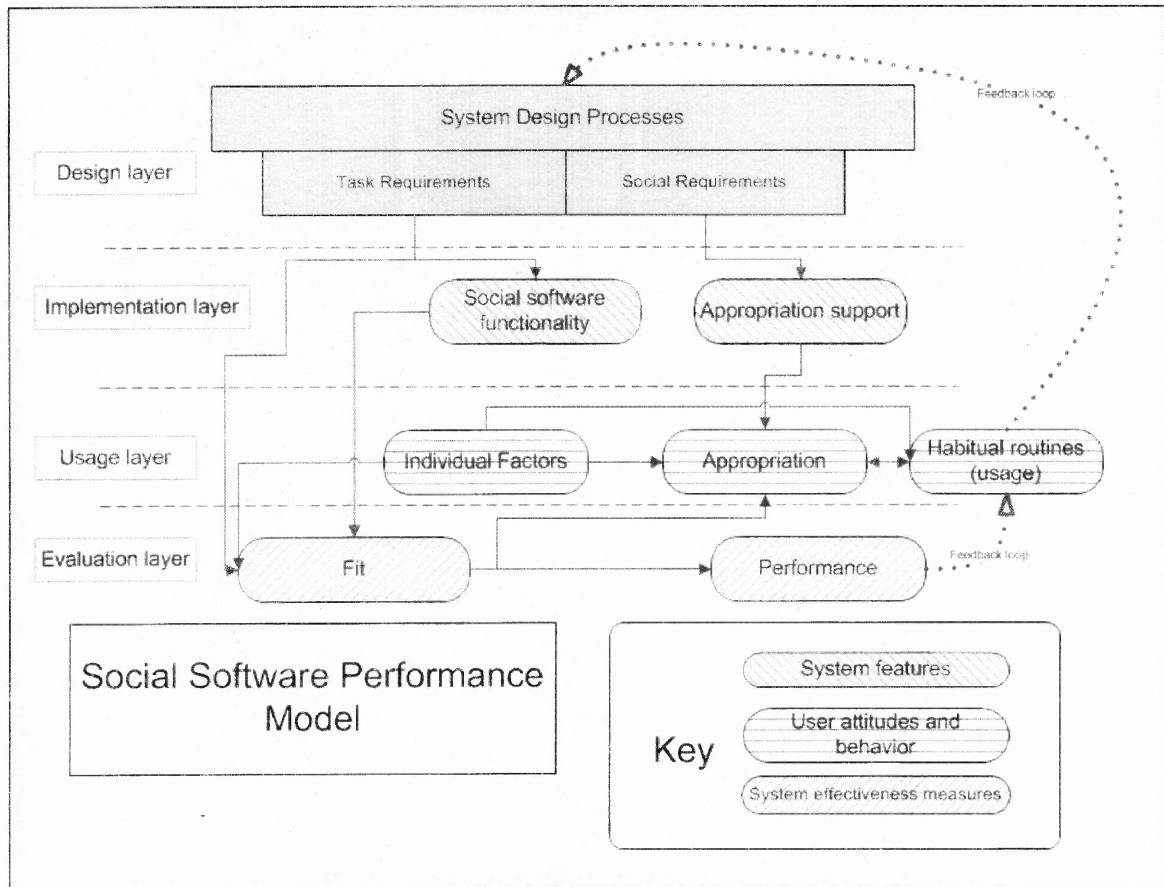


Figure 12.1 Conceptual Model: Social Software Performance Model.

Appropriation is the process by which people apply and adapt technology to their tasks. Using the terminology of Adaptive Structuration Theory (DeSanctis & Poole, 1991; DeSanctis & Poole, 1994), users faithfully appropriate the technology when they use it in compliance with what DeSanctis and Poole call the spirit of the technology. The spirit is the general values for the technology. If the technology is used in a manner not consistent with its spirit, this is referred to as unfaithful appropriation (Dennis et al., 2001). Appropriation support refers to specific design choices that intend to encourage faithful appropriation.

This leads to the focus of this research, which is an analysis of appropriation of privacy management within social networking sites. Building on the taxonomy of

appropriation as presented in Adaptive Structuration Theory (DeSanctis & Poole, 1994), constructs representing appropriation of privacy management were developed. This includes three faithful appropriation moves: the Use appropriation move, the Familiarity appropriation move, and the Restricted Scope appropriation move. One unfaithful appropriation move was developed, which is One Sided Profile Browsing.

Using these representations of appropriation, factors hypothesized to impact appropriation of privacy management were tested. The three factors hypothesized to influence appropriation are the degree of appropriation support, the level of concern for Internet privacy, and level of activity or use of these sites.

It was hypothesized the members of a social networking site with high levels of appropriation support will have more faithful appropriation of privacy management compared to members of a site with low levels of appropriation support. It was hypothesized that members with a high degree of concern for Internet privacy will have more faithful appropriation of privacy management compared to members with low levels of concern for Internet privacy. It was hypothesized that members who are more active users of these sites will have more faithful appropriation of privacy management compared to members who are less active. One interaction effect was hypothesized, which is that for members with high usage, those members with high Internet privacy concerns will have less faithful appropriation compared to members with low Internet privacy concern. The specific hypotheses and the research results are summarized in Table 12.1.

The primary goal of this research study was to understand how appropriation support impacts privacy management within social networking sites. To answer this

question, a survey was conducted using subjects from two extremely popular social networking sites, MySpace and Facebook. The subjects were recruited from the populations of students, faculty, staff, and alumni of NJIT. Measures that captured data on privacy management use were constructed based on Adaptive Structuration Theory. The results were then used to analyze the nature of privacy management use with these sites. The results of the study are summarized in the next section.

12.2 Summary of Findings

The survey was administered in November and December of 2007. A total of 222 subjects completed a valid response to the survey, 107 completing the Facebook survey and 115 completing the MySpace survey. There were 160 male subjects and 62 female subjects. The breakdown of gender between the two sites is similar, with 30 female and 77 male Facebook subjects and 32 female and 82 male MySpace subjects.

The ages of the subjects ranged from 18 to 69. The mean value is 24.53, the median is 23, and the mode is 22. The largest group of subjects was made up of undergraduates, with 58 from Facebook and 55 from MySpace. MySpace subjects were more likely to be non-students compared to Facebook. The ethnicity of the subjects is diverse, as reflecting the general population of NJIT. However, there is a noticeably higher percentage of Asian Facebook subjects, and a higher percentage of MySpace Hispanic subjects. This distribution has also been noted by other researchers (boyd & Ellison, 2007; Hargittai, 2007).

As found in earlier pilot studies, these subjects report quite active use of social networking sites. 45 Facebook and 39 MySpace subjects use the site every day or several

times a day, and another 47 Facebook and 47 MySpace subjects use the site at least one a week. Only about 18% (42 out of 222) use the site infrequently (once in a while). There is no significant difference in the frequency of use when comparing Facebook subjects to MySpace subjects.

The survey contained questions related to attitudes towards privacy, specifically a five item Concern for Internet Privacy scale that has been used in prior pilot studies. The responses to these questions are skewed towards the high end. In other words, out of a seven point scale, the mean for each of the questions is a full point above the midpoint of four out of seven. In prior pilot studies, the results were also skewed to the high end.

The survey contained measures for three examples of Faithful appropriation moves: The Use appropriation move, the Familiarity appropriation move, and the Restricted Scope appropriation move.

Use appropriation move consists of indicators that measure the extent to which members report actual use of privacy management. The means for these indicators were all around the midpoint, i.e., four out of seven. There were no significant differences found on these indicators when comparing Facebook subjects to MySpace subjects.

Familiarity appropriation move is made up of indicators that measure the extent to which members are familiar with what privacy management settings are available. When compared to the Use appropriation move measures, the means for Familiarity are at least a full point higher than the means for the Use measures. Significant differences were found between the responses from Facebook and MySpace subjects on two of the Familiarity indicators. However, the difference was found to be opposite of the predicted direction. In other words, instead of a higher level of Familiarity in the site with higher

appropriation support, MySpace has a higher level of Familiarity despite a lower level of appropriation support. This was one of the most surprising and thought provoking results of this research.

The Restricted Scope appropriation move is a measure of whether members consciously limit the scope of their online social network to only contain people they know and trust from their offline contacts. The results for the measures for the Restricted Scope appropriation move show a greater level of variance compared to the Use and Familiarity move. Facebook subjects are significantly more likely to refrain from contacting strangers compared to MySpace members. However, this is only true in general terms, because for both groups, the most frequent response for both populations was 7, indicating strongly agreeing that they do restrict the scope of their online social network.

The survey included five indicators from a previously validated scale, the Faithfulness of Appropriation scale (Chin et al., 1997). This scale was adapted to apply to privacy management use. The responses to these questions skew very strongly towards faithfulness. No significant differences were found in the answers given by Facebook subjects versus MySpace subjects.

The survey included four indicators that measured the degree of distrust subjects expressed with regard to the behavior of others on the site. The differences between Facebook and MySpace were the most extreme of all the results collected from this survey. MySpace subjects report a highly significant, substantially greater amount of distrust towards other members of the site. The MySpace scores are at least a full point

higher for three out of four indicators, and for the fourth the difference is over two full points.

The survey included several open ended questions that enabled subjects to describe the benefit they receive and the concerns they have with respect to use of social networking sites. Another question asked them to give their opinion as the overall effectiveness of privacy management.

What was quite striking about the results was how many of the subjects took time to answer open ended questions. In prior pilot studies conducted, the level of participation in open ended questions was much lower, about 50% compared to well over 90% for this survey.

When describing the benefits of use, the subjects were very enthusiastic. They described in detail how these sites enable them to stay connected to old friends. *“I would have to say that the most positive benefit is meeting people in my country that I fell out of touch with, even family members and for me that's something positive.”* Stress from hectic schedules was mediated by the ability to still stay in touch: *“Staying in contact with people I do not get to see on a regular basis as a result of being so busy.”*

Overcoming social disruptions suffered by those in the military was mentioned: *“Being able to stay in contact with my friend, in Cuba. He's in the Navy and contacting him by phone is a bit pricey.”* One subject specifically mentioned how disruptive being overseas was for his social life, and how MySpace eased his transition back to his friends: *“I am currently in the military, so I move/travel a lot. I left a lot of friends back at home and it allows them to track my progress, message me, and know when I am coming home. Also, I find that people from elementary school are coming out of the woodworks now*

and it allows for a very comfortable, low stress way of getting back in touch with long lost friends or flames.”

When asked to describe their greatest concern, many expressed anxiety about the use of these sites by children. Others specifically addressed the disturbing behavior of other members: *“Random people that I don't know would message me asking me very personal questions that I did not feel comfortable answering.”* Other members were described using the words creepy, weird, and strange. Their behavior was described as obsessive and harassing. Many described being stalked through these sites, and how uncomfortable this made them feel. While many listed some very general concerns (“privacy,” “identity theft”), subjects did describe situations that indicate anti-social behavior within these sites is a serious problem.

Using the data collected, the constructs of interest were analyzed using factor analysis methods as recommended by (Hair et al., 2006). The indicators were measured using Principal Component Analysis. This resulted in seven factors being identified, explaining 66.98% of the variance.

Next a rotated solution was attempted to clarify loadings. Two indicators were dropped because they exhibited split loadings on two factors. All remaining indicators have a factor loading of $\pm .50$ or above. The factors that were identified are the following:

- Concern for Internet Privacy – Independent variable (five indicators)
- Use appropriation move – Dependent variable (four indicators)
- Unfaithfulness – Dependent variable (five indicators)
- Familiarity appropriation move – Dependent variable (three indicators)
- Restricted Scope appropriation move – Dependent variable (three indicators)

- Distrust – Independent variable (four indicators)
- Faithfulness with System Spirit – Dependent variable (two indicators)

The evaluation of hypotheses was first conducted using ANOVA based testing, using the statistical package SPSS. A subsequent analysis was then conducted using the analysis tool Smart-PLS. The results of hypothesis testing are summarized in the Table 12.1.

