EXPLORING THE INFLUENCE OF PRIVACY MANAGEMENT TOOLS ON ONLINE INFORMATION SHARING DECISIONS

By

Muhammad Usman Aleem

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate Studies

(Business Administration)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

October 2012

Abstract

We explore the role of privacy management tools in online social networks and their influence on user's information sharing behavior. Using privacy regulation theory and social capital theory, we first develop a model that characterizes how and why individuals share their private information. Next, we use inclusive and exclusive modes of decision making to develop two tools for sharing information. Subsequently, we test our theoretical model through these tools in the context of online privacy. We find that privacy management tools not only influence sharing decisions when information sensitivity varies, but the tools also influence how individuals interpret their tie strength with their friends.

Preface

This research was conducted in accordance with the suggested ethics guidelines of the Human Ethics of the UBC Research Ethics Board. UBC Behavioral Research Ethics Board approved this research via certificate number H11-02106 October 12, 2011.

Table of Contents

ABSTRACT II

PREFACE III

TABLE OF CONTENTS IV

LIST OF TABLES VI

LIST OF FIGURES VII

ACKNOWLEDGEMENTS VIII

1 INTRODUCTION 9

2 PRIVATE INFORMATION SHARING: DETERMINANTS AND SHARING STRATEGIES 11

2.1 PRIVACY MANAGEMENT MODEL 11

2.1.1 BOUNDARY MANAGEMENT BASED ON SOCIAL CAPITAL 11

2.1.2 INDIVIDUAL CHARACTERISTICS OF USERS 15

2.2 STRATEGIES FOR SHARING INFORMATION 17

2.2.1 MIDDLING OPTIONS IN HIGH AND LOW SENSITIVITY INFORMATION 20

2.3 RESEARCH METHOD 21

2.3.1 FACEBOOK APPLICATION 21

2.3.2 PRIVACY TOOLS AS PROXY FOR INFORMATION SHARING MODES 22

2.3.3 PRE-TESTING AND MEASUREMENTS 25

2.3.4 PROCEDURE 28

2.4 STATISTICAL MODEL AND RESULTS 29

2.4.1 MULTILEVEL MODEL: PARTITIONING OF INDIVIDUAL LEVEL VARIANCE 30

2.4.2 MODEL 31

2.4.3 RESULTS 32

2.5 DISCUSSION 36

2.5.1 THRESHOLD ANALYSIS 38

2.5.2 INTERACTION OF TOOL WITH TIE STRENGTH 40

3 FUTURE RESEARCH DIRECTION 48

3.1 PROTOCOL ANALYSIS 50

3.1.1 PROCEDURE 51

4 CONCLUSION 53

4.1 LIMITATIONS 53

REFERENCES 55

APPENDICES 58

MEASURES, ITEMS AND THEIR SOURCES 58

ITEMS AND THEIR CROSS LOADINGS 59

List of Tables

TABLE 1: TYPES OF INFORMATION SHARED.. 26

TABLE 2: FOUR CONDITIONS FOR EXPERIMENT 1 29

TABLE 3: SUBJECT DISTRIBUTION FOR DIFFERENT TREATMENT CONDITIONS.. 33

TABLE 4: FULL RANDOM INTERCEPT MODEL.. 34

TABLE 5: FULL MODEL WITH TIESTRENGTH*TOOL INTERACTION 41

TABLE 6: COMPARISON OF FULL AND REDUCED MODELS 42

TABLE 7: HIGH SENSITIVITY INFORMATION 44

TABLE 8: LOW SENSITIVITY INFORMATION.. 46

TABLE 9: STEPS LEADING TO INTERVIEW QUESTIONS 51

TABLE 10: CROSS LOADINGS FOR PRIVACY CONCERNS AND PRIVACY AWARENESS... 59

TABLE 11: CORRELATIONS FOR ITEMS IN TIE STRENGTH 60

List of Figures

FIGURE 1: TWO THRESHOLDS AND "MIDDLING OPTIONS" (ADOPTED FROM YANIV ET AL. (2002)) 19

FIGURE 2: TOOL “SHARE WITH”, SHOWING SELECTION OF 4 FRIENDS.. 23

FIGURE 3: TOOL “DO NOT SHARE WITH”, SHOWING SELECTION OF 4 FRIENDS BY REMOVING 16 FRIENDS. 24

FIGURE 4: RELATIONSHIP OF SENSITIVITY OF INFOMATION AND TIE STRENGTH WITH PROBABILITY OF SHARING 36

FIGURE 5: DIFFERENCE BETWEEN SHARING INFORMATION OF LOW AND HIGH SENSITIVITY.. 37

FIGURE 6: FIXED EFFECTS FOR TOOL AND SENSITIVITY 37

FIGURE 7: CHANGING THRESHOLDS (MEANS) WITH TIE STRENGTH AND INFORMATION SENSITIVITY 39

FIGURE 8: INTERACTION OF TIE STRENGTH AND TOOL.. 43

FIGURE 9: INTERACTION OF TIE STRENGTH WITH TOOL WITHIN HIGH SENSITIVITY 45

FIGURE 10: EFFECT OF TOOL WITHIN LOW SENSITIVITY.. 47

Acknowledgements

First and foremost, I would like to thank my advisors, Prof Hasan Cavusoglu and Prof Izak Benbasat, who motivated and guided me throughout the research process.

In addition, I would like to thank Prof Ning Nan for taking the time to read my thesis and being part of my examining committee.

I would also thankful to the graduate students who helped me refine my work with their advice.

Lastly, I would thank Prof Zumbo Bruno for his guidance on the Multilevel Models.

1 Introduction

In this research, we explore the influence of privacy management tools on user's information sharing behavior in the online social networks. In particular, we are interested in the role of privacy management tools on the inconsistent sharing behavior of users when they share personal information with their friends on the online social networks. This inconsistency, also termed as the privacy paradox, is when people seem to share more than their privacy thresholds (Acquisti and Grossklags, 2005) or they seem to be unaware of what they have shared and with whom they have shared (Madejski et al., 2011). This paradox, is attributed to immediate gratification, bounded rationality, psychological distortion and limited information (Acquisti and Grossklags, 2005) and social value (Awad and Krishnan, 2006, Norberg et al., 2007). We postulate and explore that the way individuals use privacy management tools can also influence their information sharing decisions.

Our research questions provide insight to researchers of privacy in IS as well as practitioners who design and implement privacy management tools in online social networks. While the topic of privacy paradox in online social networks is not new to IS research, to the best of our knowledge, this is the first study that focuses on the role of the privacy management tools on inconsistent sharing behavior. In particular, we test the influence of the privacy management tools on the actual sharing behavior and whether these tools lead to discrepancy in online information sharing. To date, the arguments proposed to explain the inconsistent sharing behavior are based on either social value or immediate gratification and bounded rationality, but there is no research that focuses on how privacy management tools influence how individuals disclose information and potentially bias their sharing decisions.

For practitioners, this research provides a model to determine how they can design privacy tools and test the influence on actual sharing decision of users. Currently, there are no clear guidelines on how to develop tools that should lead to better decision making regarding information privacy. Using privacy regulation theory and social capital theory, we first develop a model in which we theorize how and why individuals share their private information. Next, we explore inclusive and exclusive modes of thinking that individuals can use to achieve their privacy goals. Further, we develop privacy tools that mimic these modes of thinking and test them in lab experiments. This helps us determine how individuals use these privacy tools and consequently how these tools influence individual privacy decisions.

The rest of this thesis is organized as follows:

Chapter 2 consists of the study in which we present privacy management theories to model how individuals manage private information. Our focus is on how individuals manage information with different sensitivities and what drives them to share their personal information with different friends on the social network. This theoretical model provides us with basic motivation to share personal information and hypothesize the influence of different modes of thinking, such as including (or adding) friends or exclude (or removing) unwanted friends, on information sharing decisions. Next, we use controlled experiments to investigate the sharing behavior of individuals with different privacy tools designed to stimulate the different modes of thinking in different decision-making scenarios. This allows us to determine the influence of the privacy tools on the actual privacy decisions.

In chapter 3, we present the conclusion and limitations of this study, and finally, in chapter 4, we present future research directions.

2 Private Information Sharing: Determinants and Sharing Strategies

In this chapter, we present privacy management theories to model how individuals manage private information. In addition, we propose two different strategies, modeled on inclusive-exclusive modes of thinking, which individuals can use to share online information with varying sensitivities. Next, we empirically test these strategies of sharing online information of high and low sensitivity and present our results.

2.1 Privacy Management Model

Consistent with the contemporary literature, we define *privacy* as the ability to control one's self disclosure (Smith et al., 2011). Privacy as a control dates back to Westin (1968) and Altman (1975). Altman's theory of privacy is more comprehensive and encompasses other narrower theories that emphasize control (Margulis, 2003a). Since the theory is general and suitable to explain privacy management in social environments in many different contexts, it has also been used in context of privacy as a control in MIS literature (Culnan, 1993, Dinev and Hart, 2004, Smith et al., 1996, Xu, 2007).

We also base our model, which explains how individuals manage their private information in online social networks, on Altman's Privacy Regulation Theory and its later extension in Communication Privacy Management Theory (CPM) (Petronio, 2002). These theories provide a broad conceptualization of how individuals share their information with others based on the type of information and the value attained from sharing. We further the theory by incorporating social capital theory to explain how individuals evaluate the value from sharing.

2.1.1 Boundary Management based on Social Capital

Altman defines privacy as "the selective control of access to the self" (Altman, 1975). We highlight key points of the theory that we adapt to our social networking environment. The first property involves the temporal aspect of interpersonal boundaries; how open or closed we are to others determines process of managing our boundaries. The second property distinguishes between actual and desired level for privacy. At a certain stage, the actual privacy could be higher or lower than what we desire. This in turn relates to the third property that states that privacy is non-monotonic, such that there can be states where the actual privacy is higher than the desired level, leading to social isolation. Conversely, there can be a state of crowding, where the actual privacy is lower than the desired level. In sum, people aim to strive for a balance in their privacy boundaries trying to equate the actual and desired privacy. Communication Privacy Management (Petronio, 2002) further extends this theory by suggesting privacy management as a dialectical process; a process that involves interaction among the people who share someone's private information.

Petronio further extents Altman's theory of privacy by introducing the concept of rule based privacy management and the dialectics required to sustain a certain boundary. Petronio suggests that people share private information within a private or collaborative boundary. These boundaries differ in terms of who is invited to be the part of the boundary. At any stage, a person's information can be private and the person has control over her information. However, a person can reveal this information to someone else thus making the other person privy to her private information. The decision to reveal or conceal the information involves cognitive calculus that accounts for the influence of the cumulative beliefs (Laufer and Wolfe, 1977). The beliefs involve the benefits and the costs of revealing the information. There are costs and benefits of sharing information. The costs are associated with risks of sharing information with the wrong person, at a wrong time or telling too much, benefits include greater social control to the revealer (Petronio, 2002, Margulis, 2003b).

Information can be revealed to one or more persons. Once the information is revealed, the information becomes public and the revealer loses exclusive control over the information. Consequently, the boundary is extended to incorporate more people. The new individual in the collaborative boundary assumes co-ownership of the personal information. The two individuals in this new boundary develop rules on how to manage this information. Therefore, it is prudent that a person reveals information to someone whom the revealer trusts and with whom the revealer can develop effective privacy management rules.

2.1.1.1 Role of Social Capital in Determine Value for Sharing

In an online social network, online information sharing is analogous to CPM's process of revealing information (Metzger, 2007). Individuals develop social networks to acquire benefits and their information disclosure attitude is affected by the value that a social networks offers.

Within online social networks, such as Facebook, individuals create boundaries to include friends to whom they reveal information. The revealing of information to another individual in the social network deleverages individual's control over her private information and in process creates co-owners within the boundary. Consequently, the boundary would be small or large depending on the number of people to whom information is revealed. Consistent with CPM, as individuals reveal information to others, they determine the nature of their private information, to whom they are revealing and consequently how the new co-owners will use this information. How the co-owners use the use information determines the benefits and costs of revealing.

Similarly, revealing or sharing of information in online social networks can have benefits and costs. Individuals share information with other persons to increase their social capital (Wasko and Faraj, 2005). Social capital is the ability of the individual to extract benefit by the nature of membership in social network or any other social structure (Portes, 1998). Coleman (1988) defines social capital by its function and suggests that social capital is inherent in the social structure. This structure in turn is the relation between and among the individuals that form the social network. In terms of measurement, the social capital is dependent on the following: obligations, expectation and trustworthiness of structure. "If A does something for B and trust B to reciprocate in the future, this establishes an expectation in A and an obligation on the part of B." Trust and reciprocity are usually the dominant attributes of a relationship with another person. Tie strength, a cumulative measure of relationship strength with another person, encompasses both trust and reciprocity (Coleman, 1988, Granovetter, 1973, Marsden and Campbell, 1984). The stronger the tie strength, the stronger is the relationship with that person (Krackhardt, 1992), thus greater potential for exchange for information (Garton et al., 1997). This allows us to hypothesize that individuals will share information with people with whom they have strong tie strengths.

H1: Higher tie strength will increase the probability of sharing information with another individual.

2.1.1.2 Role of the Information in Sharing Decision

While there are obvious social benefits of sharing information on OSN, there are costs associated with sharing information. When individual shares information with another person, the individual defers the control of her information to someone on her social network, usually a friend. It becomes the prerogative of the friend on how they want to use this information. The friend might willingly or unwilling decide to violate the rules of information ownership and use information for her own benefit. Consequently, the friend gains social value while the owner of information is harmed. The harm could be financial, social, physical or emotional (Glover and Benbasat, 2010).