Of the 12 hypotheses, three were supported by both ANOVA and PLS, three were partially supported, and six were not supported. In terms of evaluating the overall results, the hypotheses related to the dependent variable Faithful Appropriation Moves had the strongest results. This includes H1, H4, and H7. The PLS analysis for Faithful Appropriation Moves results in an R-squared value of .285 (see Figure 12.1 below).

The next best results were for the Faithfulness construct. This includes H6, with concern for privacy as the independent variable, and H9, with system usage as the independent variable. The PLS analysis of Faithfulness resulted in an R-Squared of 0.131.

The weakest results were for hypotheses related to predicting unfaithful moves. The hypotheses H2, H5, and H8 were not supported. There were also problems with the indicators included for unfaithful moves. In particular, the indicators for the Rejection Appropriation Move loaded on three factors (for a more detailed description see Section 9.3). The PLS analysis resulted in a low R-Squared of .083 for the unfaithful move One Sided Profile Browsing.

Table 12.1 Summary of Hypothesis Tests

Hypothesis	ANOVA Result	PLS Result
H1: Members of sites with a high level of appropriation support (Facebook) will have more faithful appropriation moves compared to members of sites with a low level of appropriation support (MySpace).	Partially supported , for Use appropriation move only	Not supported
H2. Members of sites with a high level of appropriation support (Facebook) will have less ironic (unfaithful) appropriation moves compared to members of sites with a low level of appropriation support (MySpace).	Not supported	Not supported
H3. Members of sites with a high level of appropriation support (Facebook) will report more faithfulness compared to members of sites with a low level of appropriation support (MySpace)..	Not supported	Not supported
H4. Members with high levels of Internet privacy concern will have more faithful appropriation moves compared to members with low levels of privacy concern.	Supported	Supported
H5. Members with high levels of Internet privacy concern will have less ironic appropriation moves compared to members with low levels of privacy concern.	Not supported	Not supported
H6. Members with high levels of Internet privacy concern will report more faithfulness compared to members with low levels of privacy concern.	Supported	Supported
H7. Members with high levels of usage will have more faithful appropriation moves compared to members with low usage.	Not supported*	Supported*
H8. Members with high levels of usage will have less ironic appropriation moves compared to members with low usage.	Not supported	Not supported
H9. Members with high levels of usage will report more faithfulness compared to members with low usage.	Supported	Supported
H10. For members with high usage, those members with high Internet privacy concerns will have less faithful appropriation moves compared to members with low Internet privacy concern.	Partially supported	Not supported
H11. For members with high usage, those members with high Internet privacy concerns will have more unfaithful appropriation moves compared to members with low Internet privacy concern.	Not supported	Not supported
H12. For members with high usage, those members with high Internet privacy concerns will report less faithfulness compared to members with low Internet privacy concern.	Not supported	Not supported
* For ANOVA analysis, a single binary indicator of High Use for hypothesis test. For PLS analysis, High Use and Using Both Sites were combined into a formative construct representing Overall System Usage.		

With respect to the independent variables, the hypotheses for privacy concern had the strongest results. This includes H4 and H6. In addition, the interaction effect combining concern with privacy with system usage (hypothesis H10) in order to predict unfaithful moves was supported by ANOVA analysis. Even though PLS did not find significance for this hypothesis, these results should be interpreted with caution. When compared to regression based analysis, PLS has been found to underestimate the significance of interaction effects (Goodhue, Lewis, & Thompson, 2007).

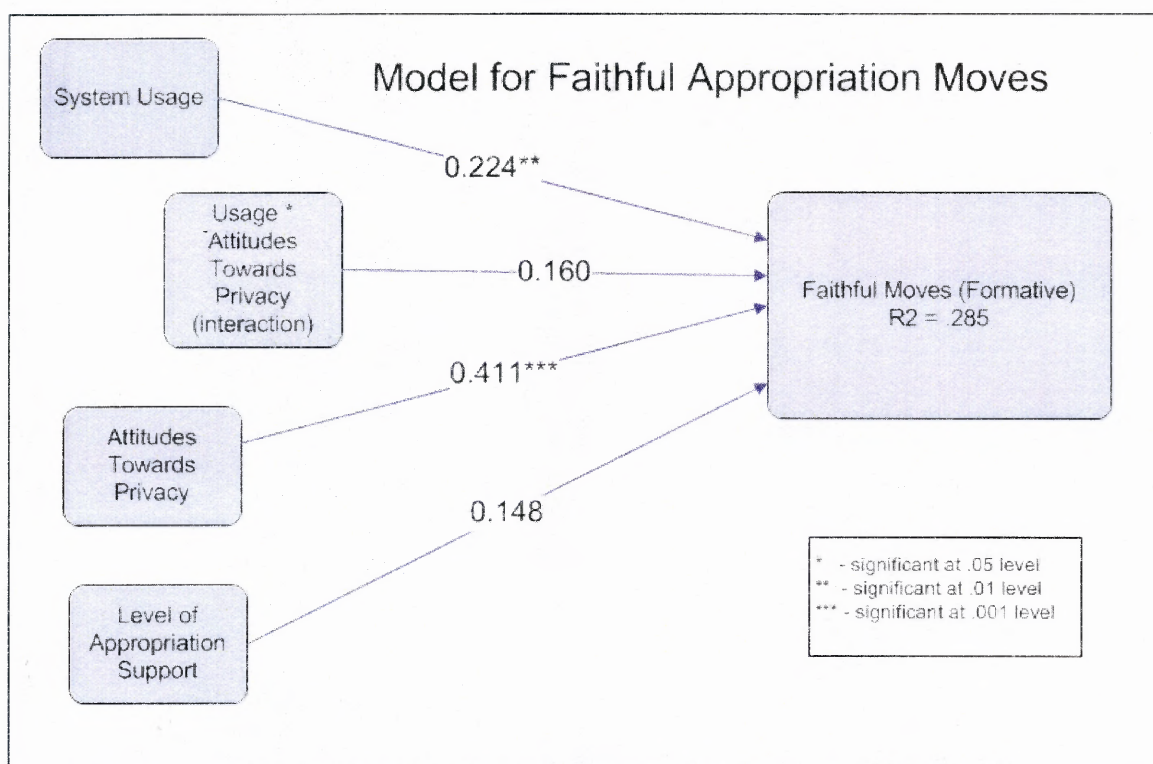


Figure 12.2 Results for PLS Analysis of Faithful Appropriation Moves

In summary, the strongest results of this study are that attitudes towards privacy and overall level of usage are reliable predictors of faithful appropriation moves. This can be seen clearly in Figure 12.2. System Usage has a path weight of .224, with a

significance level of $p < .01$. Attitudes towards privacy has a path weight of .441, with a significance level of $p < .001$. The model tested explains about 28% of the variance.

The independent variable level of appropriation support had very weak results. It was not found to be connected to faithful use. In one puzzling result, higher appropriation support was found to be significantly related to lower Familiarity with privacy management settings. A subsequent PLS analysis found the measure for appropriation support was a de facto stand-in for the social context of use. Once constructs were added to the model that represented measures of trust, the situation became clearer.

In order to improve the overall understanding of this exploratory research, data analysis was conducted using both ANOVA and PLS. This resulted in different outcomes for three different hypotheses: H1, H7, and H10. This leads to a consideration of possible reasons for different outcomes.

Hypothesis H1 predicts that high levels of appropriation support will lead to higher levels of faithful appropriation moves. For the ANOVA analysis, three separate tests were conducted, one for each appropriation move, Use, Familiarity, and Restricted Scope. Using ANOVA, H1 was only supported for one move, the Use appropriation move. For the PLS analysis, these three moves were combined into a formative construct, so the test for H1 evaluated all three moves at once and returned results that did not support the hypothesis. The differences in outcomes for H1 may be related to the fact that the ANOVA analysis was conducted separately for each move, whereas in the PLS analysis the three moves were combined into one construct.

Hypothesis H7 predicted that members with high levels of usage would display more faithful appropriation moves compared to members with low levels of usage. The

results of the PLS analysis supported H7, while the results of ANOVA did not. However, the measurement of the independent variable Usage is different for the ANOVA analysis compared to PLS. For the ANOVA analysis, Usage is a single binary variable. PLS allows some additional flexibility in modeling multi-dimensional constructs such as usage. For the PLS analysis, usage was operationalized as a combination of high use plus whether the members were active members on both sites. This variation is a possible explanation for the difference in outcomes.

Hypothesis H10 is partially supported by the ANOVA analysis, and is not supported by PLS. This hypothesis predicts an interaction effect between concern for Internet privacy and high use. A comparison of outcomes for ANOVA versus PLS has found that in some conditions, PLS is not as powerful as ANOVA in identifying interaction effects (Goodhue et al., 2007). This may be the cause of the different outcomes for H10.

12.3 Implications for Design

System designers must acknowledge the cognitive complexity of online privacy management. People learn offline privacy management through a lifetime of socialization. This knowledge is embedded as a social structure. According to Giddens, this means people can act out the structure even though they may not be able to explain it (Giddens, 1984). Privacy management offline is at the level of tacit knowledge. Because people do it “automatically,” it seems simple. In fact it is quite complex (Petronio, 2002).

Offline privacy management is supported by a lifetime of socialization into structures of privacy management (Giddens, 1984; Goffman, 1959; Lessig, 1998;

Petronio, 2002). Online privacy management is *at least* as complex as offline privacy management, and the evidence uncovered by this research suggest it is *much more* complex. Support for this conclusion comes from the fact that this study found no evidence of any established online privacy management structures, other than the assumption that nothing is private online.

The complexity of online privacy management is derived from a number of issues. The mediating effect of technology makes the audience for privacy revelations less apparent. It is the existence of the audience and their reactions that Goffman argues is the driver for self-presentation (Goffman, 1959). The conception of privacy from the information privacy perspective results in an implementation of privacy management as a set of individually controlled settings. This is contrary to Communication Privacy Management theory, which argues that people manage privacy by negotiating privacy boundaries between dyads and groups (Petronio, 2002).

Another problem is an HCI issue. When members adjust their privacy settings, they receive no feedback as to the consequences of their actions. They may think they have improved their privacy, but they have no way to know for sure. As one subject explained, *“The privacy settings are way too complicated. Sometimes I am unsure if I have achieved what I wanted after doing some changes.”*

Within system design, the term non-functional requirement refers to a quality or property of a system, used to judge its overall performance. This term can be explained in contrast to functional requirements, which describe exactly what tasks the system will perform. Examples of non-functional requirements include usability and security. A

system that does not deliver its non-functional requirements is more likely to fail or not be effective.

As new social software is created, designer must think of privacy as a non-functional system level requirement, rather than as collection of access settings to be managed by individual members. This moves privacy from an individual consideration to the level of a structural component of a system. In other words, privacy needs to belong to an online space, not be a collection of settings attached to each individual member.

As this study has shown, privacy in both Facebook and MySpace is defined from a functional perspective. In other words, “privacy” is primarily implemented as a choice for members, and members can choose what level of privacy they want for various parts of their profile.

For offline social spaces, privacy is signaled by physical characteristics: low lighting, enclosed spaces, and relative isolation from others. People who want to conduct a private conversation can recognize the privacy levels of an offline space based on physical properties. Online, the privacy is not signaled by the inherent properties of the online social space in any clear way, except for the common assumption that nothing is private.

The impact of this mismatch with respect to privacy online can be seen in an analysis of how the subjects of this study responded when they themselves encountered an issue with privacy. As described in chapter eight, out of 222 subjects, 19%, or nearly one in five, reported suffering a personal incident with respect to privacy within the past year. This includes 16 out of 107 Facebook subjects (15%) and 26 out of 115 MySpace subjects (23%), for a total of 42. Yet out of these 42, more than half said they did not

review their privacy settings in response (22 out of 42), nor did they make any adjustments to their settings (23 out of 42).

Why not? Why don't members, in response to a privacy incident, make a more concerted effort to use privacy management tools within social networking sites? This provides clear evidence that privacy management as it exists does not fit what is needed.

Instead, the evidence collected by this research indicates members use non-technical strategies to protect their privacy, such as self-editing ("I only post what I want others to see") and selective deceit (fake names and fake pictures). There is little evidence that members depend to any great extent on privacy management features. Instead, they adjust their behavior to the site in order to manage their privacy.

The conclusions to be drawn from these results are that privacy cannot be designed as group of settings that must be individually adjusted as if privacy was the same as a preference for a certain font or text color.

Research does show that social software influences the structure of social spaces and the development of norms of use (Humphreys, 2007). Just as offline social attitudes with respect to privacy have evolved over time, so must online conceptions of privacy evolve. This will require a more concerted effort to build privacy into the structure of social software, so that privacy is as apparent for online social spaces as the privacy levels of offline social spaces. This will require the conceptualization of privacy as a non-functional requirement that is pervasive within the structure of the social software system.

12.4 Re-evaluation of The Social Software Performance Model

This research model is based on an extension of the Fit Appropriation Model. Dennis et al. show that for socio-technical systems, having fit without appropriation support can lead to negative outcomes (Dennis & Garfield, 2003; Dennis et al., 2001). The primary goal of this research study was to understand how appropriation support impacts privacy management within social networking sites. By looking at two sites, one with a high level of appropriation support, and one with a low level of appropriation support, the expectation was there would be a difference in outcomes. The results, however, show that appropriation support has very little effect on outcomes. For example, when examining the impact of the model on unfaithful appropriation moves, the path weight from appropriation support is a miniscule 0.008 (see Figure 10.3).

There are three possible explanations for this. One is that appropriation support is not a factor. This is certainly an acceptable conclusion, however evidence exists that suggests other possibilities. The second is that the fit between social requirements for privacy and the implementation of privacy management functions is poor. So if there is poor fit, it does not really matter how wonderful appropriation support happens to be. There is evidence that online privacy is much more complex than designers of these systems have considered. This seems like a rich area for future research, but answering that question is beyond the scope of this dissertation.

The third explanation is that the behavior exhibited by others on these sites is a factor that determines privacy management, as described in Section 11.4. This research does provide evidence that social context influences outcomes, a perspective consistent

with information systems theory. Using this insight to reconsider the Social Software Performance Model, this leads to the following revisions to the model.

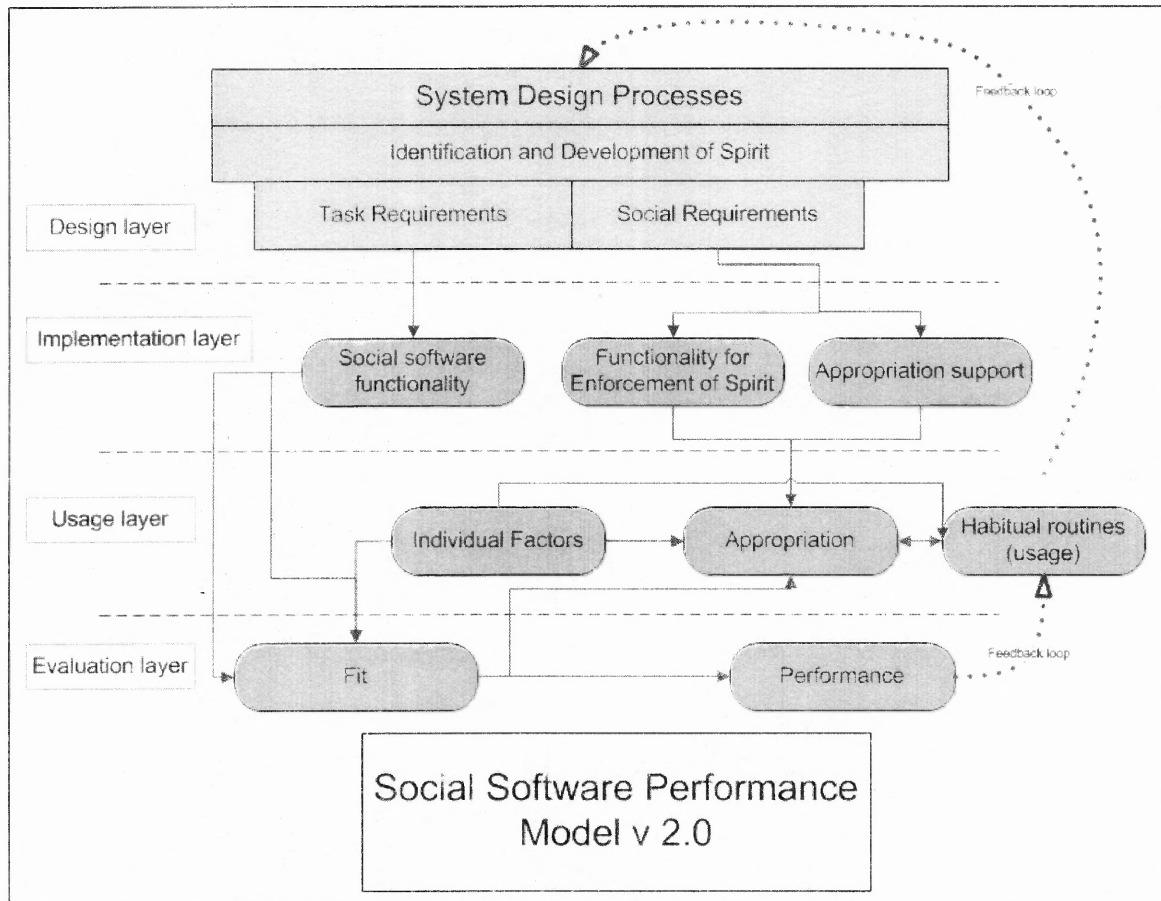


Figure 12.3 Social Software Performance Model, v. 2.0.

Designers of social software must be able to develop systems that can manage social interaction, in order to minimize negative impacts of other members' behavior. The importance of this requirement can be illustrated by the consequences of inadequate attempts to control spam (Whitworth & Whitworth, 2004). The results of this study suggest that an understanding of social context should infuse the design process. Therefore, applying the terminology of Adaptive Structuration Theory, a rigorous consideration and development of the Spirit of the system should be an important part of

the design process. As a result, the block labeled “Identification and Development of Spirit” has been added to the model (see Figure 12.3).

In the revised model, Spirit informs both the development of task requirements and social requirements. The results of this research show that the system not only must encourage faithful appropriation, but also include functionality to enforce norms and social expectations. To accomplish this, another construct labeled “Functionality for Enforcement of Spirit” has been added to the implementation layer. This construct is related to Giddens’ structures of legitimation, (Giddens, 1984). According to Giddens, these structures of legitimation define norms, along with sanctions related to transgressions. This construct embodies policy decisions and functional implementations that have the intent to manage social interaction, and control the impact of one member’s actions on others. It works in concert with appropriation support to encourage faithful privacy management, but it is a separate construct that captures how socio-technical systems enforce behavioral norms.

The data collected in the study show how important managing behavior can be within social software. Appropriation support can only encourage a particular type of appropriation; it cannot serve as a manager of social interactions. Instead, this must be considered through the development of policies and socio-technical infrastructure that addresses the broader impacts of member behavior. Several subjects said that the overall management of MySpace was a concern: *“MySpace has become a breeding ground for spam and viruses.”* In contrast, the management of Facebook was praised: *“There’s not much ‘spam’ (porn stars, fraudulent profiles, etc.) on Facebook. You do see this a LOT on MySpace though.”* *“I enjoy Facebook, I think that it is a ‘safer’ site in comparison to*

MySpace.” This supports the conclusion that privacy management is very much related to management of social interactions.

12.5 Contributions

This research had made contributions to the understanding of social software in a number of ways. An open issue within information systems research is how to evaluate usage within non-traditional, non-organization based systems, such as social networking sites and other Web 2.0 applications (Barki et al., 2007). Published measures of usage are focused on work and organizational goals, for example: “Using this system allows me to be more efficient at my job” and “This system improved the operations of my organization,” (Barki et al., 2007, p.189).

Even though information systems theory is designed to understand the use of systems in a social context, existing measures cannot be re-used without a transformation. New measures that derive from theory need to be created and tested. While there have been attempts to capture data about the use of social networking sites, there has been minimal attempt to use a theory-driven approach to model use (Shneiderman, 2007). This research has re-applied Adaptive Structuration Theory into the social software context. This has included the use of the theory to develop new measures, and the use of prior measures derived from Adaptive Structuration Theory to validate these measures.

The most significant contribution of this research is the development and partial validation of a new way of modeling privacy management use. This was accomplished through the construction of a formative construct that represents faithful appropriations of privacy management features. The methods used to validate this construct are from

techniques published in *Information Systems Research* (Barki et al., 2007) and *MIS Quarterly* (Petter et al., 2007).

This construct was derived and grounded in Adaptive Structuration Theory, and its validity was confirmed by nomological redundancy analysis using a reflective Faithfulness scale. Because the Faithfulness scale was an existing, rigorously validated scale (Chin et al., 1997), this provides stronger evidence that the formative version of faithful appropriation moves has relevance and validity with respect to the study of privacy management in social software.

This research also makes a contribution by extending theories to a new context, by applying both the Adaptive Structuration Theory and the Fit Appropriation Model to the use of privacy management in social networking sites. Using types and sub-types of appropriation moves from Adaptive Structuration Theory, new measures were developed to provide empirical evidence for the type of appropriation carried out in social networking sites. These new measures, with further efforts to establish validity and reliability, can be adapted to other forms of social software and other components of Web 2.0 applications.

This research also adapted an existing scale, the Faithfulness of Appropriation Scale, resulting in an updated version applicable to Web 2.0 technologies. Another outcome of this research is the Concern for Internet Privacy Scale and a demonstration of its predictive relevance to privacy management within social networking sites.

A contribution of this research is the application of IS theory to software used primarily in a non-organization setting. It is not known how the lack of an organizational context will affect the ability of IS theory to predict outcomes. There has been little

effort to apply IS theory outside of organizations, even though these types of information systems are growing enormously.

Another important contribution of this research is the introduction of a model, the Social Software Performance Model. This model attempts to explain the development and usage of social software. Social software is one of the most important types of system on the Internet. Functionality to support social interaction is becoming a critical deliverable for many information systems. Most systems that support customers or members of an organization must support social interaction. This is a very complex requirement to deliver. It is not understood how to determine the effectiveness of social interaction functions delivered in an information system. This model introduced in this research, given more rigorous testing, can have predictive power regarding the development and usage of social software.

12.6 Limitations

Limitations to this study are related to the administration of the study. Subjects for this study were members of the NJIT community that participate on Facebook and MySpace. The NJIT community is not representative of the populations of either site. In addition, due to technical constraints the subjects were recruited through one way in Facebook (through email) versus MySpace (by using the site to contact subjects). This difference could have introduced an unknown bias in the type of subjects who responded.

As an indication of the volatility of online privacy, it was quite remarkable that both sites experienced nationwide adverse publicity related to privacy incidents *during* the administration of the survey. In the case of MySpace, a story broke in December 2007

describing how a parent, impersonating a teenage boy, had bullied and taunted a former friend of her daughter to the point of suicide (Maag, 2007). In November 2007, Facebook released new technology that tracked members' Internet shopping activities and then included those details in automated notifications sent to friends within their online social network. A national campaign led by the political organization MoveOn.org resulted in considerable changes to this attempt to leverage member behavior for marketing purposes (Story & Stone, 2007). Subjects explicitly mentioned both of these incidents in their free form comments. Either incident could have introduced bias into the responses of subjects.