Based on CPM, the nature of private information is the one of the main factors in assessing the cost of sharing personal information. When the individual perceives high risk of revealing information, they will conceal (Petronio, 2002). Thus, the boundary in which there is private information of high sensitivity, there will probably be none or a few people. An individual will share sensitive information with another person if she trusts that the other person would not misuse or jeopardize her trust. As the individuals perceive greater value for sharing, they will expand the boundary. This is also consistent with commoditization aspect of personal information where individuals evaluate cost and benefits of their information and share information if they perceive greater value (Campbell and Carlson, 2002, Davies, 1997). Therefore, as the potential for the value increases, individuals will include more people within their boundary. The private information in a larger boundary is ought to be less sensitive, consequently has a very low of harm.

Therefore, as the sharing of information with another individual is dependent on the calculus of benefits emerging from tie strength and costs emerging from sensitivity of the information, the individuals will form a restricted boundary for highly sensitive information and include few friends, and form a larger boundary for less sensitive information with a greater number of friends.

> H2: Higher sensitivity of information will lower the probability of sharing information with another individual.

In addition, we propose an interaction between sensitivity of information and the tie strength. As the sensitivity of the information decreases, individuals will try to maximize the benefits by increasing their sharing even if the tie strength is low. Granovetter (1973) showed that weak ties can be as important as the strong ties. Individuals can glean non-redundant value that they cannot get from their strong ties. College students can benefit from developing and maintaining weak ties to get future references for employment (Ellison et al., 2007). Similarly, people can get advise on subjects they are not familiar with (Constant et al., 1996). Consequently, given that the sensitivity of the information is low, the individual will share information with other people on the social network with low tie strength. That is, the impact of tie strength on sharing information extenuates as the information to be shared becomes less sensitive.

> H3: Tie strength will lead to greater probability of sharing information only when sensitivity of information is high as compared to when sensitivity of information is low.

2.1.2 Individual Characteristics of Users

CPM theory suggests individuals vary in their perceptions associated with benefits and risk of disclosing information (Metzger, 2007, Petronio, 2002). This is consistent with privacy studies which are not based on CPM (Pavlou et al., 2007, Angst and Agarwal, 2009) and other studies investigating online information disclosure (Culnan, 1984, Rafaeli and Raban, 2005). The extant literature argued and showed that an individual's privacy concerns related to sharing information online should influence her sharing behavior (Culnan and Armstrong, 1999, Dinev and Hart, 2006a, Phelps et al., 2000, Malhotra et al., 2004). Drawing on the findings of past research, we postulate that an individual's privacy concerns should negatively influence her decision of sharing information with another person. In addition, these concerns are moderated by the tie strength. If the tie strength between two individuals is high, then individual's privacy concerns would be alleviated and the individual would share the information. This is because privacy concerns stem from individual perception of how their friends will use or misuse private information. Tie strength, however represents the strength of a relationship between two people. Consequently, if the tie strength is high then the sharer of information will not be concerned about misuse and her privacy concerns will lowered.

> H4a: High privacy concerns should lower the probability of sharing information with another individual.
>
> H4b: Compared to when tie strength is low, influence of privacy concerns on sharing information will be lower when the tie strength is high.

Moreover, individual's awareness of privacy related issues should also affect their sharing behavior (Bulgurcu et al., 2010). Privacy awareness is related to an individual's general understanding of contemporary privacy related issues and her knowledge of the costs and risks associated with sharing information on online social networks can pose (Schrammel et al., 2009, Bonneau and Preibusch, 2010). Consequently, an individual who is more aware of the privacy threats will be more cautious towards sharing information. In addition, similar to hypothesis 4b, we would expect the influence of privacy awareness to taper when the tie strength is high. An individual's privacy awareness will influence her general sharing behavior whenever she considers sharing information with another person. However, if the friend under consideration has high tie strength with her, then the general perception about sharing information would have lower influence, since a friend with high tie strength will not misuse the information. Consequently, when the tie strength is high the influence of privacy awareness will be reduced.

> H5a: High privacy awareness should lower the probability of sharing information with another individual.

> H5b: Compared to when tie strength is low, influence of privacy awareness on sharing information will be lower when the tie strength is high.

2.2 Strategies for Sharing Information

As proposed in the previous section, individuals create boundaries in which they include people with whom they want to share information. In online social networks, creating such a boundary can be achieved by selecting certain friends from among all the friends on an individual's social network. Furthermore, individuals control their privacy using privacy tools afforded on the OSN platform. In this section, we propose that people on OSNs can share their private information using two broad modes of thinking: *inclusive* and *exclusive*. Inclusive mode is akin to selecting items from a set of choices, while exclusive mode is similar to removing the unwanted options from a set and retaining the rest (Yaniv et al., 2002, Levin et al., 1998). Since sharing of information in OSNs is similar to selecting friends from all the friends, either inclusive or exclusive mode can be used to select the appropriate set of friends. In addition, we propose using inclusive mode of thinking is better when sharing sensitive information and using excluding mode of thinking is better when sharing less sensitive information.

Using the ideas of CPM theory, we propose that the goal of sharing information on OSNs is similar to developing a boundary around the personal information and by including or excluding friends. When sharing information on an online social network, the individual has to determine the friends with whom they want to share the information. These friends can be selected by eliminating those friends who possess very low tie strength, thereby retaining friends who possess positive attributes. Alternatively, one can directly select friends with high tie strength. The former strategy is exclusion and the later one is inclusion.

When individual wants to share information with high sensitivity, we expect that the boundary containing such information would be very restricted. There would be a very few co-owners or friends within that boundary. The individual would only add these friends if the individual they have high tie strength with them. Essentially, the friends within the boundary are not likely to misuse the information or to harm the owner of the information. Similarly, when individual wants to share information with low sensitivity, we would expect the boundary to be loose and contain many friends. The lax boundary would provide the individual an opportunity to obtain maximum benefits of sharing information with more people with less exposure to potential risks as the information is less likely to be misused in order to cause any significant harm.

Both sharing tasks can be achieved using either inclusive or exclusive modes. While procedurally these modes appear to be identical to each other and should lead to the same results, it has been shown that they are not the same (Yaniv and Schul, 2000). In general, compared to inclusive mode, exclusive mode leads to a high probability that a given option would be retained in the choice set (Yaniv et al., 2002). This discrepancy has been shown to exist in various of multi-attribute choice settings, such as screening the job candidates and choosing the car to purchase. When screening job candidates, subjects who used ‘accepting’ (i.e., inclusion) strategy selected fewer candidates as compared to the subjects who used ‘rejecting’ (i.e., exclusion) strategy (HuberMargaret A and Northcraft, 1987). Similarly, when subjects were asked to narrow down a set of selection from among 24 different types of cars, those who were asked to ‘include’ selected fewer cars as compared to those who were asked to ‘exclude’(Levin et al., 1998).

Inclusion-exclusion discrepancy is due to the 'middling' options (Yaniv et al., 2002). When individuals are offered a choice set, they have two thresholds: a threshold for inclusion and one for exclusion. All the options above the inclusion threshold are guaranteed to be selected. Similarly, the options that are below the exclusion threshold are guaranteed to be removed. These options have a clear-cut fate.

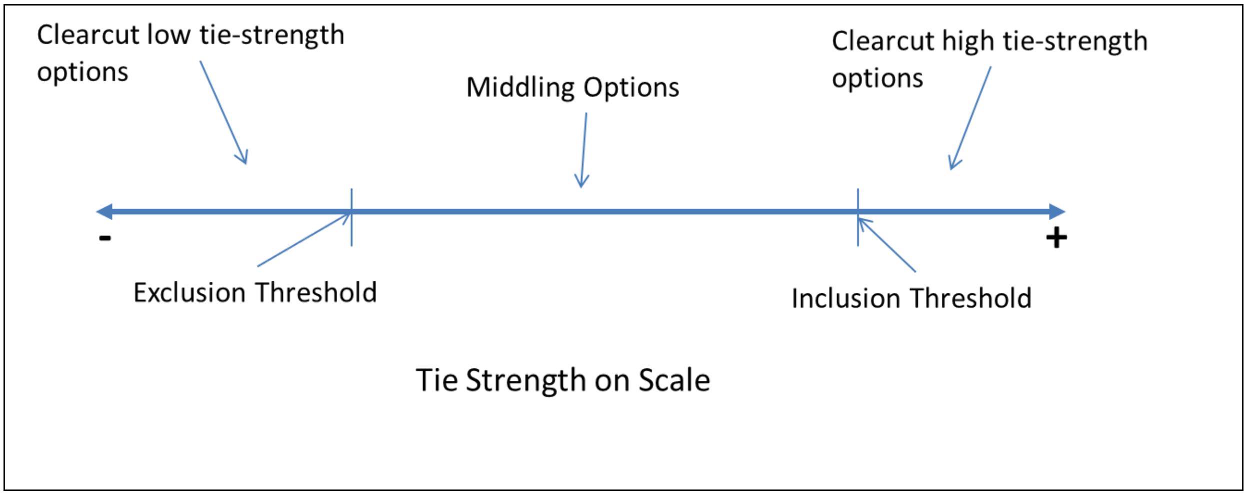


Figure 1: Two Thresholds and "Middling Options" (adopted from Yaniv et al. (2002))

The discrepancy occurs when an individual using exclusion mode does not exclude an option from the choice set with value lower than the inclusion threshold but higher than the exclusion threshold. Another way of saying is that an option that fails to meet the inclusion criteria is not necessarily removed. This is because the individual assesses an option worthy to be excluded only if its score in the evaluation criteria is sufficiently lower than the inclusion threshold. Consequently, options in the middling range are "retained".

We conjecture that a similar discrepancy would surface in our context. When choosing from among a set of friends based on the tie strength, these two thresholds emerge. Accordingly, friends who have sufficiently high tie strength are placed above the inclusion threshold and friends with sufficiently low tie strength are placed below the exclusion threshold. Additionally there are some friends in the middling category. Thus, if an individual is asked to decide two sub-sets, one which the information is shared to and the other which the information will not be shared to, it is expected that two non-complementary sharing results would be obtained when a different mode of thinking is used. Consistent with (Yaniv et al., 2002, Mourali and Nagpal, 2011, HuberMargaret A and Northcraft, 1987), the number friends that information will be revealed to using inclusive mode would be lower than the number of friends that information will be revealed to using exclusive mode.

2.2.1 Middling Options in High and Low Sensitivity Information

In this section, we show that while an individual might want to share information with high or low sensitivity, inclusive mode will always lead to lower sharing as compared to exclusive mode.

When an individual wants to share information with high sensitivity, their objective is to select a few friends with whom they have high tie strength. Using inclusive mode, this is simple task of selecting those friends that meet the inclusion criteria and not considering the rest. On the other hand, if individuals use exclusion criteria, they will remove the friends that fall below the exclusion threshold, but not the friends that lie between the two thresholds, the middling options. Therefore, individuals will share with more friends when using exclusive mode as compared to inclusive mode. This relates to a state of personal privacy in which the desired privacy is less than actual privacy and the individual will be overcrowded and feel less control over their privacy.

Conversely, when individuals intend to share information with low sensitivity, as the potential of harm is low, they would seek to maximize the social value by sharing with as many friends as possible. When using inclusive mode, the individuals will find many friends that are above the inclusion threshold for the low sensitive information and not consider the rest. On the contrary, when the individuals use exclusion mode, they can find friends (albeit fewer than the high information sensitivity case) who fall below the exclusion threshold and remove them from the choice set, thus retaining the middling options. Therefore, the resulting boundary would be less restrictive when using exclusive mode as compared to inclusive mode. Since the goal of sharing low sensitivity information is to maximize the value of sharing, using inclusive mode would lead to a restrictive boundary, leading to a privacy state in which actual privacy is greater than desired privacy and causing isolation.

In general, when sharing information with different sensitivities, while the goals of sharing might differ, using exclusion mode the subjects would share with more friends as compared to using inclusion mode. The difference arises as the middle options are retained in the exclusion mode but not in the inclusion mode.

> H6: There is a lower probability of sharing with a friend when using inclusive mode than with exclusive mode.

2.3 Research Method

The purpose of this study is to understand the drivers of information sharing on online social networks and explore the influence of privacy management tools on the individual information sharing. We developed a theoretical model in which we propose how and why individuals share information. In addition, we hypothesize two modes of sharing and how these modes would influence the sharing decisions. We tested these hypotheses as experiments in a lab. Performing the experiment in the lab allowed us more control over the environment in which the subjects interact with the technology artifact enabling information sharing.