It is also important to keep in mind that the nature of these sites is in constant flux. New features are rolled out on a frequent basis. Privacy policies can change. Therefore these results only report on a snapshot in time. Extending any findings to the future, or to other sites, must be done with caution.

12.7 Future Research

The data collected for this study has much more potential for further analysis. The study collected a large number of qualitative responses. Future research could involve a more detailed coding and analysis of these answers. In addition, the results of the analysis based on dividing subjects into three groups (Facebook only, MySpace only, and using both) showed promise. Further analysis can be carried out based on Use Profile, including the development of a method to conduct a three way group analysis using PLS. Further analysis can also be carried out by looking more closely at the results for individual indicators, instead of combining them into a summative scale. Future work

could involve treating each individual indicator in a scale as a repeated measure, and then looking at the results.

The next step in the development of the formative construct for Faithful appropriation moves will be to validate it using LISREL, following the multiple indicators, multiple causes approach (MIMIC) as used to establish a formative construct for system usage in (Barki et al., 2007). This method is also based on comparing formative versions with reflective versions of the same construct. Positive results from this additional analysis would add to the validity of the construct, because it depends on a more established and well regarded method for structural equation modeling (Gefen et al., 2000).

The results of this study provide evidence that Adaptive Structuration Theory has relevance with regard to the design of social software. Future research can continue in this vein, using Adaptive Structuration Theory and the concept of “faithfulness” in order to define measures for social responsibility as implemented in social software. This would involve developing a richer understanding of faithfulness and unfaithfulness as expressed in the philosophy of social networking sites. In addition, it would be important to pursue how a particular philosophy or spirit is implemented into tools within these sites.

The development and use of formative constructs can be further extended by developing additional measures of appropriation moves. Additional measures for faithful appropriation moves can be added to the Faithful formative construct. In addition, new measures that capture unfaithful appropriation moves can be created, and then combined for a formative version of unfaithful moves.

This research used a simple ranking of high versus low with respect to appropriation support. The results of this study show that appropriation support cannot be modeled accurately with such a simplistic ranking. Future research includes the analysis and development of a richer set of dimensions that can be used to evaluate and rank instances of appropriation support.

Results from qualitative analysis found that subjects experienced a conflict between presenting themselves to their friends in a truthful way, while still making their profiles “safe” for others to see (such as potential employers). This problem seems to be connected to a pattern found among some users of these sites of creating and maintaining multiple profiles (or avatars, in the case of virtual worlds). Future research could involve an exploration of how and why individuals create and support different instances of their online digital identity.

Future research can also consider how national identity and cultural issues influence the management of privacy. Since these sites do function on a global scale, it is important to see to what extent social interaction and privacy management differ in other countries. As a way of establishing the validity of the research model and the measures of appropriation, these measures can be applied to other sites, such as Friendster and Orkut.

The study of information systems is a large academic field, one that is continually expanding with the development of new systems. The study of social networking sites is a recent addition to this academic field. The results of this research show that information systems theory can be adapted in order to describe and model behavior within these types of systems. It seems the use of technology becomes more social every day. This is despite a palpable disrespect for privacy and lack of basic civility. These anti-social forces must

be addressed by designers of socio-technical systems, or their use will eventually wither. The long term success of social software will depend on the ability of designers to build agile, reliable privacy protection mechanisms.

APPENDIX A

SUMMARY OF MISSING DATA

This appendix presents a table that summarizes missing data for the demographic questions, usage, and those measures relevant to the evaluation of appropriation moves.

Table A.1 Summary of Missing Data

Variable	Valid	Missing or no response
Gender	222	0
Age	222	0
Ethnicity	222	0
Citizenship	222	0
School status	220	2
How often do you visit [name of social networking site]?	222	0
Do you have an account on the other site (i.e., MySpace or Facebook)?	222	0
What information do you include on your profile?		
Photograph	222	0
Real name	221	1
Hometown	221	1
Email address	217	5
Cell phone number	212	10
Relationship status	220	2
Sexual orientation	219	3
Instant messenger screen name	212	10
How often do you update your profile on [name of social networking site]?	222	0
How often do you post a message to a friend's wall?	222	0
Compared to a year ago do you use social networking sites more or less frequently?	222	0
Within the last three months I have read an article that discusses privacy within social networking sites.	221	1
There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy.	221	1
I never accept friend requests from people I have not met in person.	221	1
Adjusting the privacy settings for [name of social networking site] is a waste of time.	220	2
I have personalized my privacy settings on [name of social networking site].	220	2
When using [name of social networking site], I ignore contact from people whom I have not met in person.	221	1
I have researched how to prevent unwanted contact from other members of [name of social networking site].	219	3

Table A.1 Summary of Missing Data (Continued)

Variable	Valid	Missing or no response
Gender	222	0
I am confident that I know how to control who is able to see my profile on [name of social networking site].	219	3
I would not like other people on [name of social networking site] to know whether I viewed their profile.	220	2
I believe most of the profiles I view on [name of social networking site] are exaggerated to make the person look more appealing.	219	3
I feel that the privacy of my personal information is protected by [name of social networking site].	220	2
The original founders of [name of social networking site] would view my use of the privacy settings as inappropriate.	220	2
I am familiar with my privacy settings on [name of social networking site].	221	1
I have been contacted by people through [name of social networking site] whom I did not trust.	220	2
When I need to modify my privacy settings for [name of social networking site], I am able to do it.	220	2
In general, how concerned are you about your privacy while you are using the internet?	220	2
Are you concerned about online organizations not being who they say they are?	219	3
Are you concerned about online identity theft?	218	4
Are you concerned about people online not being who they say they are?	220	2
Are you concerned about people you do not know obtaining personal information about you from your online activities?	219	3
Please indicate your opinion as to the overall value you place on the importance of protecting your privacy on [name of social networking site].	220	2
Within the last three months I have read an article that discusses privacy within social networking sites.	221	1
Over the past year did you experience any incidents that led you to be concerned about privacy when using [name of social networking site]?	222	0

APPENDIX B

CONSENT FORM AND SURVEY INSTRUMENT

This appendix includes the research consent form, the questions that make up the research instrument, and a copy of the IRB approval for this study.

CONSENT FORM

NEW JERSEY INSTITUTE OF TECHNOLOGY
323 MARTIN LUTHER KING BLVD.
NEWARK, NJ 07102

CONSENT TO PARTICIPATE IN A RESEARCH STUDY

TITLE OF STUDY: An investigation of the nature of social interaction on social networking sites

RESEARCH STUDY:

I, _____, have been asked to participate in a research study under the direction of Dr. Roxanne Hiltz and of Cathy Dwyer, a Ph.D. student in Information Systems. Other professional persons who work with them as study staff may assist to act for them.

PURPOSE:

The purpose of this study is to collect your perceptions regarding the importance of and the use of social networking sites. Social networking sites such as Facebook and MySpace have attracted millions of members. The goal of this research is to understand how people use social networking sites to maintain and develop friendships. This understanding can be used to improve technology based systems that depend on the development of social relationships. This includes systems such as those that support online learning, as well as those that support professional collaboration.

DURATION:

My participation in this study will last for approximately 15 minutes to complete the survey.

PROCEDURES:

I have been told that, during the course of this study, the following will occur:

Following this consent form, you will find a series of questions to answer online.

PARTICIPANTS:

I will be one of about 200 participants in this study.

EXCLUSIONS:

I will inform the researcher if any of the following apply to me:

You must be at least 18 years old.

Although it is not likely that an unauthorized person will obtain your responses while you are in the process of entering them, or will be able to break into a server that will be storing the data, it is always possible that a determined hacker could do so. The server that stores the questionnaire responses will reside at NJIT and will not have the level of security that "secure" systems such as credit card systems employ. There is no completely secure interaction online-- as an online participant in this research, there is always the risk of intrusion by outside agents (i.e., hacking) and, therefore the possibility of being identified exists.

There also may be risks and discomforts that are not yet known.

I fully recognize that there are risks that I may be exposed to by volunteering in this study which are inherent in participating in any study; I understand that I am not covered by NJIT's insurance policy for any injury or loss I might sustain in the course of participating in the study.

CONFIDENTIALITY:

I understand confidential is not the same as anonymous. Confidential means that my name will not be disclosed if there exists a documented linkage between my identity and my responses as recorded in the research records. Every effort will be made to maintain the confidentiality of my study records. If the findings from the study are published, I will not be identified by name. My identity will remain confidential unless disclosure is required by law.

COMPENSATION FOR PARTICIPATION:

I have been told that I will receive a \$5 coupon that will enable me to download songs from iTunes.

RIGHT TO REFUSE OR WITHDRAW:

I understand that my participation is voluntary and I may refuse to participate, or may discontinue my participation at any time with no adverse consequence. I also understand that the investigator has the right to withdraw me from the study at any time.

INDIVIDUAL TO CONTACT:

If I have any questions about my treatment or research procedures, I understand that I should contact the principal investigator at:

Professor Roxanne Hiltz Hiltz@njit.edu 973 596 3388

If I have any addition questions about my rights as a research subject, I may contact:

Dawn Hall Apgar, PhD, IRB Chair
New Jersey Institute of Technology
323 Martin Luther King Boulevard
Newark, NJ 07102
(973) 642-7616
dawn.apgar@njit.edu

SIGNATURE OF PARTICIPANT

I have read this entire form, or it has been read to me, and I understand it completely. All of my questions regarding this form or this study have been answered to my complete satisfaction. I agree to participate in this research study.

Subject Name: _____

Signature: _____

Date: _____

SIGNATURE OF READER/TRANSLATOR IF THE PARTICIPANT DOES NOT READ ENGLISH WELL (Only needed if English fluency is not an exclusion criteria)

The person who has signed above, _____, does not read English well, I read English well and am fluent in (name of the language) _____, a language the subject understands well. I have translated for the subject the entire content of this form. To the best of my knowledge, the participant understands the content of this form and has had an opportunity to ask questions regarding the consent form and the study, and these questions have been answered to the complete satisfaction of the participant (his/her parent/legal guardian).

Reader/Translator Name: _____

Signature: _____

Date: _____

SIGNATURE OF INVESTIGATOR OR RESPONSIBLE INDIVIDUAL (Only required for consent forms of projects requiring full IRB approval)

To the best of my knowledge, the participant, _____, has understood the entire content of the above consent form, and comprehends the study. The participants and those of his/her parent/legal guardian have been accurately answered to his/her/their complete satisfaction.

Investigator's Name: _____

Signature: _____

Date: _____

SURVEY INSTRUMENT: AN INVESTIGATION OF THE NATURE OF SOCIAL INTERACTION ON SOCIAL NETWORKING SITES

This document contains a revised survey instrument, for proposal E88-07.

Date of original approval: March 27, 2007, final revision November 21, 2007.

This revision adds question U2 (on page 2) and 11 questions at the end, questions 33 – 43, and replaces all earlier versions of the survey.

Principal investigators: Catherine Dwyer (IS PhD student) and Roxanne Hiltz

The purpose of this study is to compare user behavior on two social networking sites, Facebook and MySpace. Two online surveys will be created – one for members of MySpace, and one for members of Facebook. The questions will be the same for both surveys, but will be customized for each social networking site. In this document the text [name of social networking site] will be replaced in the online version with the text MySpace or Facebook, as appropriate to the survey.