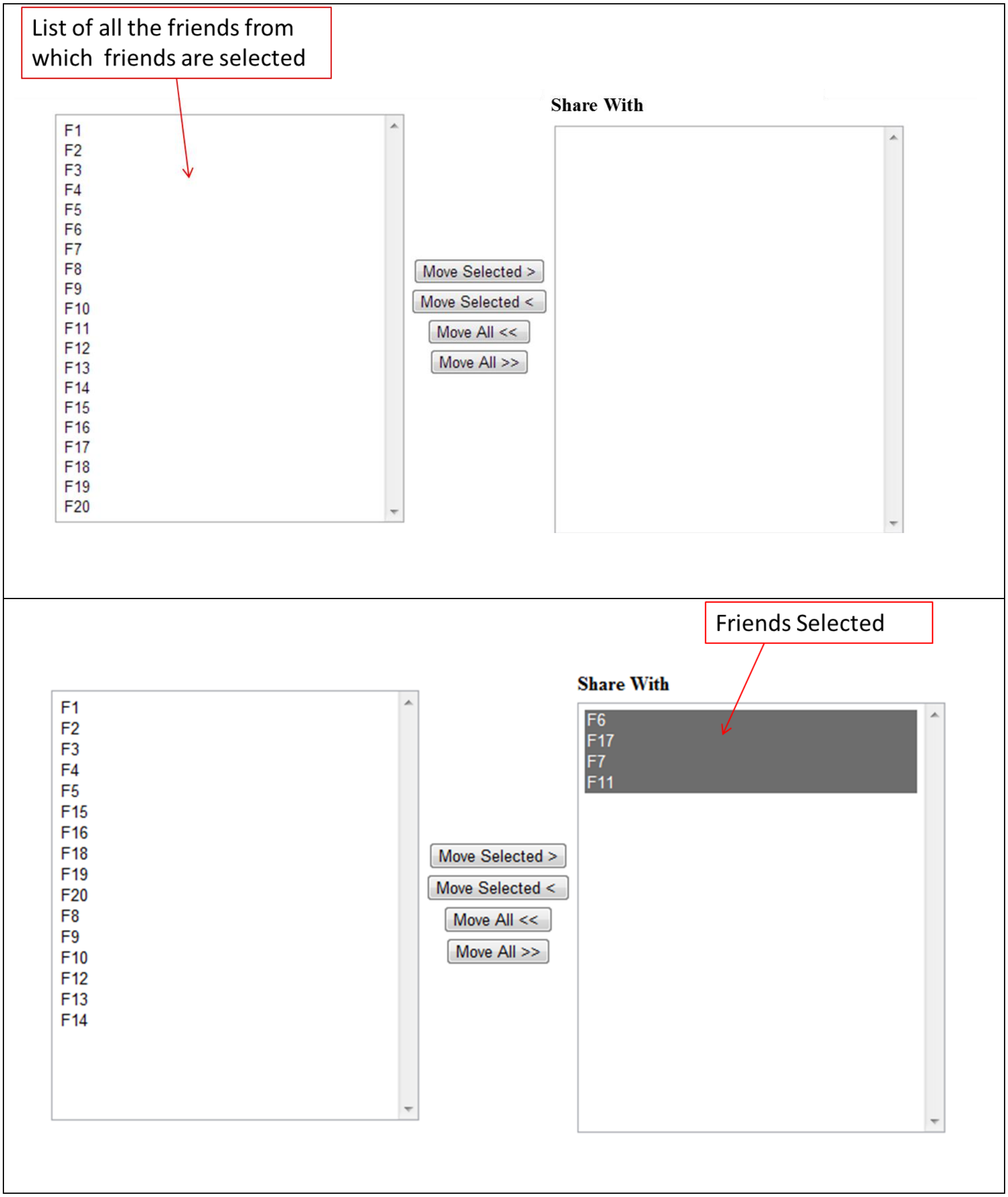
2.3.1 Facebook Application

We developed a Facebook application that subjects could link to their Facebook profile. This allowed us to gather friend related information from subject's profile on Facebook. The information gathered includes the names of friends, demographic information of the subjects and her friends such as gender, age etc.

Accessing information about friends allowed us to create realistic sharing scenarios to test our hypotheses. The scenarios describe situations in which subjects decide to share some personal information.

2.3.2 Privacy Tools as Proxy for Information Sharing Modes

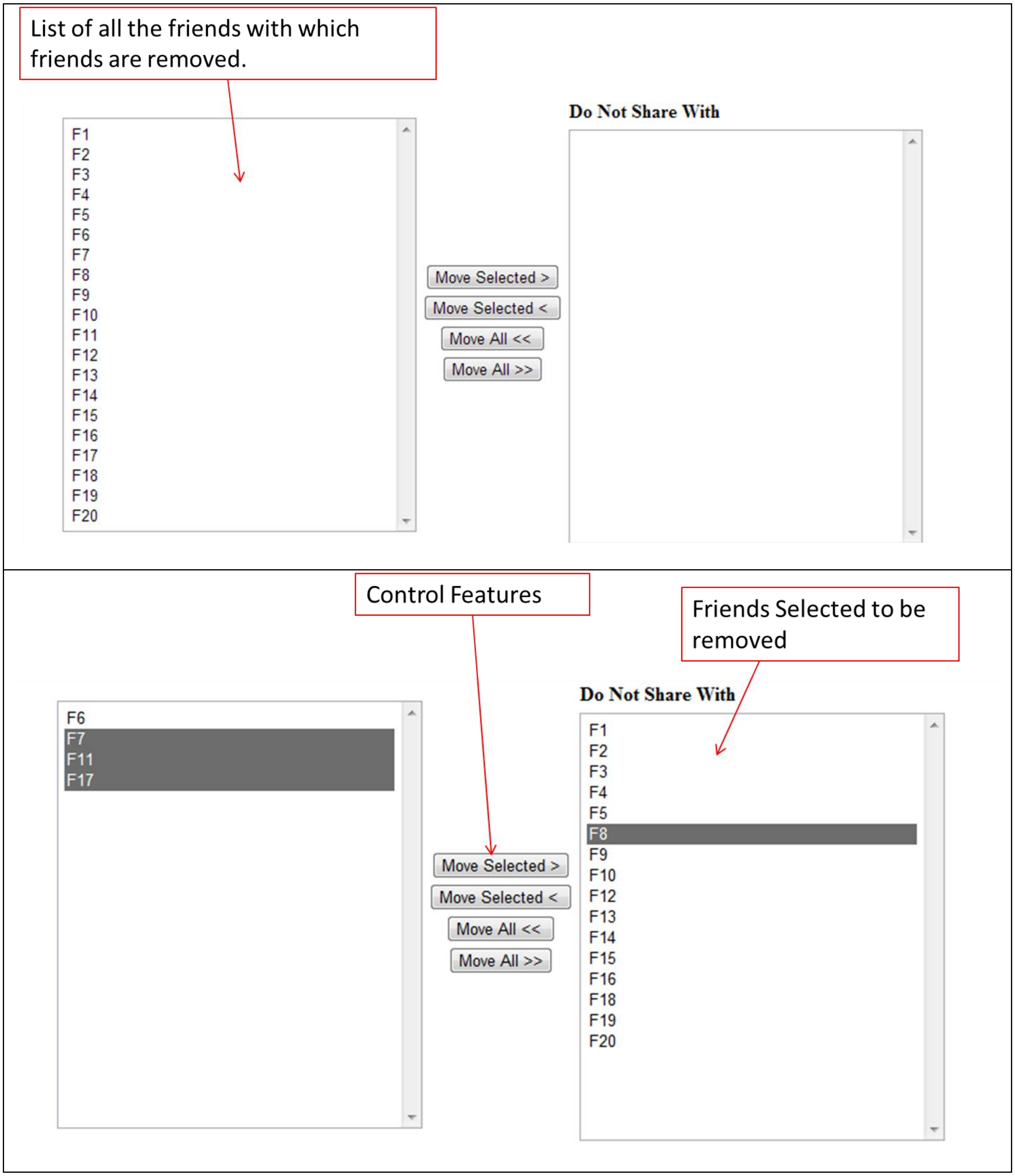
In order to operationalize our two strategies of decision-making, we develop two simple privacy controls that allow us to model these decision-making strategies. The two strategies have two corresponding tools that help individuals in making appropriate decisions: (i) “Share With” (SW) and (ii) “Do Not Share With” (DN). The former is procedurally consistent with the inclusive mode of thinking where an individual chooses from a set of friends with whom they want to share information. The latter relates to the exclusive mode of thinking where the individual removes people from a larger set until she is content with the remaining set, a set of friend to whom information is revealed.



List of all the friends from which friends are selected

Friends Selected

Figure 2: TOOL "Share With", showing selection of 4 friends



List of all the friends with which friends are removed.

Control Features

Friends Selected to be removed

Figure 3: TOOL "Do Not Share With", showing selection of 4 friends by removing 16 friends.

The privacy management tools that we designed will induce different mode of thinking when making sharing decision. For instance, if the individual was asked to share information using SW, then she would seek the friends with high tie strength, thus inducing inclusive mode where she seeks friends with high tie strength that are above the inclusive threshold. Similarly, when using DN, she would seek friends with sufficiently low tie strength that can be removed from the choice set. This would be equivalent to exclusive mode where the she would seek to remove friends with low tie strength that fall below the exclusion threshold and retaining the middling options. Drawing on the inclusion-exclusion discrepancy (Yaniv et al., 2002), an individual's sharing behavior will be directly influenced by the privacy tools and the strategy afforded by the privacy tools. In particular, as compared to privacy tool DN, the privacy tool SW will lead to sharing of information with fewer friends. This is because the tool DN will lead to sharing with a few additional friends that would not be considered using SW.

Given that tools can offer differing modes of sharing and influence sharing behavior, tool themselves can offer features that can hinder sharing and lead to inconsistent behavior. Since the focus of our study is to determine the impact of the strategies offered by the tool, we ensured that the tools offer same features and the same usability. In addition, to avoid confounding in our results, the features set provided should not benefit one tool over the other. Further, we ensured that the tools are easy to understand and easy to use by including common features such as buttons for selecting multiple friends using "ctrl-click" and "select-all".

Figure 2 and Figure 3 show how the tools can be used to share information with 4 friends. Initially, the left column shows list of all the 20 friends and subjects select friends either to share or not to share with the information based on the type of the tool.

2.3.3 Pre-Testing and Measurements

In our experiment, sensitivity of the information and privacy tools were used as treatments. All the perceptual measures and their items are presented in the appendix.

2.3.3.1 Sensitivity

Since information sensitivity is relative to each individual, we have the subject rate how sensitive she perceives different information items. This helped us determine subject's perception about sensitivity of information (Hui et al., 2007). In first pre-test, we generated 35 different categories of personal information that subjects can potentially share on the social network. Then, we had a set of 22 subjects rate the sensitivity of these information types on a 7-point scale. This gave us a spectrum based on sensitivity of the information items for each subject. From these, we choose 20 information items that would maximize the variance for each subject to include in the main study. This would essential to create scenarios for high and low sensitivity. The final selection of information items are presented in Table 1.

Facebook Status	Status Picture
Family Members Information	Relationship Status
Biography	Religious Views
Birthday	Political Views
Home Address	Current Location
Current Debt	Office Address
Undergraduate GPA	Current Salary
Friend I Love the Most	Friend I Like the Least
Pictures of Family Members	Email
Pictures of Last Halloween Party	Pictures of Partner

Table 1: Types of Information Shared

2.3.3.2 Privacy Tools

In the second round of pretesting, our focus was on the information provided for each privacy tool. We wanted to ensure that subjects accurately interpret the strategy offered by the privacy tool so that they can make their sharing decision. Using interviews and subjective responses, we performed multiple changes.

Some concerns arose, as the subjects seemed to be primed when we used words such as “privacy controls”. These words were changed to “information sharing tools”. Another problem arose with the names of the privacy tools: “Share With” and “Do Not Share With”, as subjects seemed to prefer “Share With” as it has some positive connotations. Framing effects have been known to influence decision makers (Kahneman and Tversky, 1984, Tversky and Kahneman, 1986). While such effects are relevant to our domain, our focus is on the actual strategy employed by the privacy tool rather than the effect caused by the name of the privacy tool. This framing effect was removed by giving neutral names to these tools: Tool A and Tool B, respectively.

Another issue we encountered during the pre-testing was that subjects seemed to rush through the study. We catered this with using two-pronged approach. First, we offered additional incentive of CAD 25 to subjects. This prize was to be awarded to two randomly selected subjects based on the quality of their responses in the open-ended questions. Secondly, we slowed down the usage of the tool by increasing the number of pages and thus spreading out the information that subjects needed to read to understand the tool. Both strategies helped as the average time spent on using the tools increased, in addition in the interviews the subjects seemed clearer about the strategies offered by the tools.

2.3.3.3 Tie Strength

Another determinant of information sharing is the Tie Strength with the person with whom the information is shared. We focus on the asymmetric attributes of a social network to control for the influence of different level of ties in a social network. These attributes only focus on individual’s interpretation of her social network’s properties. We use the approach by (Granovetter, 1973), who defines tie strength as “a (probably linear) combination of the amount of time, the emotional intensity, the intimacy (mutual confiding), and the reciprocal services”. The measures were adopted from Gilbert and Karahalios (2009). These subjective measures were shown to represent 85% of the variance of the actual tie strength between two friends based on real information exchange on Facebook.

2.3.3.4 Individual Privacy Characteristics

Privacy concerns and privacy awareness were included to account for individual's privacy characteristics. Privacy concern measures were adopted from (Dinev and Hart, 2006b) and modified for our study while privacy awareness measures were adopted from (Bulgurcu et al., 2010).

2.3.3.5 Dependent Variable: Sharing Decision

Our dependent variable reflected individual's decision of whether the individual shares or not shares information with a friend. This sharing was represented in terms of choice and thus we had a binary variable where '1' represented that individual chose to share information with their friend and '0' represented that individual did not choose to share information with their friend.