Survey

1. Are you ____ male or ____ female ____ no response
2. What is your age? _____ no response _____
3. If you are a student,
Are you a : ____ Freshman
 ____ Sophomore
 ____ Junior
 ____ Senior
 ____ Masters (or graduate certificate) student
 ____ Ph.D. student
 ____ Faculty
 ____ Staff
 ____ Not a student
 ____ Other, please specify
 ____ No response
4. Please indicate your ethnicity:
White _____
Black or African American _____
American Indian and Alaska Native _____
Asian _____
Native Hawaiian and Pacific Islander _____

Hispanic	_____
Mixed race	_____
No response	_____
Other, please specify	_____
no response	_____

5. Country of citizenship: _____ no response _____

Usage questions

U1) How often do you visit Facebook?

- (1) Never
- (2) Once in a while
- (3) Once a week
- (4) Several times a week
- (5) Every day
- (6) Several times a day

U2) Do you also have an account on MySpace?

- (1) I do not have an active account on MySpace.
- (2) I have an account on MySpace, but I use it infrequently (about once a month or less)
- (3) I have an account on MySpace, and I use it frequently (more frequently than once a month)
- (4) other, please describe

U3) Please indicate what information you include on your profile on [name of social networking site]:

Photograph	_____ yes _____ no
Real name	_____ yes _____ no
Hometown	_____ yes _____ no
Email address	_____ yes _____ no
Cell phone number	_____ yes _____ no
Relationship status	_____ yes _____ no
Sexual orientation	_____ yes _____ no
Instant messenger screen name	_____ yes _____ no

U4) How often do you update your profile on [name of social networking site]?

- (1) Never
- (2) Once in a while
- (3) Once a week
- (4) Several times a week
- (5) Every day

U5) How often do you post a message to a friend's wall (or profile)?

- (1) Never
- (2) Once in a while
- (3) Once a week
- (4) Several times a week
- (5) Every day

U6) Compared to a year ago do you use social networking sites more frequently or less frequently?

- I use social networking sites about the same as a year ago
- I use social networking sites much more frequently than a year ago
- I use social networking sites much less often than a year ago
- Other please describe: _____

The following questions will be answered by this scale:

1 ----- 2----- 3----- 4----- 5----- 6----- 7
 Strongly Disagree Strongly Agree

I have personalized my privacy settings on [name of social networking site].

I have modified the privacy settings for my profile on [name of social networking site].

I have adapted the privacy settings to control who can view my profile on [name of social networking site].

In order to control who can contact me using [name of social networking site] I have adjusted my privacy settings.

I am familiar with my privacy settings on [name of social networking site].

When I need to modify my privacy settings for [name of social networking site], I am able to do it.

I am confident that I know how to control who is able to see my profile on [name of social networking site].

I am comfortable with my ability to adjust my privacy settings.

I use [name of social networking site] only to contact people I see in person on a regular basis.

I never accept friend requests from people I have not met in person.

When using [name of social networking site], I ignore contact from people who I have not met in person.

I don't use [name of social networking site] to make contact with people whom I've never heard of.

I would like to know who has viewed my profile on [name of social networking site].

I would not like other people on [name of social networking site] to know whether I viewed their profile.

I have been contacted by people through [name of social networking site] whom I did not trust.

I believe most of the profiles I view on [name of social networking site] are exaggerated to make the person look more appealing.

I don't believe most of the information people put on their profiles on [name of social networking site].

There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy.

Adjusting the privacy settings for [name of social networking site] is a waste of time.

I don't bother to look at the privacy settings for my profile on [name of social networking site].

I don't use the privacy settings to control who can access my profile.

I don't know what my privacy settings are on [name of social networking site].

The founders of [name of social networking site] would disagree with how I use the privacy settings.

I probably use the privacy settings for [name of social networking site] improperly.

The original founders of [name of social networking site] would view my use of the privacy settings as inappropriate.

I failed to use the privacy settings of [name of social networking site] as they should be used.

I did not use the privacy settings in [name of social networking site] in the most appropriate fashion.

Concern for Internet Privacy

1. In general, how concerned are you about your privacy while you are using the internet?
Never |---1-----2-----3-----4-----5-----6-----7---| Always
2. Are you concerned about online organizations not being who they say they are?
Never |---1-----2-----3-----4-----5-----6-----7---| Always
3. Are you concerned about online identity theft?
Never |---1-----2-----3-----4-----5-----6-----7---| Always
4. Are you concerned about people online not being who they say they are?
Never |---1-----2-----3-----4-----5-----6-----7---| Always
5. Are you concerned about people you do not know obtaining personal information about you from your online activities?
Never |---1-----2-----3-----4-----5-----6-----7---| Always

6. I have changed the default settings for my profile to make it more private.
Strongly Disagree | --1---2---3--4---5---6--7---| Strongly Agree
7. I have taken time to learn what steps [name of social networking site] takes to protect my privacy.
Strongly Disagree | --1---2---3--4---5---6--7---| Strongly Agree
8. I am knowledgeable about the contents of the privacy policy for [name of social networking site].
Strongly Disagree | --1---2---3--4---5---6--7---| Strongly Agree
9. I have researched how to prevent unwanted contact from other members of [name of social networking site].
Strongly Disagree | --1---2---3--4---5---6--7---| Strongly Agree
10. Within the last three months I have read an article that discusses privacy within social networking sites.
Strongly Disagree | --1---2---3--4---5---6--7---| Strongly Agree
11. I feel that the privacy of my personal information is protected by [name of social networking site].
Strongly Disagree | --1---2---3--4---5---6--7---| Strongly Agree
12. I trust that [name of social networking site] will not use my personal information for any other purpose.
Strongly Disagree | --1---2---3--4---5---6--7---| Strongly Agree
13. Please indicate your opinion as to the overall value you place on the importance of protecting your privacy on [name of social networking site].
- 1 ----- 2----- 3----- 4----- 5----- 6----- 7
Not valuable or important Extremely valuable and important
14. Over the past year did you experience any incidents that led you to be concerned about privacy when using [name of social networking site]?
Yes no

(these questions will be asked only if subject answers “yes”)

15. Did you review your privacy settings after this incident?
Yes _____ no _____
16. Did you make any adjustments or changes to your privacy settings after this incident?
Yes _____ no _____

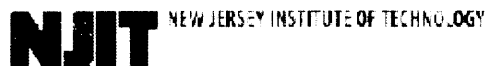
Open Ended Questions

What is the most positive benefit you get from your use of [name of social networking site]?

What is your greatest concern regarding the use of [name of social networking site]?

Please comment on how effective you think the privacy protection is for [name of social networking site]

Any other additional comments related to your use of [name of social networking site]?



**Institutional Review Board: HHS FWA 00003246
Notice of Approval
IRB Protocol Number: E88-07**

Principal Investigators: Catherine Dwyer and Roxanne Hiltz
Information Systems

Title: An Investigation of the Nature of Social Interaction on Social Networking Sites

Performance Site(s): NJIT

Sponsor Protocol Number (if applicable):

Type of Review: FULL ☒ EXPEDITED ☐

Type of Approval: NEW ☒ RENEWAL ☐ MAJOR REVISION ☐

Approval Date: March 27, 2007

Expiration Date: March 26, 2008

1. **ADVERSE EVENTS:** Any adverse event(s) or unexpected event(s) that occur in conjunction with this study must be reported to the IRB Office immediately (973) 642-7616.
2. **RENEWAL:** Approval is valid until the expiration date on the protocol. You are required to apply to the IRB for a renewal prior to your expiration date for as long as the study is active. Renewal forms will be sent to you, but it is your responsibility to ensure that you receive and submit the renewal in a timely manner.
3. **CONSENT:** All subjects must receive a copy of the consent form as submitted. Copies of the signed consent forms must be kept on file with the principal investigator.
4. **SUBJECTS:** Number of subjects approved: 200.
5. The investigator(s) did not participate in the review, discussion, or vote of this protocol.
6. **APPROVAL IS GRANTED ON THE CONDITION THAT ANY DEVIATION FROM THE PROTOCOL WILL BE SUBMITTED, IN WRITING, TO THE IRB FOR SEPARATE REVIEW AND APPROVAL.**

Dawn Hall Appgar, PhD, LSW, ACSW, Chair IRB

March 27, 2007

APPENDIX C

PILOT STUDIES

This appendix contains a report and summary of prior studies conducted that led to the constructs and survey instrument tested in this dissertation.

REPORT OF PILOT STUDIES

This dissertation is the culmination of three years of research on a subject that has yet to receive a significant amount of academic attention. Few if any measures for items regarding the use of these sites were available, and so these had to be developed and validated. Measures for privacy concern as well as usage of the sites have been tested in several studies. More detailed descriptions of prior studies can be found in (Dwyer, 2007; Dwyer, Hiltz, & Jones, 2006; Dwyer et al., 2007; Dwyer et al., 2008). The next section describes a pilot study conducted in August 2007 that reviews an investigation of new measures for appropriation moves with respect to privacy management.

SURVEY INSTRUMENT

A pilot study was administered using an online survey in August 2007 to test new measures of appropriation moves regarding privacy management in social networking sites. Appropriation moves define types of use with respect to adoption of advanced information technologies. These moves are defined in a taxonomy that is part of Adaptive Structuration Theory (DeSanctis & Poole, 1994).

These measures of appropriation moves were tested for two social networking sites, Facebook and MySpace. Two versions of the survey were created, one for members of Facebook, and the other for members of MySpace. Subjects were recruited by posting messages in public forums in Facebook and MySpace offering \$5 for completion of the survey.

The survey was available for eight days. The goal was to obtain about 50 subjects in order to carry out reliability tests on the appropriation measures. Ideally, this translates into 25 Facebook subjects and 25 MySpace subjects. During the administration, it turned out to be much harder to recruit MySpace subjects. Facebook subjects were more willing to complete the survey. The total subjects included in the study are 35 subjects from Facebook and 16 subjects from MySpace, for a total of 51.

Reliability analysis (Cronbach's alpha) was administered to the measures of appropriation moves. One existing scale was tested (Faithfulness of Appropriation Scale), and six new measures of appropriation moves were tested. Feedback from the reliability analysis was used to eliminate 16 questions from the survey. Five measures (including the Faithfulness scale) were found to have good alpha results (.8 or higher). One measure has marginal results (expressing a bad opinion about others) and one has poor results and will be dropped (using fake information).

Factor analysis was also administered. A rotated solution found that the measures loaded independently on each appropriation move. This supports the use of this survey with a larger, randomly drawn sample.

RESULTS

This pilot study was designed to test new measures of appropriation moves with respect to privacy management in social networking sites. Six new measures consisting of a total of 38 questions were included. All questions were measured on a 7 point semantic differential scale, from 1 (Strongly Disagree) to 7 (Strongly Agree). The question order was determined using random numbers. Two versions of the study were created, one for

members of Facebook, and one for members of MySpace. It was made available online on August 21, 2007 and closed on August 28, 2007. The Facebook version was completed by 35 subjects, and the MySpace version was completed by 16 subjects (51 in total).

The survey was completed by 22 female and 29 male subjects (in Facebook, 16 female and 19 male, and in MySpace, 6 female and 10 male). The age of subjects varies from a low of 18 to a high of 58, with the mean being 24.43. The mean age for Facebook subjects is 22.11, and the mean age for MySpace is 29.5. This result is significant, $F=7.280$ and $p = .01$. A higher proportion of Facebook subjects are students compared to MySpace (88.8% for Facebook versus 56.3% for MySpace).

FINDINGS WITH REGARD TO MEASURES OF APPROPRIATION MOVES

This section describes the reliability analysis conducted for the measures. The goal of this analysis was to eliminate weak questions and strengthen as much as possible the remaining scales. A pre-existing scale that was adapted to social networking sites was tested (the Faithfulness of Appropriation Scale), as well as six new scales. The results of this analysis are described below.