2.3.4 Procedure

The experiment was a between-subject across different levels of sensitivity and privacy tool. We recruited subjects at a North American university campus and who were compensated CAD10 for their time. The subjects first subscribed to our experiment application. This is the process by which subject add a third party application to their profile on Facebook. As subjects subscribe to the application, they also authorize the application to access certain information from their profile. This is one of the reasons that we performed our experiments in the lab as it provided us the opportunity to pacify any concerns that arose due to data access. In order to protect the identity of the subjects and their friends we had designed the application to code alpha-numerically all identifiable information such as names of the subjects and their friends. The application collected the subject's gender, date of birth and total number of friends. In terms of friends, the application randomly selected 20 friends from total list of friends. The application collected their names, date of birth and gender.

At the first screen, the subjects were provided basic information about the experiment and were informed of the additional incentive of winning $25 for the quality of their responses in subjective feedback. Next, the subjects revealed the sensitivity of 20 different types of personal information by rating each on a 7-

point scale. Using this rating, the application sorted information items based on each subject's level of sensitivity. This allowed us to find which personal information was most or least sensitive for the subject. The application then randomly assigned each subject to one of the four experimental scenarios. These scenarios are shown in Table 2**.** Based on the scenario and actual rating of sensitivity of the information, the application asked the subjects to share the most (or least) sensitive information item using one of the tools, either SW or DN depending on the scenario the subject was randomly assigned. The application selects 20 friends from the subject's Facebook account and presents them as a list of friends to be considered for the sharing decision. Once the subjects have made their sharing decision, they were asked to rate the "tie strength" for each of the 20 friends (chosen earlier) in their list. Although this can be an arduous task, we used the technique followed by Gilbert and Karahalios (2009), in which they were able to have subjects rate an average of 63 friends in period of 30 minutes. In our experiment, subjects spent most of the time on rating friends. On average, our studies took 25 minutes to finish, where subjects spent around 15 minutes on rating their friends. Finally, subjects rated their privacy concerns and privacy awareness rate on a 7-point scale.

Scenarios	Sensitivity of Information	Tool provided
Scenario 1	Low Sensitivity	Share With (SW)
Scenario 2	Low Sensitivity	Do Not Share With (DN)
Scenario 3	High Sensitivity	Share With (SW)
Scenario 4	High Sensitivity	Do No Share With (DN)

Table 2: Four Conditions for Experiment 1

2.4 Statistical Model and Results

Since one of the objectives of this study is to determine the influence of privacy tools on individual level decision making, we have to ensure that our between-subject design allows us to infer the influence on sharing decisions at the individual level. Conventional methods use control variables to manage the individual effects in the model. Our model on the other hand has multiple ratings within a same subject. It is evident from our data that we have a multilevel model as individual ratings are nested within subjects. Therefore, if we were to consider the model to be single level, our explained variance would be inflated (Hox, 2010) and consequently incorrect interpretation of level-1 fixed effects. In addition, since each subject performs 20 ratings, modeling this as single model would also violate the independence assumption (Krull and MacKinnon, 2001) as groups of ratings are influenced by different raters.

2.4.1 Multilevel Model: Partitioning of Individual Level Variance

Modeling the data as multilevel allows us to enjoy the advantage of partitioning individual level variance and to parse out the impact of the fixed effect variables involved in sharing decision without individual effects. This method is similar to the classic example of models involving nested data, where students are nested within organizational context of classrooms and schools. Multilevel model allowed such data to model within-class variance, which is the variance among the students and between-class variance, which is the variance due to different classes. The between class attributes is usually due to higher-level variables such as teachers (Bryk and Raudenbush, 1988).

Similarly, our data is nested within the individuals. The multilevel model allows us to partition the sharing decision variance within the individual and among the individuals. When viewed from the point of view of "measures within subjects", multilevel modeling can be shown to test hypotheses comparable to those tested by repeated measures analysis of variance (Gardner, 2008, Osborne, 2000, Ellis, 1999). For variance within individuals, we are solely interested in the influence of the determinants of sharing described in previous sections, these attributes include sensitivity of the information, tie strength with the person, decision making strategy afforded by the privacy tool, which could be either inclusive or exclusive and the interaction between sensitivity and tie strength. Since each individual is different and can perceive these attributes differently, we need to cater for variance among the individuals. Multilevel modeling helps us model the between-individual variance, thus improving our estimates of direct determinants of the sharing decision.

Assuming that we have a multilevel model, the next step is to determine how the higher-level variables affect the outcome of sharing with a friend. In our context, the individual level attributes, privacy concerns and privacy awareness are the higher-level variables. These individual level characteristics can affect the outcome in two ways: 1) random intercept, influence the intercept so that each subject has a different sharing threshold from which they share and/or 2) random slope, influence their perception contribution of sensitivity of information on likelihood of sharing, leading to difference in the slopes for each subject. Hence, depending on how the higher-level variables influence the sharing, three models are possible. We tested all three models and based on comparison of robust standard errors (Raudenbush, 2004) [1], only random intercept model showed statistically significant results.

2.4.2 Model

The experiment allows us to capture data at individual sharing level. We had all the subjects determine whether they want to share their information with each of their friends, providing us with 20 sharing decisions per subject. Each decision can be modeled as a binary of whether the information was shared or not shared with the friend. Thus, the outcome of decision to share with a friend is a logit-link function of

[1] In order to determine the stability of the model, we compare the results of unit-specific model's standard error with their robust standard errors. A significant difference shows that the estimate of random component of the model is not stable and the fixed effects cannot be interpreted. A model can have unstable error estimates in the presence of significant fixed effects. Since only the results for random intercept were stable under different methods of estimation methods, we discarded other models.

sensitivity of the information (to be shared), tie strength with the person with whom information is shared and the tool used to make the decision. Sensitivity is coded high=1 and low=0 respectively and similarly the tool was coded SW=1 and DN=0. Tie strength is a continuous variable, which was the linear sum of the five items adopted from (Gilbert and Karahalios, 2009). In addition, tie strength was group centered thus removing the individual influence on the tie strength. This allows us to interpret the intercept as the expected outcome for a sharing decision of a subject j, whose covariate values are equal to the subject's j means (that is, the mean across all the decisions by the subject j). This is helpful in separating the between-group and the within-group components from the total variation to investigate how subjects affect the sharing decision, explicitly accounting for the group structure into the model (Enders and Tofighi, 2007).

In all, there were 760 decisions nested within 38 subjects.

2.4.3 Results

42 subjects took part in the study. We averaged the time spent on using the tool during the experiment and if subjects spent time lesser than 2 standard deviations than the average time spent, the results were dropped. In addition, we also read the subjective responses to determine whether spending such low time was due to lack of interest or just quick a response. Consequently, based upon the time spent and subjective responses, 4 subjects were dropped from the analysis. Eventually, we had 38 subjects whose results were used in model. Among these 38 subjects, we had 19 subjects equally distributed in low and high sensitivity conditions. Within high sensitivity condition, 11 subjects used SW tool while 8 subjects used DN tool. In the low sensitivity condition, 10 subjects used SW tool, while 9 subjects used DN tool. These statistics are summarized in Table 3.

		Tool		Total
		SW	DN	
Sensitivity	LOW	10	9	19

	HIGH	11	8	19
Total		21	17	38

Table 3: Subject Distribution for Different Treatment Conditions

2.4.3.1 Reliability of Constructs

All constructs have Cronbach's alpha greater than 0.70, which showed internal consistency of the measures (Cronbach, 1951, Cortina, 1993). Factor loadings across the items are presented in the appendix.

2.4.3.2 Full Random Intercept Model

Error! Reference source not found. shows the results of full random intercept model, only the intercept s modeled as random while we have privacy concerns interacting with sensitivity of the information. The model can be mathematically represented as follows:

Level 1:

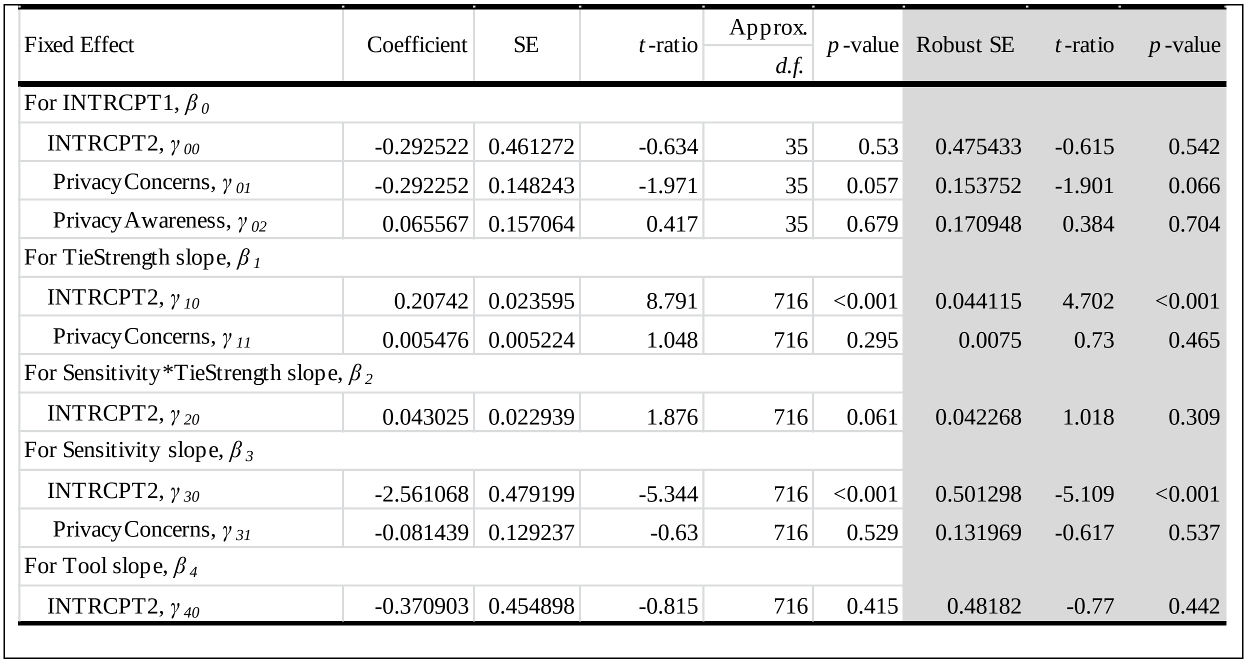
$$\text{Probability } (Shared_{ij}=1|\beta_j) = \phi_{ij}$$
$$\log[\phi_{ij}/(1 - \phi_{ij})] = \eta_{ij}$$

$$\eta_{ij} = \beta_{0j} + \beta_{1j}*(TieStrength_{ij}) + \beta_{2j}*(Tool_{ij}) + \beta_{3j}*(Sensitivity*TieStrength)_{ij}* + \beta_{4j}*(Sensitivity_{ij}) \qquad \textbf{(1)}$$

Level 2:

$$\begin{aligned} \beta_{0j} &= \gamma_{00} + \gamma_{01}*(PrivacyConcerns_j) + \gamma_{02}*(PrivacyAwareness_j) + u_{0j} \\ \beta_{1j} &= \gamma_{10} + \gamma_{11}*(PrivacyConcerns_j) \\ \beta_{2j} &= \gamma_{20} \\ \beta_{3j} &= \gamma_{30} + \gamma_{31}*(PrivacyConcerns_j) \\ \beta_{4j} &= \gamma_{40} \qquad \textbf{(2)} \end{aligned}$$

The equations above show a random intercept model with equation (1) showing the Level-1 relationship among the factors that determine subject's choice of sharing with his friend. $\boldsymbol{\eta}_{ij}$ is a single sharing decision, where i is the friend with whom information is shared or not shared and j is the individual sharing the information. $\boldsymbol{\beta_0}$ is the intercept for each individual and shows the group difference (decision for each subject). This Equation (2) shows that $\boldsymbol{\beta_0}$ is influenced by the individual attributes of privacy concerns, and privacy awareness. It has been modeled as random so that individual variance is incorporated by its fluctuation. Thus each individual's attributes, privacy concerns and privacy awareness, influences their privacy decision making. These attributes are represented as the sum of grand mean individual variance.



Fixed Effect	Coefficient	SE	*t*-ratio	Approx. *d.f.*	*p*-value	Robust SE	*t*-ratio	*p*-value
For INTRCPT1, β_0								
INTRCPT2, γ_{00}	-0.292522	0.461272	-0.634	35	0.53	0.475433	-0.615	0.542
PrivacyConcerns, γ_{01}	-0.292252	0.148243	-1.971	35	0.057	0.153752	-1.901	0.066
PrivacyAwareness, γ_{02}	0.065567	0.157064	0.417	35	0.679	0.170948	0.384	0.704
For TieStrength slope, β_1								
INTRCPT2, γ_{10}	0.20742	0.023595	8.791	716	<0.001	0.044115	4.702	<0.001
PrivacyConcerns, γ_{11}	0.005476	0.005224	1.048	716	0.295	0.0075	0.73	0.465
For Sensitivity*TieStrength slope, β_2								
INTRCPT2, γ_{20}	0.043025	0.022939	1.876	716	0.061	0.042268	1.018	0.309
For Sensitivity slope, β_3								
INTRCPT2, γ_{30}	-2.561068	0.479199	-5.344	716	<0.001	0.501298	-5.109	<0.001
PrivacyConcerns, γ_{31}	-0.081439	0.129237	-0.63	716	0.529	0.131969	-0.617	0.537
For Tool slope, β_4								
INTRCPT2, γ_{40}	-0.370903	0.454898	-0.815	716	0.415	0.48182	-0.77	0.442

Table 4: Full Random Intercept Model

2.4.3.3 Full Random Intercept Model

Table 4 shows the estimation for full maximum likelihood for the full random intercept model. The reliability estimate of the random intercept $\boldsymbol{\beta_0}$ was 0.82. This showed that in addition to the two factors attributed to individual's sharing behavior (privacy concerns and privacy awareness), there is additional variance that is not explained by the variables, but is captured by the model. Thus, our model allows us to predict the sharing results as consequence of our fixed variables while it separates the individual level variance from the fixed effects. The variance explained by the random coefficient is significant, where $u_{0j} =$ 5.78 (χ^2=385, df=35, p<0.001).

First, we consider the influence of level-2 effects. Both the interactions proposed in hypothesis 4b and 5b are not significant, shown by γ_{11} and γ_{31}. We had proposed that privacy concerns would influence how individuals evaluate tie strength and sensitivity of the information shared. It seems that subjects focus on the aspects of tie strength and sensitivity without the influence of their privacy concerns. Neither their privacy concerns nor privacy awareness of the individuals influence the sharing decisions as shown by non-significant γ_{01} and $\gamma_{02,}$ thus rejecting hypotheses 4 and 5. This does not include the additional individual level variance that is represented by u_{0j}. In other words, while privacy concerns and privacy awareness are not significant and do not influence the intercept for each individual, there is additional explicitly identified individual level variance reflected by u_{0j}. (Neter et al., 1996).

The significant results for the tie strength and sensitivity of information, shown by significant γ_{10} and γ_{30}, confirm hypothesis 1 and 2. As the sensitivity increases, it negatively affects the sharing behavior and the probability of sharing with a friend decrease significantly. Similarly, the tie strength also determines whether the subject will share information with that friend. Although, the coefficient is lower than sensitivity but it is still significant. The interaction between sensitivity and tie strength (γ_{20}) proposed in hypothesis 3 is not significant, In addition, there is a difference in the standard and robust errors for the interaction term of sensitivity and tie strength, showing that this fixed effect is either not significant or unstable. This is usually due to the non-normal distribution of the residuals. In this case, the fixed effects of such terms cannot be used for meaningful inference. Lastly, tool does not turn out to be a significant predictor of sharing. We discuss the hypothesis 6 in next section.

2.5 Discussion

One of the purposes of the study was to explore how two different modes of thinking, reflected as online privacy management tools, influence the privacy decision making of an individual. In addition, we postulated that when subjects share using inclusive mode (SW) the probability that they would select a friend would be lower as compared to the probability selecting a friend when using exclusive mode (DN). This is due to the middling options that are considered when subjects use the exclusive mode. For experimental purpose, our application provided a set of 20 friends at time of decision making. Thus, subjects had to sift through a list of 20 friends and then include or exclude a corresponding set of friends from the list (depending on the privacy tool provided).

For hypothesis 1 and 2, the results validate our model. Figure 4 shows the probability of sharing information given the sensitivity of the information and tie strength, with rest of the variables held at their mean.

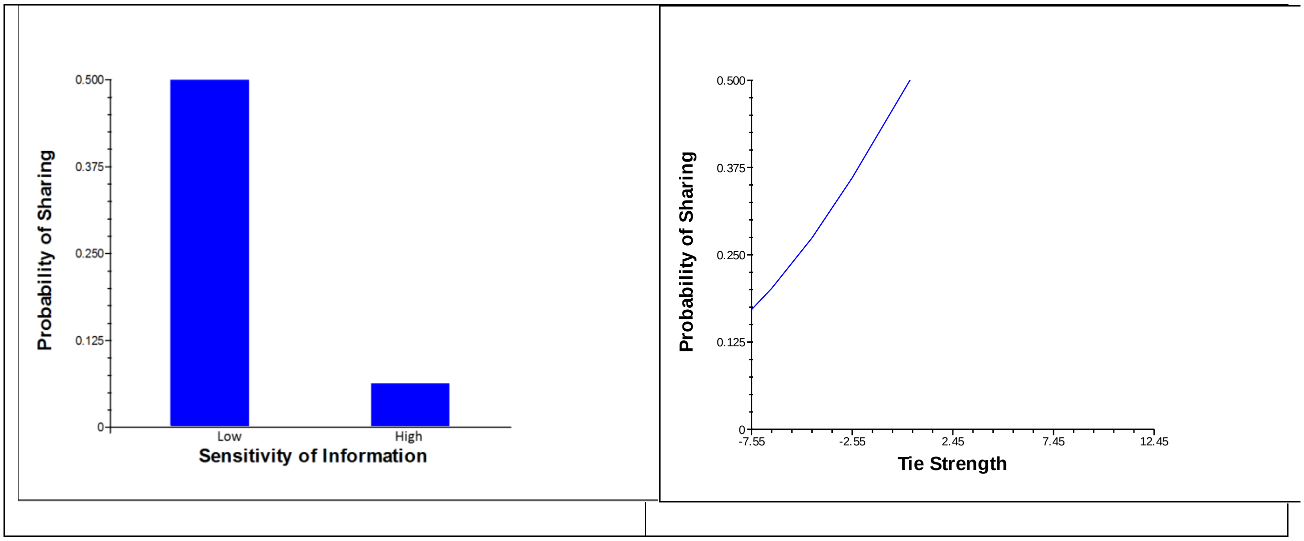


Figure 4: Relationship of Sensitivity of Infomation and Tie Strength with Probability of Sharing

Figure 5 shows the probability of sharing of information when sensitivity of information and tie strength are modeled in the same graph. Depending on the sensitivity of information, sharing levels differ. Clearly, higher tie strength is a stronger predictor for high sensitivity of information as compared to low sensitivity; this is shown by higher probability of sharing as the tie strength increases. Furthermore, when sharing less sensitivity information once the base tie strength is achieved, the graph levels off.

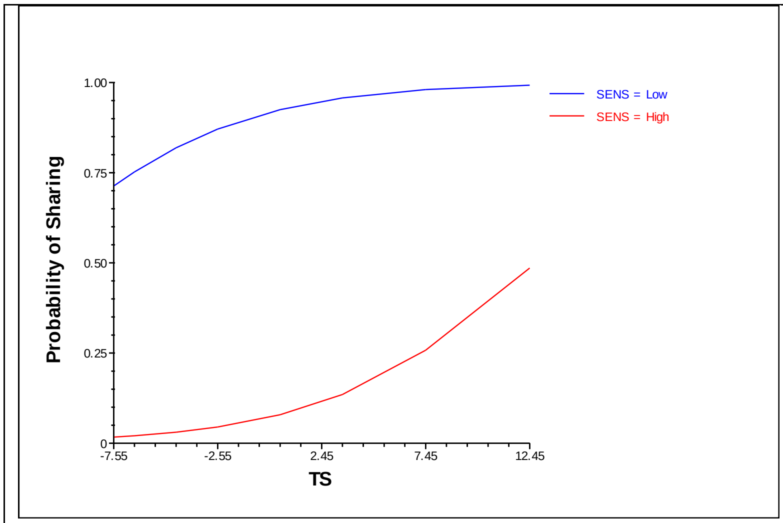


Figure 5: Difference between sharing information of low and high sensitivity

The insignificant result for the impact of Tool contradicts our hypothesis 6 suggesting that the Tool did not influence subjects' choices and consequently the decision-making strategy afforded to the subjects.

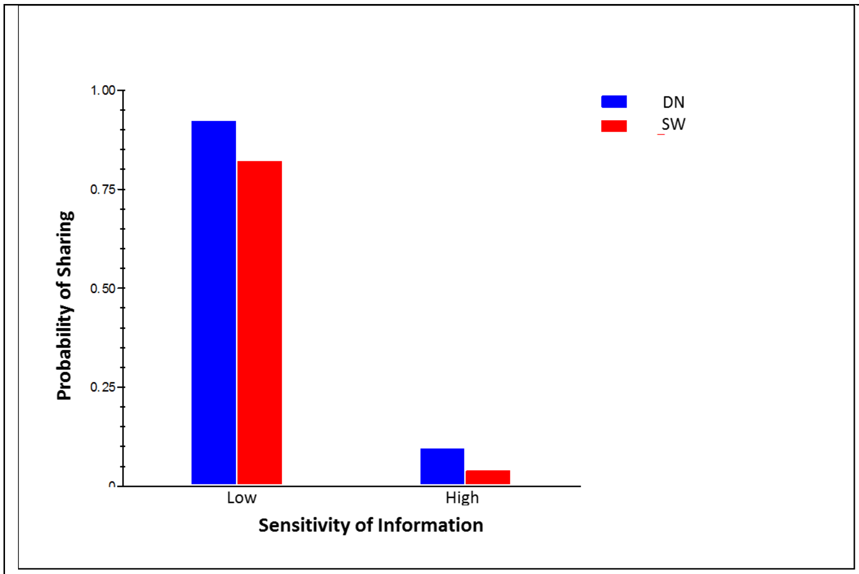


Figure 6: Fixed effects for Tool and Sensitivity

Figure 6 shows the probability of sharing information based on tool given the sensitivity. Other variables are held at mean. The red bars represent the probability of sharing information using SW tool, while blue line represents using DN. These tools are grouped based on the sensitivity of the information. As expected, given a tool, the probability of sharing sensitive information is lower than sharing information with less sensitivity. Furthermore, there is no significant difference between sharing levels when different tools used for a given level of sensitivity, evident in insignificant difference between the red and blue bars. This possibly implies that subjects chose similar sets of friends with both the tools. While there is no significant statistical difference, both bars for SW are lower than corresponding bars for DN, showing that, though not significant, there is some impact of the tool in the expected direction on the ensuing sharing decision.

2.5.1 Threshold Analysis

Since hypothesis 6 was not significant, we further probe into the data to find how the actual thresholds manifested. To determine the thresholds we first standardize the tie strength for each individual. This removes the individual variance within the tie strength scores. Next, we determine the tie strength at which individual decides to share. For inclusion threshold the last tie strength, below which individuals do not share is considered the inclusion threshold. Similarly, for exclusion threshold, first tie strength above which everyone is selected is considered the exclusion threshold. We find that exclusion threshold mean (0.13) is greater than inclusion threshold mean (0.00).

To further investigate the thresholds, we break down the data based on sensitivity. We assume that information sensitivity leads to this overlapping of thresholds. For instance, the exclusion threshold could be very high if the information sensitivity is very high and individuals would seek to protect their information. Similarly, when the information sensitivity is low, the threshold would also be lower.

For high sensitivity information, the mean for exclusion threshold is 1.09 and mean for inclusion threshold is 0.69. Since the mean exclusion threshold is greater than the inclusion threshold, the result is opposite to hypothesis 6, where we assumed that the inclusion threshold would be greater than exclusion threshold, with middling values in between. Given the results, it seems that the thresholds cross over each other and consequently there are no middling values.

For information with low sensitivity, we find that the mean of exclusion threshold (-0.61) is smaller than the mean of inclusion threshold (-0.91). This is consistent with our hypothesis 6.