For each of the proposed new scales, and the existing Faithfulness of Appropriation Scale, a reliability analysis was performed using SPSS v. 13.0. For the new measures, addition test were performed to reduce the number of items in the scale. This was done to both eliminate weak results and reduce the number of questions in the survey.

Each of the scales described below is followed by a table summarizing the results of the reliability analysis. The table includes the following columns:

- **Scale Mean if Item Deleted:** The value of the mean for the scale if the question on each row was deleted. This is a measure of how far the results for a question move the mean in one direction or another.
- **Scale Variance if Item Deleted:** This indicates the value of the variance if the question in each row is deleted. Values with lower variances are indications of a more homogenous response.
- **Corrected Item-Total Correlation:** This is a measure of how much each item correlates with the total mean. Values are higher if the item correlates strongly with the total mean calculated for all the measures. A method for improving the results for Cronbach's alpha is by dropping items with a low item-total correlation (Bernard, 2000).
- **Cronbach's Alpha If Item Deleted:** This is a revised calculation of Cronbach's alpha if the question in each row is dropped.

FAITHFULNESS OF APPROPRIATION SCALE

This pilot study includes an adaptation of a scale previously tested to determine the degree of Faithfulness with regard to appropriation (Chin et al., 1997). The original implementation of the scale measures faithfulness of appropriation of electronic meeting systems technology. The questions in this scale have been reworded to apply to privacy management in social networking sites. You can see below a table that summarizes the reliability results. This summary, and all the other tables, show a generic version of the question. In the actual surveys, the phrase [name of social networking site] is replaced with Facebook or MySpace. This version of the Faithfulness scale, as adapted for privacy management in social networking sites, was found to have a Cronbach's alpha of .849.

Table C.1 Faithfulness of Appropriation Scale

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
I probably use the privacy settings for [name of social networking site] improperly.	9.32	25.651	.672	.816
I failed to use the privacy settings of [name of social networking site] as it should be used.	9.82	29.253	.567	.841
I did not use the privacy settings in [name of social networking site] in the most appropriate fashion.	9.48	25.724	.817	.776
The founders of [name of social networking site] would disagree with how I use the privacy settings.	9.42	27.269	.653	.820
The original founders of [name of social networking site] would view my use of the privacy settings as inappropriate.	9.80	28.857	.600	.833

DIRECT USE APPROPRIATION MOVE - FAMILIARITY

This move is a measurement of the degree to which subjects express familiarity with privacy settings. This is an example of an explicit appropriation move, and is considered a faithful appropriation (as defined in Adaptive Structuration Theory, see (DeSanctis & Poole, 1994)). Six questions were tested (see below). As before, the phrase [name of social networking site] was replaced by Facebook and MySpace in the appropriate survey. The top four results will be kept (dropping question 22 and 28). The questions to

be kept will be selected based on the highest values for item total correlation, as recommended by Bernard (Bernard, 2000). These four questions show a Cronbach's alpha of .919.

Table C.2 Familiarity Appropriation Move

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
I am confident that I know how to control who is able to see my profile on [name of social networking site].	29.04	48.915	.514	.907
I know how to adjust my privacy settings to control who is able to contact me through [name of social networking site].	28.22	48.636	.685	.871
I am comfortable with my ability to adjust my privacy settings.	28.24	48.730	.758	.860
When I need to modify my privacy settings for [name of social networking site], I am able to do it.	27.96	49.457	.794	.857
If I wanted to change who can view my profile, I would know how to do it.	28.08	46.993	.773	.857
I am familiar with my privacy settings on [name of social networking site].	28.14	48.458	.782	.857

ACTUAL USE APPROPRIATION MOVE

This scale measures to what extent subjects report actual use of privacy management. As with the familiarity scale, this appropriation move is a faithful appropriation. Six questions were tested, and the top four will be kept based on the item-total correlation (see Table 8.3). The questions that will be dropped are 46 and 53. This scale has a Cronbach's alpha of .908.

Table C.3 Actual Use Appropriation Move

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
I have modified the privacy settings for my profile on [name of social networking site].	24.40	71.393	.750	.847
In order to control who can contact me using [name of social networking site] I have adjusted my privacy settings.	24.56	73.741	.777	.842
I have personalized my privacy settings on [name of social networking site].	24.27	72.074	.823	.833
I have reviewed my privacy settings so that I know my privacy is protected.	23.71	89.062	.487	.886
I have adapted the privacy settings to control who can view my profile on [name of social networking site].	24.15	73.914	.778	.842
I have set up my privacy settings so that I am comfortable with who can contact me using [name of social networking site].	24.02	85.000	.505	.886

PARTIAL APPROPRIATION OF PRIVACY STRUCTURES

This appropriation move involves using part of the structure, rather than all of it. It is a faithful appropriation. This move concerns to what extent do members restrict their contact with others on the site. This is a partial appropriation because they are using the site, but restricting who they communicate with. This is a faithful appropriation because taking steps to protect your privacy is consistent with the spirit of the privacy settings. Five questions were tested, and one was dropped (question 43). The Cronbach's alpha for this scale is .856.

Table C.4 Partial Appropriation Move

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
I never accept friend requests from people I have not met in person.	15.65	45.766	.643	.832
I don't use [name of social networking site] to make contact with people whom I've never heard of.	14.77	44.861	.733	.806
When using [name of social networking site], I ignore contact from people who I have not met in person.	15.56	43.783	.818	.784
I don't trust anyone I don't already know on [name of social networking site].	15.48	50.425	.539	.856
I use [name of social networking site] only to contact people I see in person on a regular basis.	16.54	50.296	.619	.836

UNRELATED APPROPRIATION MOVE (USING FAKE INFORMATION)

This appropriation move is an example of unrelated use. This involves using an opposing structure rather than the structure at hand. This is an example of an unfaithful appropriation.

Table C.5 Using Fake Information

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
My online profile is very different from who I am in person.	14.77	19.183	.127	.364
I include made up information on my profile.	14.91	18.688	.171	.345
I am hesitant to share information about myself with others on [name of social networking site].	12.51	17.081	.130	.366
I don't think it is a good idea to have a lot of valid information on my profile.	12.30	14.431	.251	.278
I include fake information on my profile in order to protect my privacy.	14.77	16.618	.251	.293
I leave out information about my home town on my profile to protect myself.	13.51	14.386	.163	.359

This move relates to the extent to which members include fake information on their profile. Fake information is an unrelated appropriation because it opposes the spirit of the social networking site, which is sharing information about who you really are. The

reliability analysis for this scale had very poor results, Cronbach's alpha of .367.

Therefore this scale is being dropped from the study.

Table C.6 Summary of Results for Bad Opinion Construct

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
I worry that I will be embarrassed by wrong information others post about me on [name of social networking site].	20.33	28.183	.174	.498
People should be embarrassed by what they include on their [name of social networking site] profile.	19.08	30.035	-.025	.609
There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy.	17.88	24.026	.487	.359
I don't believe most of the information people put on their profiles on [name of social networking site].	19.31	24.800	.410	.393
I believe most of the profiles I view on [name of social networking site] are exaggerated to make the person look more appealing.	18.65	21.898	.553	.306
I have been contacted by people through [name of social networking site] whom I did not trust.	18.84	24.389	.157	.537

CONTRAST OF PRIVACY STRUCTURES (EXPRESSING A BAD OPINION)

This scale is an example of a criticism of the privacy structure, but without a specific contrast or comparison. It is an example of a unfaithful appropriation. These questions measure the extent to which members have a bad opinion about other people on the site. This is related to appropriation of privacy setting, because a robust set of privacy protection functions would be expected to screen out people who do not seem trustworthy. Six questions were tested, with a poor initial Cronbach's alpha of .476. Once two questions were dropped (16 and 19), the Cronbach's alpha increased to .682, which is just below the acceptable value of .7. Since this is a new measure and the Cronbach's alpha is marginally acceptable, this scale will be kept.

EXPRESSING JUDGMENTS ABOUT THE STRUCTURE

This appropriation move measures to what extent subjects criticize, disagree with or otherwise directly reject appropriation of the structure. This is an example of a unfaithful appropriation. Six questions were tested for this scale, and two were dropped (24 and 29). The remaining scale has a Cronbach's alpha of .804.

Table C.7 Rejection of Privacy Settings

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
It is not worth the trouble to change the privacy settings for [name of social networking site].	13.06	49.061	.513	.812
I don't think the privacy settings on [name of social networking site] do much to protect my privacy.	12.06	47.670	.485	.815
I don't use the privacy settings to control who can access my profile.	12.32	38.526	.614	.795
Adjusting the privacy settings for [name of social networking site] is a waste of time.	13.00	42.870	.724	.771
I don't bother to look at the privacy settings for my profile on [name of social networking site].	12.70	41.127	.695	.772
I don't know what my privacy settings are on [name of social networking site].	12.70	40.953	.577	.801

FACTOR ANALYSIS OF APPROPRIATION MOVE MEASURES

Additional analysis was carried out on the remaining appropriation measures to determine their factor loading. One caveat about this analysis is that the sample size of 50 is at the absolute minimum for factor analysis (Hair et al., 2006). This makes any in depth analysis on these measures premature. However, the purpose of this analysis is to test in general the soundness of these measures. For this purpose, the results do support going forward with these measures with a larger sample.

The first step was a principal components analysis (see below). This created a solution with five factors. Questions for **Actual Use** and **Rejection** load on the first factor, but **Actual Use** loads with positive values and **Rejection** loads with negative values. In addition, questions for **Familiarity** also load with positive values on the first factor. This is logical because each of these appropriation moves is related to each other. The positive ones are both examples of direct use, and the negative one is a rejection of direct use.

Partial use loads on the second factor as negative values. Its fourth question (question 54) is a split factor, loading on both the second factor and the fourth factor. **Expressing a Bad Opinion** loads with one question on the second factor and three questions on the third factor. No questions load above .5 on the fifth factor.

Table C.8 Principal Component Matrix

Approp. Move	Question	Component				
		1	2	3	4	5
Actual Use	I have personalized my privacy settings on [name of social networking site].	.881	.063	.148	-.260	.079
Actual Use	I have adapted the privacy settings to control who can view my profile on [name of social networking site].	.805	.118	.226	-.268	-.076
Actual Use	I have modified the privacy settings for my profile on [name of social networking site].	.790	-.088	.229	-.243	.140
Rejection	I don't bother to look at the privacy settings for my profile on [name of social networking site].	-.769	-.055	-.004	-.070	.433
Rejection	I don't use the privacy settings to control who can access my profile.	-.744	-.012	-.120	.051	.201
Actual Use	In order to control who can contact me using [name of social networking site] I have adjusted my privacy settings.	.721	-.185	.395	-.281	.037
Familiarity	I am familiar with my privacy settings on [name of social networking site].	.721	.421	-.012	.422	-.032
Rejection	I don't know what my privacy settings are on [name of social networking site].	-.708	.127	.163	-.179	.278
Familiarity	When I need to modify my privacy settings for [name of social networking site], I am able to do it.	.688	.501	-.018	.093	.390
Familiarity	If I wanted to change who can view my profile, I would know how to do it.	.684	.496	-.034	.041	.385
Familiarity	I am comfortable with my ability to adjust my privacy settings.	.632	.473	-.016	.484	.035

Next an effort was made to find a rotated solution. Using the Equamax method, a rotated solution was found that shows that the scale questions load as expected for each appropriation move (see below). The Equamax method combines the Quartimax and Varimax approaches. Quartimax attempts to simplify the row of each factor, and Varimax attempts to simplify the column. Equimax does a little of both (Hair et al., 2006).