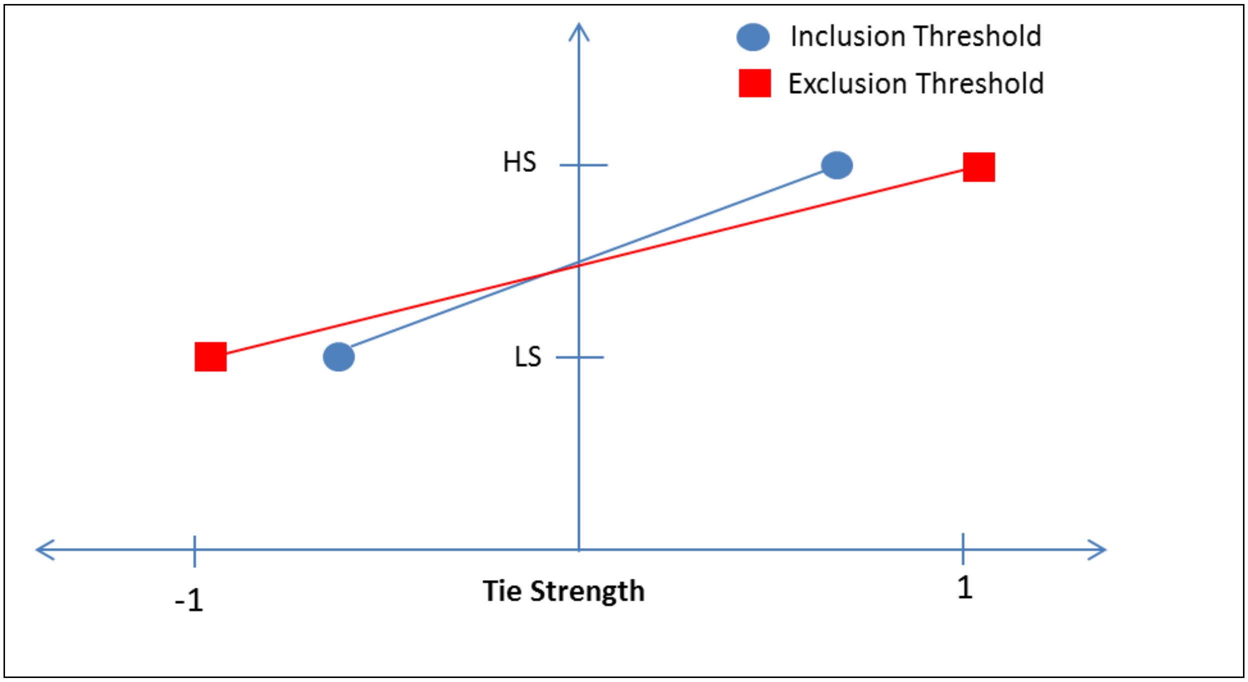


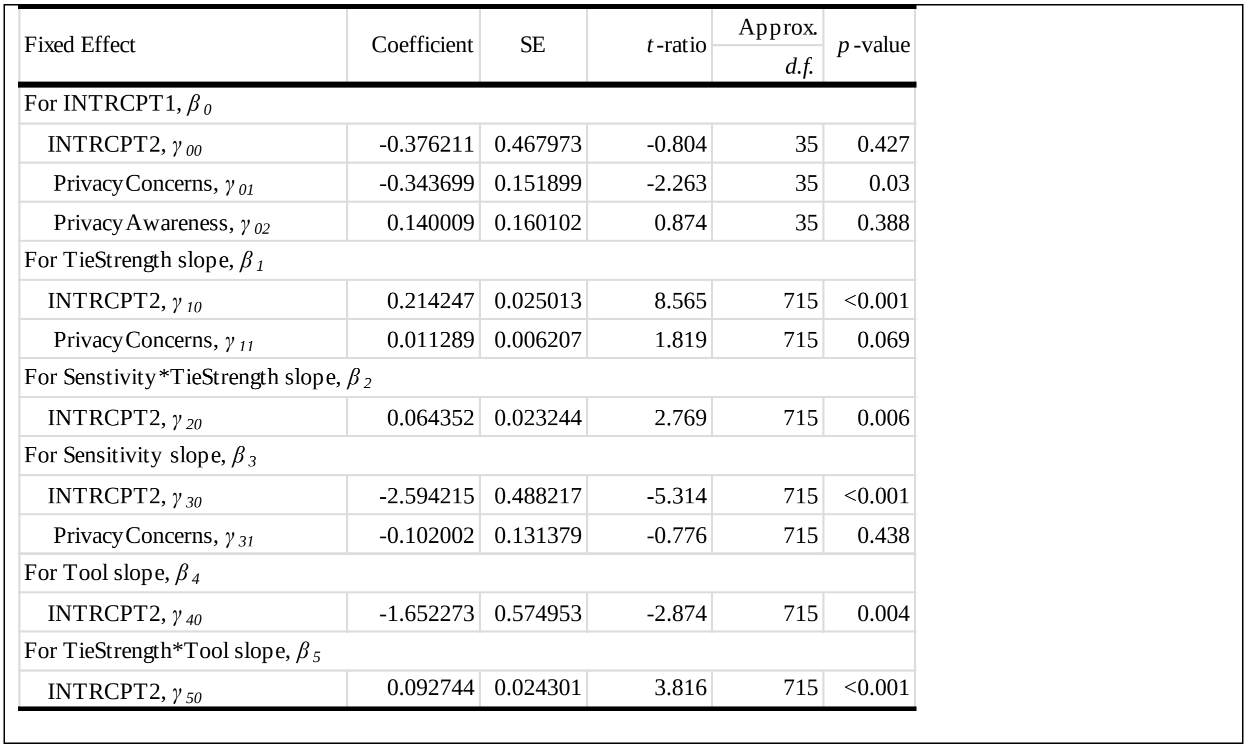
Figure 7: Changing Thresholds (Means) with Tie Strength and Information Sensitivity

Lastly, we note that both means for inclusion and exclusion threshold for high sensitivity information are greater than the means for low sensitivity information (Figure 7). In addition, we observe that when sensitivity of information increases (low to high) in conjunction with increase in tie strength, the mean of exclusion threshold becomes greater than the mean of inclusion threshold. This seems to show that when sharing high sensitive information, subjects using DN have more strict exclusion threshold as compared to inclusion threshold, which is contradictory to our hypothesis 6. This change in behavior allows us to further our analysis with an interaction term between tool and tie strength.

2.5.2 Interaction of Tool with Tie Strength

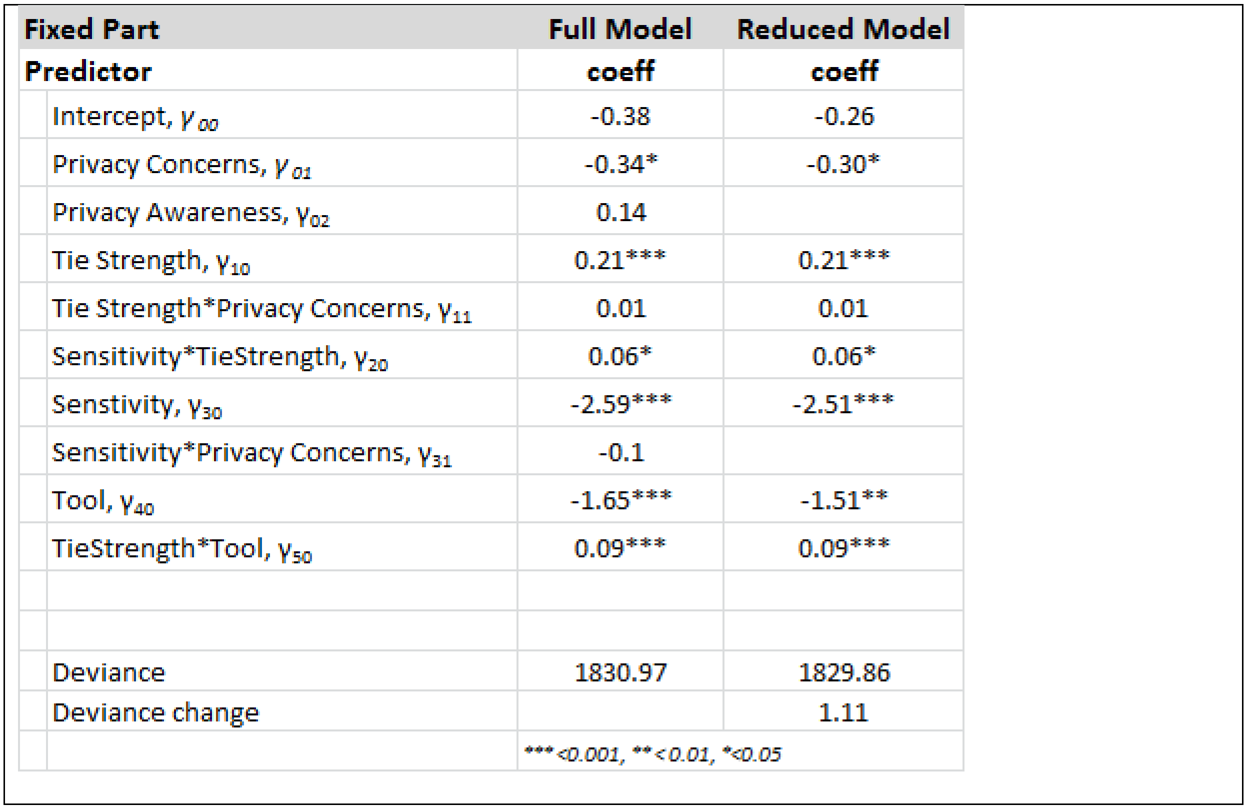
We repeat the data analysis with the inclusion of interaction term for tie strength with tool. The results are shown in Table 5. We use contrast coding for tool, with SW=1 and DN=-1 to fully interpret the results of interaction. Similarly, sensitivity is also coded HS=1 and LS=-1.

Interestingly, the interaction term for tie strength and tool is significant. In order to further refine the model, we remove the variables associated with non-significant coefficients γ_{02} and $\gamma 31$ from the model. For simplicity of comparison, the coefficients and deviance of the full and reduced models are compared in Table 6. The change in deviance of the model was 1830.97 - 1829.86 = 1.11, which is not significant ($P(\chi^2, df=1 \geq 1.11)=.22$)**,** thus we accept the reduced model. In addition, in Table 6, we find that in addition to the effect of tie strength, the effect of tool also becomes significant.



Fixed Effect	Coefficient	SE	*t*-ratio	Approx.	*p*-value
				d.f.	
For INTRCPT1, β_{0}					
INTRCPT2, γ_{00}	-0.376211	0.467973	-0.804	35	0.427
PrivacyConcerns, γ_{01}	-0.343699	0.151899	-2.263	35	0.03
PrivacyAwareness, γ_{02}	0.140009	0.160102	0.874	35	0.388
For TieStrength slope, β_{1}					
INTRCPT2, γ_{10}	0.214247	0.025013	8.565	715	<0.001
PrivacyConcerns, γ_{11}	0.011289	0.006207	1.819	715	0.069
For Senstivity*TieStrength slope, β_{2}					
INTRCPT2, γ_{20}	0.064352	0.023244	2.769	715	0.006
For Sensitivity slope, β_{3}					
INTRCPT2, γ_{30}	-2.594215	0.488217	-5.314	715	<0.001
PrivacyConcerns, γ_{31}	-0.102002	0.131379	-0.776	715	0.438
For Tool slope, β_{4}					
INTRCPT2, γ_{40}	-1.652273	0.574953	-2.874	715	0.004
For TieStrength*Tool slope, β_{5}					
INTRCPT2, γ_{50}	0.092744	0.024301	3.816	715	<0.001

Table 5: Full Model with TieStrength*Tool Interaction



Fixed Part	Full Model	Reduced Model
Predictor	coeff	coeff
Intercept, γ_{00}	-0.38	-0.26
Privacy Concerns, γ_{01}	-0.34*	-0.30*
Privacy Awareness, γ_{02}	0.14	
Tie Strength, γ_{10}	0.21***	0.21***
Tie Strength*Privacy Concerns, γ_{11}	0.01	0.01
Sensitivity*TieStrength, γ_{20}	0.06*	0.06*
Senstivity, γ_{30}	-2.59***	-2.51***
Sensitivity*Privacy Concerns, γ_{31}	-0.1	
Tool, γ_{40}	-1.65***	-1.51**
TieStrength*Tool, γ_{50}	0.09***	0.09***
Deviance	1830.97	1829.86
Deviance change		1.11
	*** <0.001, ** < 0.01, *<0.05	

Table 6: Comparison of Full and Reduced Models

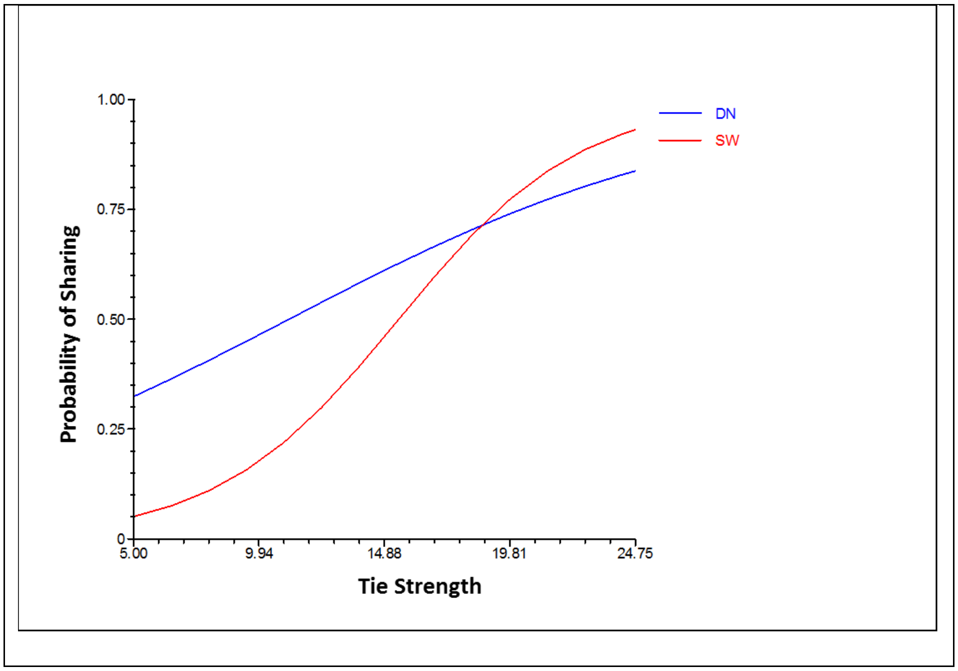
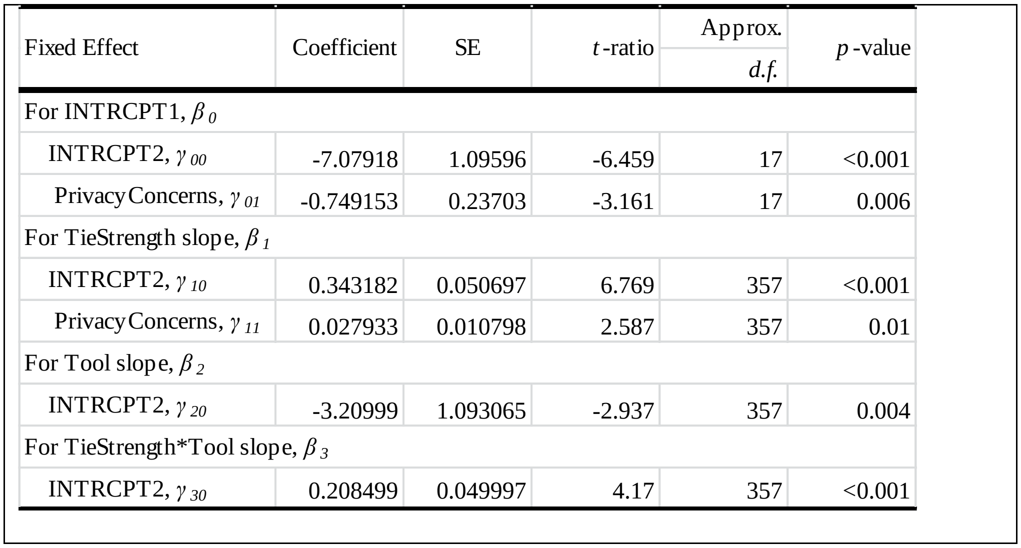


Figure 8: Interaction of Tie Strength and Tool

Figure 8 shows the graphical results when the interaction of tool and tie strength is included within the mode. Comparing it to Figure 7, as tie strength increases, the inclusion threshold line for SW moves to the left reducing the middle area and when the tie strength rises above 18 points, the inclusion range surpasses the exclusion range, thus removing the 'middling values'. In addition, we see that as the tie strength changes, the probability of sharing also increases. The probability of exclusion, as presented by the blue line, shows a continuous linear change, while the probability of inclusion shows growth that is much more aggressive as the tie strength increases and crosses over the blue line for very high value of tie strength. As proposed earlier, we expect that information sensitivity also influences the thresholds, thus we breakdown the data to determine the influence of this interaction at different levels of sensitivity.

2.5.2.1 Interaction in High Sensitivity Information

We split the data into high and low levels of sensitivity. This helps us focus on the interaction effect of tie strength and tool while controlling for the effect of sensitivity. Table 7 shows the results with only high sensitivity information. We find that both tool and the interaction terms are significant.



Fixed Effect	Coefficient	SE	*t* -ratio	Approx. *d.f.*	*p* -value
For INTRCPT1, β_0					
INTRCPT2, γ_{00}	-7.07918	1.09596	-6.459	17	<0.001
PrivacyConcerns, γ_{01}	-0.749153	0.23703	-3.161	17	0.006
For TieStrength slope, β_1					
INTRCPT2, γ_{10}	0.343182	0.050697	6.769	357	<0.001
PrivacyConcerns, γ_{11}	0.027933	0.010798	2.587	357	0.01
For Tool slope, β_2					
INTRCPT2, γ_{20}	-3.20999	1.093065	-2.937	357	0.004
For TieStrength*Tool slope, β_3					
INTRCPT2, γ_{30}	0.208499	0.049997	4.17	357	<0.001

Table 7: High Sensitivity Information

Since the interaction effect is significant, we focus on the interpretation of the interaction effect results. Figure 9 helps visualize the effect. We see as the tie strength increases the probability of sharing using SW tools increases exponentially until it reaches one. On the other hand, the probability of sharing using DN does not increase at the same pace. Essentially, when the tie strength is sufficiently high, the probability that the information is shared with a friend when using SW is greater than that when using DN, This is not consistent with our hypothesis 6 in which we proposed that given a tie strength, the probability of sharing with DN results is greater than the probability of sharing with SW. We proposed this hypothesis as we assumed that when subjects use DN, the subjects should automatically consider the high tie strength friends, as high tie strength friends should be higher than the exclusion thresholds. Our threshold analysis also showed that exclusion threshold become higher than inclusion threshold as the tie strength increases. This is also reflected in Figure 9 where DN is lower than SW for high tie strength. Our hypothesis is only true as long as the tie strength is below the point where two curves intersect. Consequently, subjects seem to change the way they use the tool when both the information sensitivity and the tie strength are high.

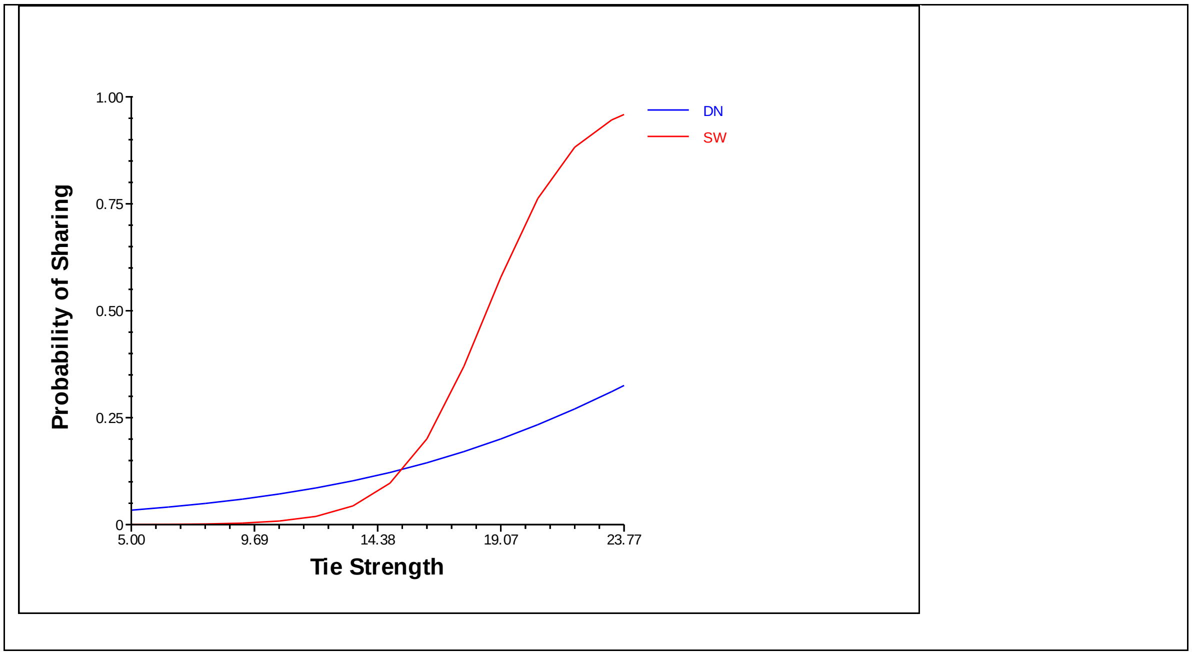
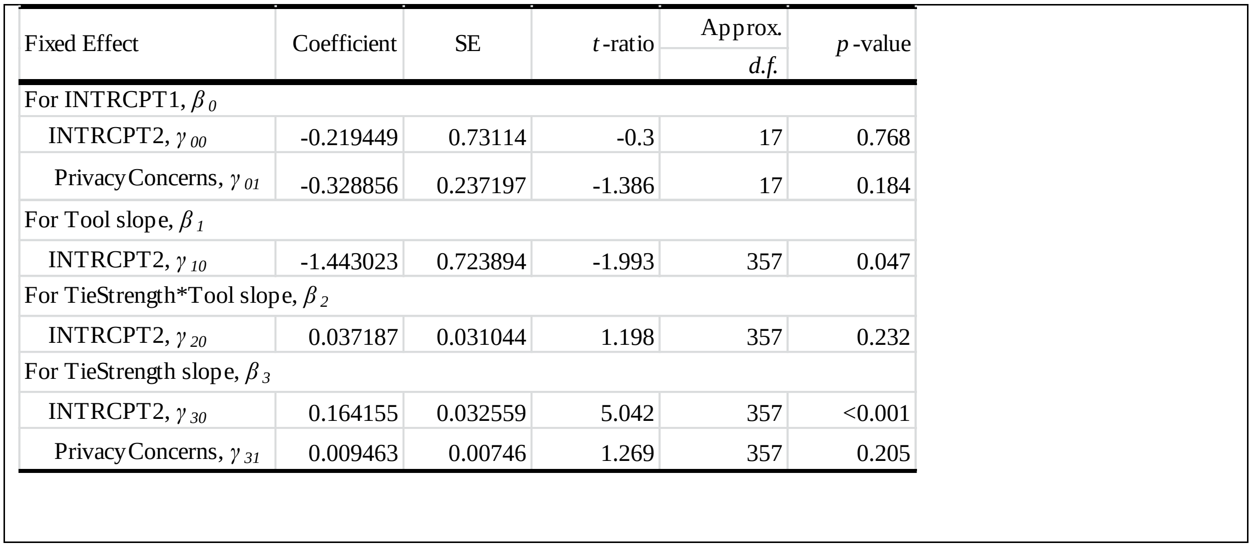


Figure 9: Interaction of Tie Strength with Tool within High Sensitivity

Compared to Figure 7, if hypothesis 6 is correct, then for high sensitivity the SW should be sharing less compared to DN for the same tie strength. That is, the threshold should move to the left at a lower rate. However, this is not the case.

2.5.2.2 Interaction Low Sensitivity Information

Similar to the analysis in the previous section, we estimated the model of information sharing only with low sensitive information. Table 8 shows the results of our estimations. The interaction of tie strength and tool is not significant, while the effect of tool is significant with p-value below .05.



Fixed Effect	Coefficient	SE	*t*-ratio	Approx. *d.f.*	*p*-value
For INTRCPT1, β_0					
INTRCPT2, γ_{00}	-0.219449	0.73114	-0.3	17	0.768
PrivacyConcerns, γ_{01}	-0.328856	0.237197	-1.386	17	0.184
For Tool slope, β_1					
INTRCPT2, γ_{10}	-1.443023	0.723894	-1.993	357	0.047
For TieStrength*Tool slope, β_2					
INTRCPT2, γ_{20}	0.037187	0.031044	1.198	357	0.232
For TieStrength slope, β_3					
INTRCPT2, γ_{30}	0.164155	0.032559	5.042	357	<0.001
PrivacyConcerns, γ_{31}	0.009463	0.00746	1.269	357	0.205

Table 8: Low Sensitivity Information

The coefficient is negative and since we coded DN=-1 and SW=1, this means that the mean of DN is greater than SW. Consequently, the probability of sharing with a friend is greater with DN as compared to SW. This confirms hypothesis 6 when information sensitivity is low. Figure 10 shows the effect of the tool as the tie strength increases. We see that as the tie strength increases, the probability of sharing using SW increases quickly, while there is no significant influence on the probability using DN. Consistent with our hypothesis 6, if the tie strength is high, the friends would lie above the inclusion threshold and are thus selected.

When using DN, subjects only eliminate friends with very low tie strength. This is evident from almost flat graphs which lower only when the tie strength is very low. This also shows that the exclusion threshold is very low. Thus, the probability of sharing information using DN is very high, even for the friends that were not considered using SW. We believe these are the middling options.

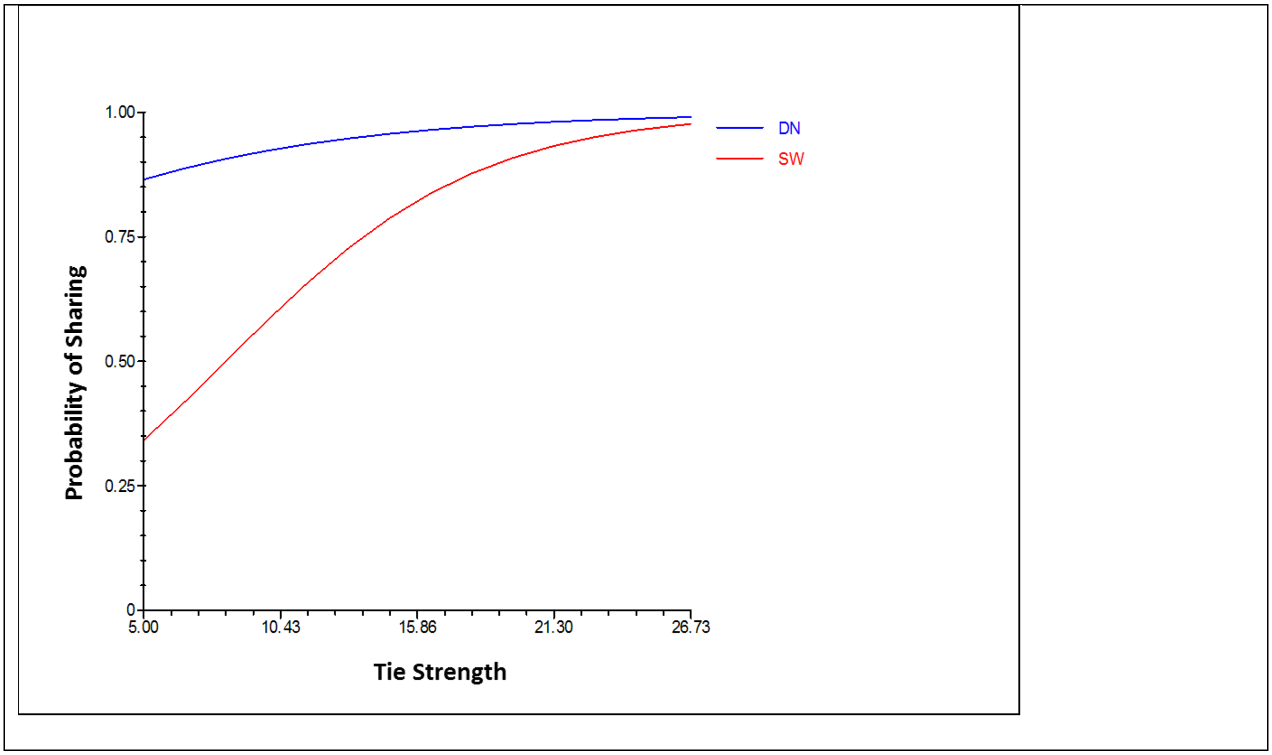


Figure 10: Effect of Tool within Low Sensitivity

3 Future Research Direction

As proposed in previous sections, while the process of inclusion and exclusion appear to be mirror images, subjects respond to situations differently even when the situations seems normatively and objective equivalent (Levin et al., 2002). For instance, in our study, people share with more or less number of friends depending on whether they had to add or remove friends. This can also be explained through "status quo bias", where individuals have propensity to the defer to the current state until they have a strong reason to act (Kahneman and Tversky, 1979, Thaler, 1980).