Table C.9 Rotated Component Matrix

Appropriation Moves	Component				
	1	2	3	4	5
Actual Use					
In order to control who can contact me using [name of social networking site] I have adjusted my privacy settings.	.792	.148	.278	-.237	.089
I have personalized my privacy settings on [name of social networking site].	.776	.392	.101	-.294	-.149
I have modified the privacy settings for my profile on [name of social networking site].	.753	.300	.239	-.204	-.075
I have adapted the privacy settings to control who can view my profile on [name of social networking site].	.744	.311	-.004	-.373	-.030
Familiarity					
I am comfortable with my ability to adjust my privacy settings.	.032	.841	-.054	-.384	.008
When I need to modify my privacy settings for [name of social networking site], I am able to do it.	.377	.840	-.103	-.020	-.163
If I wanted to change who can view my profile, I would know how to do it.	.403	.807	-.122	-.010	-.190

Table C.9 Rotated Component Matrix (Continued)

I am familiar with my privacy settings on [name of social networking site].	.124	.799	-.032	-.470	-.022
Partial appropriation					
When using [name of social networking site], I ignore contact from people who I have not met in person.	.173	-.286	.834	-.162	-.016
I don't use [name of social networking site] to make contact with people whom I've never heard of.	.135	-.024	.825	-.235	-.212
I never accept friend requests from people I have not met in person.	.263	-.091	.814	.248	.109
I use [name of social networking site] only to contact people I see in person on a regular basis.	-.132	.164	.740	-.388	.048
Rejection of Privacy Settings					
I don't bother to look at the privacy settings for my profile on [name of social networking site].	-.364	-.276	-.032	.754	.088
I don't know what my privacy settings are on [name of social networking site].	-.215	-.269	-.239	.647	.243
Adjusting the privacy settings for [name of social networking site] is a waste of time.	-.523	.172	-.153	.558	.305
I don't use the privacy settings to control who can access my profile.	-.507	-.279	-.101	.513	.048
Expressing a Bad Opinion					
I don't believe most of the information people put on their profiles on [name of social networking site].	-.057	-.179	-.008	.069	.794

Table C.9 Rotated Component Matrix (Continued)

I believe most of the profiles I view on [name of social networking site] are exaggerated to make the person look more appealing.	-.130	-.071	.138	.042	.790
There are a lot of profiles on [name of social networking site] for people who do not seem trustworthy.	.233	.028	-.172	.298	.693
I have been contacted by people through [name of social networking site] whom I did not trust.	-.094	.043	-.524	-.071	.546
Extraction Method: Principal Component Analysis. Rotation Method: Equamax with Kaiser Normalization. Rotation converged in 23 iterations.					

The appropriation move with the strongest factor loading is **Actual Use**, and the one with the weakest is **Expressing a Bad Opinion**. One of the questions for **Expressing a Bad Opinion** is a split factor, loading at .524 with **Partial Appropriation**. This is the only question that is a split factor in the rotated solution. This question loads with **Partial Appropriation** in the un-rotated solution. The findings for this rotated factor analysis are consistent with the results found with the reliability analysis. The results of this factor loading provide additional justification for further use and development of these measures.

OTHER MEASURES

In addition to new measures of appropriation moves, this survey also contained questions previously tested in prior studies. This includes a five item scale that measures the degree of concern with regard to Internet privacy, adapted from (Buchanan et al., 2007). In addition, two questions measure One Sided Profile Browsing, described as a paradox

appropriation move. One Sided Profile Browsing occurs when members can learn who views their profile while at the same time restricting information as to what profiles they themselves view. Two questions are asked, one as to whether they would like to see who else has viewed their profile, and one asking if they would allow others to know when they have viewed their profile. Answers in the extreme for both questions match One Sided Profile Browsing. Since these questions ask about opposite conditions, it is not appropriate to test using Cronbach's alpha.

EVALUATION OF MAIN EFFECTS

The data collected from this pilot study does provide evidence that there are differences in the appropriation moves of members of Facebook versus members of MySpace. It must be noted, however, that the number of subjects in this pilot study is small and the sample is not random. While these results support the hypotheses derived from the Social Software Performance Model, they cannot as of yet be generalized to the complete population. The results are described in greater detail below.

Faithful Appropriation Moves

H1. Members of Facebook will have more faithful appropriation moves compared to members of MySpace.

Partially supported.

There are three measures of faithful appropriation moves: Actual Use, Familiarity, and Partial Use. Each of these is a four item summative scale, with a minimum of four and a maximum of 28. There were no significant differences found when comparing the

results for Facebook and MySpace for the Actual Use and Familiar measures. It must be noted that the p level for the Actual Use measure is .08, just beyond the significance level of .05. Since this is a borderline result, it is possible that a larger sample may lead to significant results. There is a significant difference found for the Partial Use appropriation measure. This difference is predicted by H1, therefore this result partially supports H1.

Table C.10 Results for Faithful Appropriation Moves

	Actual Use	Familiar	Partial***
Facebook	20.029	23.588	17.758
MySpace	15.813	22.733	10.467
Total	18.680	23.327	15.479
*** p <.001			

NEGATIVE APPROPRIATION MOVES

H2. Members of Facebook will have fewer negative appropriation moves compared to members of MySpace.

Supported.

There are two appropriation moves that measure negative appropriation, BadOpinion and Negation. Both of these are four item summative scales, with a minimum of four and a maximum of 28. There are significant differences for both these measures in the expected direction when comparing the results for Facebook versus MySpace. These results therefore support H2.

Table C.11 Results for Negative Appropriation Moves

	BadOpinion***	Negation**
Facebook	14.794	8.606
MySpace	20.667	13.143
Total	16.592	9.957
** p < .01 *** p < .001		

H3. Members of Facebook will have more faithful appropriation compared to members of MySpace.

Not supported.

The Faithfulness Appropriation Scale is a five item summative scale with a minimum of five and a maximum of 35. There were no significant differences found in the Faithful of Appropriation scale. Therefore H3 is not supported.

Table C.12 Results for Faithfulness of Appropriation Scale

	Faithful
Facebook	12.618
MySpace	10.563
Total	11.960

EFFECT SIZE

Table C.13 presents a summary of the effect sizes for each of the appropriation moves.

Table C.13 Effect Sizes for Appropriation Moves

Measures of Association	Eta	Eta Squared
Faithful	0.15	0.02
Actual Use	0.25	0.06
Familiar	0.07	0.00
Partial	0.48	0.23
BadOpinion	0.53	0.28
Negation	0.34	0.12

Effect sizes for each of the measures were calculated using the Eta and Eta squared functions. Two of the measures exhibited a medium to medium-low effect size. These are Partial (Eta squared = .23) and BadOpinion (Eta squared = .28). One of the measures, Negation, has a low effect size (Eta squared = .12). The other measures have effect sizes that are too low to have practical significance.

REFERENCES

- Ackerman, M. (2000). The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility. *Human-Computer Interaction*, 15(2/3), 179-203.
- Acquisti, A., & Gross, R. (2006). *Imagined Communities: Awareness, Information Sharing and Privacy on The Facebook*. Paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK.
- Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(1), 179-211.
- Allison, I., & Merali, Y. (2007). Software process improvement as emergent change: A structurational analysis. *Information and Software Technology*, 49, 668-681.
- Atal, M., & Wilson, C. (2007, August 30). Feeling Trashed on the Web? How to avoid having your brand message hijacked. *Business Week*.
- Backstrom, L., Huttenlocher, D., Kleinberg, J., & Lan, X. (2006). Group formation in large social networks: membership, growth, and evolution. In *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 44-54). Philadelphia, PA, USA: ACM Press.
- Bansler, J. P., & Havn, E. (2006). Sensemaking in Technology-Use Mediation: Adapting Groupware Technology in Organizations. *Computer Supported Cooperative Work*, 15, 55-91.
- Barki, H., Titah, R., & Boffo, C. (2007). Information System Use-Related Activity: An Expanded Behavioral Conceptualization of Individual-Level Information System Use. *Information Systems Research*, 18(2), 173-192.
- Barley, S. R. (1986). Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments. *Administrative Science Quarterly*, 31(1), 78-108.
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9).
- Barrish, M. (2003). *The Obvious*. Retrieved July 27, 2006, from <http://obvious.com/archives/03110501.shtml>.
- Bernard, H. R. (2000). *Social Research Methods*. Thousand Oaks, CA: Sage Publications, Inc.

- BestWeekEver. (2006). *MySpace Comments of the Rich and Famous*. Retrieved November 3, 2006, from <http://www.bestweekever.tv/tag/Jessica+Simpson>.
- Bettman, J. R., Luce, M. F., & Payne, J. W. (1988). Constructive consumer choice processes. *Journal of Consumer Research*, 25(3).
- Boehm, B. (2002). Get ready for agile methods, with care. *IEEE Computer*, 35(1), 64-69.
- boyd, d. (2004). *Friendster and Publicly Articulated Social Networks*. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Vienna, Austria.
- boyd, d. (2006a). Friends, friendsters, and top 8: Writing community into being on social network sites. *First Monday*, 8(11-12).
- boyd, d. (2006b). *What I Mean When I Say "email is dead" in Reference to Teens*. Retrieved November 16, 2006, from http://www.zephoria.org/thoughts/archives/2006/11/07/what_i_mean_whe.html.
- boyd, d. (2007, May 2007). *Social Network Sites: Public, Private, or What?* Retrieved July 25, 2007, from http://kt.flexiblelearning.net.au/tkt2007/?page_id=28.
- boyd, d., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1).
- boyd, d., & Heer, J. (2006). *Profiles as Conversation: Networked Identity Performance on Friendster*. Paper presented at the Hawaii International Conference on System Sciences, Kauai, Hawaii.
- Brooks, L. (1997). Structuration theory and new technology: Analysing organizationally situated computer-aided design (CAD). *Information Systems Journal*, 7(2), 133-151.
- Buchanan, T., Paine, C., Joinson, A., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165.
- Caldwell, L. M. (2007, August 6). *Daddy Dearest: Rudy Giuliani's daughter is supporting Barack Obama*. Retrieved September 27, 2007, from <http://slate.com/id/2171730/>.
- Chiaromonte, P., & Martinez, E. (2006, March 18). Jerks In Space. *The New York Post*, p. 6.
- Chin, W. W. (1998). The Partial Least Squares Approach for Structural Equation Modeling. In G. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 295-336). Mahwah: Lawrence Erlbaum Associates.

- Chin, W. W., Gopal, A., & Salisbury, W. D. (1997). Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation. *Information Systems Research*, 8(4), 342.
- Coughlan, S. (2006). *Dial H for History*. Retrieved January 28, 2007, from http://news.bbc.co.uk/2/hi/uk_news/magazine/5360892.stm.
- Coutu, D. L., Joerres, J. A., Fertik, M., Palfrey Jr., J. G., & boyd, d. (2007). *We Googled You: Should Fred hire Mimi despite her online history?* Retrieved July 25, 2007, from <http://harvardbusinessonline.hbsp.harvard.edu/>.
- CRA. (2003). *Four Grand Challenges in Trustworthy Computing*. Retrieved December 17, 2006, from <http://www.cra.org/reports/trustworthy.computing.pdf>.
- DavisWiki. (2006). *The UC Davis Varsity Facebook Team*. Retrieved November 3, 2006, from [http://www.daviswiki.org/Varsity Facebook Team](http://www.daviswiki.org/Varsity_Facebook_Team).
- Dennis, A., & Garfield, M. (2003). The adoption and use of GSS in project teams: Toward more participative processes and outcomes. *MIS Quarterly*, 27(2), 289-323.
- Dennis, A., Wixom, B., & Vandenberg, R. (2001). Understanding Fit and Appropriation Effects in Group Support Systems via Meta-Analysis. *MIS Quarterly*, 25(2), 167-193.
- DeSanctis, G., & Poole, M. S. (1991). *Understanding the differences in collaborative system use through appropriation analysis*. Paper presented at the Twenty-Fourth Annual Hawaii International Conference on System Sciences, Kauai, HI, USA.
- DeSanctis, G., & Poole, M. S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science*, 5(2), 121-147.
- Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, 13(1).
- Donath, J., & boyd, d. (2004). Public Displays of Connection. *BT Technology Journal*, 22(4), 71-82.
- Dourish, P. (2003). The Appropriation of Interactive Technologies: Some Lessons from Placeless Documents. *Computer Supported Cooperative Work*, 12(4), 465-490.
- Dwyer, C. (2007). *Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS), Hawaii.

- Dwyer, C., Hiltz, S. R., & Jones, Q. (2006). *Discovering Boundaries for Mobile Awareness: An Analysis of Relevant Design Factors*. Paper presented at the Americas Conference on Information Systems, Acapulco, Mexico.
- Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace*. Paper presented at the Thirteenth Americas Conference on Information Systems, Keystone, Colorado.
- Dwyer, C., Hiltz, S. R., & Widmeyer, G. (2008). *Understanding Development and Usage of Social Networking Sites: The Social Software Performance Model*. Paper presented at the 41st Annual Hawaii International Conference on System Sciences (HICSS), Hawaii.
- Facebook. (2006). *Facebook Privacy Policy*. Retrieved March 3, 2008, from www.facebook.com.
- Facebook. (2008). *Facebook Home Page*. Retrieved March 2, 2008, from www.facebook.com.
- Fuller, R., & Dennis, A. (2004). *Does Fit Matter? The Impact of Fit on Collaboration Technology Effectiveness Over Time*. Paper presented at the 37th Hawaii International Conference on System Sciences, Hawaii.
- Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. *Communications of the AIS*, 4(7).
- Giddens, A. (1979). *Central Problems in Social Theory*. Berkeley, CA: University of California Press.
- Giddens, A. (1984). *The Constitution of Society*. Berkeley, CA: University of California Press.
- Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday and Co.
- Goodhue, D. (1995). Understanding User Evaluations of Information Systems. *Management Science*, 41(12), 1827-1844.
- Goodhue, D. (1998). Development and measurement validity of a task-technology fit instrument for user evaluations of information systems. *Decision Sciences*, 29(105-139).
- Goodhue, D., Klein, B. D., & March, S. T. (2000). User evaluations of IS as surrogates for objective performance. *Journal of Information Management*, 38(2).
- Goodhue, D., Lewis, W., & Thompson, R. (2007). Research Note—Statistical Power in Analyzing Interaction Effects: Questioning the Advantage of PLS with Product Indicators. *Information Systems Research*, 18(2), 211-227.

- Goodhue, D., Lewis, W., & Thompson, R. L. (2006). *PLS, Small Sample Size, and Statistical Power in MIS Research*. Paper presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences - Volume 08.
- Goodhue, D., & Thompson, R. L. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, 19(2), 213-236.
- Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks*. Paper presented at the 2005 ACM Workshop on Privacy in the Electronic Society.
- Grudin, J. (2001). Desituating Action: Digital Representation of Context. *Human-Computer Interaction*, 16(2-4), 269-286.
- Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). *Multivariate Data Analysis*. (Sixth ed.). Upper Saddle River, New Jersey: Prentice Hall.
- Hargittai, E. (2007). Whose space? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication*, 13(1).
- Hempel, J. (2005, December 12). The MySpace Generation. *Business Week*, 3963, 86.
- Hughes, T. (1989). The Evolution of Large Technological Systems. In W. Bijker, T. Hughes & T. Pinch (Eds.), *The Social Construction of Technological Systems* (pp. 51-87). Cambridge, MA: The MIT Press.
- Humphreys, L. (2007). Mobile social networks and social practice: A case study of Dodgeball. *Journal of Computer-Mediated Communication*, 13(1).
- Hunt, K. (2007, May 27). Fallen soldiers' MySpace profiles live on in cyberspace. *International Herald Tribune*.
- Jones, H., & Soltren, J. H. (2005). *Facebook: Threats to Privacy*. Retrieved July 25, 2007, from <http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf>.
- Jones, M. (1997). Structuration Theory. In W. Currie & B. Galliers (Eds.), *Rethinking Management Information Systems* (pp. 103-135). New York: Oxford University Press.
- Keen, P. (1981). Information Systems and Organizational Change. *Communications of the ACM*, 24(1), 24-33.
- Keen, P., & Morton, M. S. (1978). *Decision Support Systems: An Organizational Perspective*. Reading, MA: Addison-Wesley, Inc.

- Lampe, C., Ellison, N., & Steinfield, C. (2006). *A face(book) in the crowd: Social searching versus social browsing*. Paper presented at the 20th Anniversary Conference on Computer Supported Cooperative Work, Banff, Alberta, Canada.
- Lampe, C., Ellison, N., & Steinfield, C. (2007). *A familiar face(book): profile elements as signals in an online social network*. Paper presented at the SIGCHI conference on Human factors in computing systems, San Jose, California, USA.
- Lange, P. G. (2007). Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication*, 13(1).
- Lawler, J., & Molluzzo, J. (2005). *A Study of Data Mining and Information Ethics in Information Systems Curricula*. Paper presented at the Information Systems Educators Conference, Columbus, Ohio.
- Lee, A. S. (1997). Researching MIS. In W. Currie & B. Galliers (Eds.), *Rethinking Management Information Systems* (pp. 7-27). New York: Oxford University Press.
- Lessig, L. (1998). *The Architecture of Privacy*. Retrieved December 11, 2006, from http://lessig.org/content/articles/works/architecture_priv.pdf.
- Lindzey, G., & Aronson, E. (Eds.). (1985). *The Handbook of Social Psychology* (3rd ed. Vol. I). New York: Random House.
- Liu, H. (2007). Social network profiles as taste performances. *Journal of Computer-Mediated Communication*, 13(1).
- Liu, H., & Maes, P. (2005). *InterestMap: Harvesting Social Network Profiles for Recommendations*. Paper presented at the International conference on intelligent user interfaces, San Diego, CA.
- Lyytinen, K., Mathiassen, L., & Ropponen, J. (2000). Attention Shaping and Software Risk-A Categorical Analysis of Four Classical Risk Management Approaches. *Information Systems Research*, 9(3), 223-255.
- Ma, M., & Agarwal, R. (2007). Through a Glass Darkly: Information Technology Design, Identity Verification, and Knowledge Contribution in Online Communities. *Information Systems Research*, 18(1), 42-67.
- Maag, C. (2007, December 16). When the Bullies Turned Faceless. *The New York Times*.
- Majchrzak, A., Rice, R., Malhotra, A., & King, N. (2000). Technology Adaptation: The Case of a Computer-Supported Inter-Organizational Virtual Team. *MIS Quarterly*, 24(4), 569-600.

- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355.
- Marcus, M. L. (1994). Electronic mail as medium of managerial choice. *Organization Science*, 5(1), 502-527.
- Mathias, A. (2007, October 6, 2007). The Fakebook Generation. *The New York Times*.
- Milgram, S. (1967). The Small World Problem. *Psychology Today*, 1, 60-67.
- Minch, R. P. (2004). Privacy issues in location-aware mobile devices. *Proceedings of the Hawaii International Conference on System Sciences*, 37, 2019-2028.
- Mintz, J. (2005, December 8). Friendster's 'Eww' Moment. *The Wall Street Journal*, p. B1.
- MySpace. (2006). *MySpace Home Page*. Retrieved March 3, 2008, from www.myspace.com.
- Nunnally, J. (1967). *Psychometric Theory*. New York: Mc-Graw-Hill.
- Ollman, B. (1971). *Alienation: Marx's Conception of Man in Capitalist Society*. Cambridge: Cambridge University Press.
- Orlikowski, W. (1992). The Duality of Technology: Rethinking the concept of Technology in Organizations. *Organization Science*, 3(3), 398-427.
- Payne, J. W., Bettman, J. R., & Johnson, E. J. (1993). *The Adaptive Decision Maker*. Cambridge, UK: Cambridge University Press.
- Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.
- Petter, S., Straub, D. W., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. *MIS Quarterly*, 31(4), 623-656.
- Poole, M. S., & DeSanctis, G. (1989). *Use of group decision support systems as an appropriation process*. Paper presented at the Hawaii International Conference on System Sciences, Hawaii.
- Poole, M. S., & DeSanctis, G. (2004). Structuration Theory in Information Systems Research: Methods and Controversies. In M. E. Whitman & A. B. Woszczynski (Eds.), *The Handbook for Information Systems Research*. Hershey, PA: The Idea Group.
- Putnam, R. D. (2000). *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon and Schuster.

- Read, B. (2006, January 20). Think Before You Share: Students' online socializing can have unintended consequences. *Chronicle of Higher Education*, p. 121.
- Ringle, C. M., Wende, S., & Will, A. (2005). *SmartPLS*. Retrieved February 1, 2008, from <http://www.smartpls.de>.
- Rosenblum, D. (2007). What Anyone Can Know: The Privacy Risks of Social Networking Sites. *IEEE Security and Privacy*, 5(3), 40-49.
- Rosenthal, R., & Rosnow, R. (1991). *Essentials of Behavioral Research: Methods and Data Analysis*. (Second ed.). New York: McGraw Hill.
- Salisbury, W. D., Chin, W. W., Gopal, A., & Newsted, P. R. (2002). Research Report: Better Theory Through Measurement-Developing a Scale to Capture Consensus on Appropriation. *Information Systems Research*, 13(1), 91-103.
- Schneier, B. (2006). *Facebook and Data Control*. Retrieved May 6, 2007, from http://www.schneier.com/blog/archives/2006/09/facebook_and_da.html.
- Schrobsdorff, S. (2006, January 27, 2006). Predators Playground? *Newsweek*.
- Shneiderman, B. (2007). Web Science: A Provocative Invitation to Computer Science. *Communications of the ACM*, 50(6), 25-27.
- Simon, H. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, LXII, 99-118.
- Smith, H. J., Milberg, S., & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, 20(2), 167-196.
- Spring, T. (2007, May 14). *Military Bans YouTube, MySpace, and Other Sites*. Retrieved September 12, 2007, from <http://blogs.pcworld.com/staffblog/archives/004378.html>.
- Stone, B. (2007, May 22). MySpace to Share Data With States on Offenders. *The New York Times*, p. D1.
- Story, L., & Stone, B. (2007, November 30). Facebook Retreats on Online Tracking. *The New York Times*.
- Stutzman, F. (2006). *Student Life on the Facebook*. Retrieved March 2, 2007, from http://ibiblio.org/fred/facebook/stutzman_fbook.pdf.
- Tavani, H. T. (2000). *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Hoboken, NJ: John Wiley and Sons.

- Thompson, J. D. (1967). *Organizations in Action*. New Brunswick, NJ: Transaction Publishers.
- Van der Heijden, H. (2004). User Acceptance of Hedonic Information Systems. *MIS Quarterly*, 28(4).
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward A Unified View. *MIS Quarterly*, 27(3), 425-478.
- Webb, M. (2004). *On Social Software*. Retrieved November 3, 2006, from http://interconnected.org/home/2004/04/28/on_social_software.
- Westin, A. F. (1996). *Harris-Equifax Consumer Privacy Survey*. Atlanta, GA: Equifax, Inc.
- Whitworth, B., & de Moor, A. (2004). *Legitimate by Design: Towards Trusted Virtual Community Environments*. Paper presented at the 35th Hawaii International Conference on System Sciences, Hawaii.
- Whitworth, B., & Whitworth, E. (2004). Spam and the Social-Technical Gap. *Computer*, 37(10).
- Wiredu, G. O. (2007). User appropriation of mobile technologies: Motives, conditions and design properties. *Information and Organizations*, 17(2), 110-129.