Levin et al. (2001) explained the existence of "status quo" using the example of job screening, where subjects were asked to add or remove from a pool of job applicants for further interview. Levin and his colleagues explained that when subjects are using exclusion then their status quo is to retain an option until there is good reason to remove it. Similarly, when using inclusion, the status quo is to have an option left out until there is a good reason to include it. In addition, Levin et al. suggest that when subjects were asked to remove options from a set, they experience "loss aversion". This is because when subjects are asked to remove a job applicant from a given list they feel that they are losing value associated with that applicant; consequently, they retain the option, leading to greater number of options.

In the present study, mostly the subjects include fewer friends in the inclusion mode. This can be explained as subjects' gain in perceived value when they add (inclusion mode) a friend is lower compared to the loss in perceived value when they remove a friend (exclusion mode). In other words, inclusion mode will lead to a lower probability of sharing with a friend as compared to the exclusion mode. However, in the condition where the tie strength and information sensitivity were high we found, to the contrary, that the probability of sharing in inclusion mode became higher. We believe that this discrepancy, and consequently the interaction, occurs when the value from perceived gains becomes higher than the value from perceived losses.

As seen in Figure 9, the interaction only happens when the information sensitivity and tie strength are both high. We propose that in this scenario, even when using inclusive mode, the value from the gains is sufficiently high for the subjects to add a friend. This is not surprising as, consistent with social capital theory; we would predict that very high tie strength would lead to a greater social capital. In addition, if the information is very private, or highly sensitive, we anticipate that owner of the information would tend keep this information safe, and only share when the perceived value of sharing is sufficiently high.

A similar phenomenon has also been observed in marketing literature, where the influence of value led to a higher probability of adding an option in inclusive mode. Mazumdar and Jun (1993) showed that in a given set, if there was a significant difference in prices of the products, then influence of ‘status quo’ in inclusive mode decreased. This is because when the subjects perceive higher relative gains, the influence of ‘status quo’ (add only if there is enough gain) induced by inclusive mode diminishes (Heath et al., 1995).

Park et al. (2000) tested this phenomenon by framing subjects in inclusion and exclusion modes. They researched scenario of adding (removing) ‘options’ or features to (from) existing products. They showed that if the options were priced at the same level, then to avoid loss the subjects preferred keeping options in the exclusion mode but did not add options in the inclusion mode. They further theorized that when in inclusion mode, if the gains of adding an option are significantly high, then the subjects will not default to ‘status quo’ and add the option. Thus, when the gains are high enough, the subjects perceive a loss if they do not add the option.

In our context, we propose that when perceived value associated with gains of adding a friend are sufficiently high, the subjects will overcome “status quo bias” in inclusion mode and add friends. Consider a person who decides to share high sensitivity information such as “Home Address”. To understand the influence we need to evaluate two scenarios:

1) Sharing high sensitivity information with high tie strength friend using inclusive mode.
2) Sharing high sensitivity information with high tie strength friend using exclusive mode.

When using inclusive mode, she will seek friends with whom she has high tie strength and can gain benefits from sharing. She will possibly consider future benefits such as inviting the friend over or sharing a car. While the benefits could range in number and intensity, in general, her focus will be towards evaluating potential benefits.

However, when using exclusive mode, she will seek the friends that have negative attributes and remove them from the list. This is because she is sharing highly sensitive information and friends with negative attributes will induce her to think of ways how a friend can misuse her information and cause her harm. As focus is on negative attributes, even a friend with high tie strength might look suspect. This is consistent with prospect theory where losses loom larger than gains. Subsequently in our case, negatives attributes will over weigh the positive attributes.

In sum, when evaluating a high tie strength friend in context of sharing high sensitivity information, inclusive mode will frame her focus towards evaluating the benefits while exclusive mode will frame her focus towards costs emerging from harms. Since costs have more influence, she will have greater probability of removing a friend when using exclusive mode as compared to including a friend using inclusive mode.

3.1 Protocol Analysis

We propose using protocol analysis to confirm that in the given scenario, subjects' decisions were influenced by the benefits and costs associated with sharing information with high tie strength friends. What we seek to investigate is that when the subjects shared high sensitivity information with high tie strength friends using inclusive mode, they focused on the positive attributes and consequently on the benefits of sharing information. Similarly, when the subjects shared information using exclusive mode, their focus was on the negative attributes and consequently on the costs.

While marketing researchers have used perceptual measures in evaluation of value, their research questions involved determining the influence of different prices, which can be easily tested by offering actual money. However, in our scenario, the value is very subjective and therefore protocol analysis provides a better approach to glean the essence of benefits and costs from the subject's responses. A single perceptual measure will not be reliable enough to capture the three dimensions (the tool, tie strength with the friend and the information shared) that emerge from sharing information.

3.1.1 Procedure

We propose using interviews to illicit subjects' responses after sharing of information. In terms of analysis, our objective is to extract the keywords that will highlight positives or negatives. We propose using the PANAS scales (Watson et al., 1988) to rate the keywords. The PANAS scale is a commonly used measure emotional or affective responses. The advantage of using this measure is that its reliability has been tested and it has been successfully used in IS research. Consistent with our existing design, we will create two scenarios of using inclusive (SW) and exclusive (DN) mode in high sensitivity in which subjects will be required to share one of the most sensitive information items and then answer the subsequent questions in a brief interview. Details are provided in the Table 9. We propose interviewing 10-15 subjects for each condition.

Table 9: Steps leading to Interview Questions

Step 1	Step 2	Step 3	Step 3
Rate Sensitivity	Use the tool to share most sensitive information.	Rate friends	1. Why did you share this information? 2. From the group of 20 friends, recall two of the friends with whom you had the strongest relationship and two with whom you had the weakest relationship.

			a. How did you *feel* about the sharing information with these two friends? Describe any feelings you experienced associated with *advantages* and *disadvantages* in sharing information with them.

Once the audio data has been collected, we will extract the keywords associated with positive affect and negative affect and rate the keywords based on the PANAS scale. Within PANAS, we intend to focus on the positive affect and negative affect as the high order influences. In general, if the information sensitivity is high we expect two results:

1) When the tie strength is high, the positive affect when sharing information using SW (inclusive mode) will be higher than the negative affect when sharing information using DN (exclusive mode).
2) When the tie strength is low, the positive affect when sharing information using SW will be lower than negative affect when sharing information using DN.

4 Conclusion

The purpose of this research was to explore the influence of the IT management tools on privacy decision making in online social networks. We presented a model of how individuals manage their private information and how this information can be shared on online social networks by using privacy tools. We found that the influence of privacy tools varies with the level of sensitivity of information as well as the tie strength of the friends with whom information is shared. When sharing information with low sensitivity, our model holds true, as subjects seemed to share more when using exclusive mode. The results were not as consistent when subjects shared highly sensitive information. The effect of the tools switched as the tie strength increased, which is a surprising result and requires further study.

Both results are important to IS researchers as they show that privacy management tools influence an individual's online sharing decisions. To date, the privacy paradox has been attributed to either individual level mismanagement of privacy decisions, or the additional social value attained in OSNs. This research furthers the sources of paradox by suggesting that privacy tools themselves can contribute to the variance in sharing decisions. In context of booming online social networks, this is a significant finding, since further research can be conducted to determine how these tools can be used to improve decision making such that individuals make decisions that are commensurate to their privacy profile without compromising the social value.

4.1 Limitations

As with any research, our experimental work also has shortcomings that raise issues about the generalizability of our results to contemporary social networks. One key issue is our operationalization of tools in lab environment. To ensure that our subjects were not overworked, we used a list of only 20 friends for each tool. Since our purpose was to test the influence of inclusive-exclusive thinking modes, this was an appropriate size. However, this size is not indicative of actual social networks where users have an average of 200 friends. How the size of the set of friends influences sharing decision and impact the role of tools is an interesting question and should be investigated by future studies.

Another aspect that our study overlooked is that we only operationalized two ways of sharing decisions. While these two decisions making modes should encompass most of the sharing decisions, there can be other aspects of tools, such as enabling using groups or searching friends by name, that confer different strategy for information sharing. For the purpose of controlled study, we were only able to focus on a two modes of decision-making. Our results should be interpreted as such.

Lastly, our sample size consisted of undergraduate students, which is not representative of actual online social network population. While the age group of undergraduate students does make them one of the dominant/active users of online social networks, it would be prudent to extend this study to a more diverse sample.

References

ACQUISTI, A. & GROSSKLAGS, J. 2005. Privacy and rationality in individual decision making. *Ieee Security & Privacy,* 3**,** 26-33.

ALTMAN, I. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

ANGST, C. M. & AGARWAL, R. 2009. Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly,* 33**,** 32p.

AWAD, N. F. & KRISHNAN, M. 2006. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly***,** 13-28.

BONNEAU, J. & PREIBUSCH, S. 2010. The privacy jungle: On the market for data protection in social networks. *Economics of Information Security and Privacy***,** 121-167.

BRYK, A. S. & RAUDENBUSH, S. W. 1988. Toward a more appropriate conceptualization of research on school effects: A three-level hierarchical linear model. *American Journal of Education***,** 65-108.

BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. 2010. INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly,* 34**,** 523-A7.

CAMPBELL, J. E. & CARLSON, M. 2002. Panopticon. com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media,* 46**,** 586-606.

COLEMAN, J. S. 1988. Social Capital in the Creation of Human-Capital. *American journal of sociology,* 94**,** S95-S120.

CONSTANT, D., SPROULL, L. & KIESLER, S. 1996. The kindness of strangers: The usefulness of electronic weak ties for technical advice. *Organization Science***,** 119-135.

CORTINA, J. M. 1993. What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology,* 78**,** 98.

CRONBACH, L. J. 1951. Coefficient alpha and the internal structure of tests. *Psychometrika,* 16**,** 297-334.

CULNAN, M. J. 1984. The dimensions of accessibility to online information: Implications for implementing office information systems. *ACM Transactions on Information Systems (TOIS),* 2**,** 141-150.

CULNAN, M. J. 1993. How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly,* 17**,** 341-363.

CULNAN, M. J. & ARMSTRONG, P. K. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science***,** 104-115.

DAVIES, S. G. 1997. Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. *Technology and privacy: The new landscape,* 143.

DINEV, T. & HART, P. 2004. Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology,* 23**,** 413-422.

DINEV, T. & HART, P. 2006a. An extended privacy calculus model for e-commerce transactions. *Information systems research,* 17**,** 61-80.

DINEV, T. & HART, P. 2006b. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce,* 10**,** 7-29.

ELLIS, M. V. 1999. Repeated measures designs. *The Counseling Psychologist,* 27**,** 552-578.

ELLISON, N. B., STEINFIELD, C. & LAMPE, C. 2007. The benefits of Facebook ìfriends:î Social capital and college studentsí use of online social network sites. *Journal of Computer Mediated Communication,* 12**,** 1143-1168.

ENDERS, C. K. & TOFIGHI, D. 2007. Centering predictor variables in cross-sectional multilevel models: A new look at an old issue. *Psychological Methods,* 12**,** 121-138.

GARDNER, R. 2008. Hierarchical Linear Modeling: A Primer (Measures within People).

GARTON, L., HAYTHORNTHWAITE, C. & WELLMAN, B. 1997. Studying online social networks. *Journal of Computer‐Mediated Communication,* 3**,** 0-0.

GILBERT, E. & KARAHALIOS, K. Predicting tie strength with social media. 2009. ACM, 211-220.

GLOVER, S. & BENBASAT, I. 2010. A Comprehensive Model of Perceived Risk of E-Commerce Transactions. *International Journal of Electronic Commerce,* 15**,** 47-78.

GRANOVETTER, M. S. 1973. The strength of weak ties. *American journal of sociology***,** 1360-1380.

HEATH, T. B., CHATTERJEE, S. & FRANCE, K. R. 1995. Mental Accounting and Changes in Price: The Frame Dependence of Reference Dependence. *Journal of Consumer Research,* 22**,** 90-97.

HOX, J. J. 2010. *Multilevel analysis: Techniques and applications*, Taylor & Francis.

HUBERMARGARET A, V. L. & NORTHCRAFT, G. B. 1987. Decision bias and personnel selection strategies. *Organizational Behavior and Human Decision Processes,* 40**,** 136-147.

HUI, K. L., TEO, H. H. & LEE, S. Y. T. 2007. The value of privacy assurance: an exploratory field experiment. *MIS Quarterly,* 31**,** 19-33.

KAHNEMAN, D. & TVERSKY, A. 1979. Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society***,** 263-291.

KAHNEMAN, D. & TVERSKY, A. 1984. Choices, values, and frames. *American psychologist,* 39**,** 341.

KRACKHARDT, D. 1992. The strength of strong ties: The importance of philos in organizations. *Networks and organizations: Structure, form, and action,* 216**,** 239.

KRULL, J. L. & MACKINNON, D. P. 2001. Multilevel modeling of individual and group level mediated effects. *Multivariate behavioral research,* 36**,** 249-277.

LAUFER, R. S. & WOLFE, M. 1977. Privacy as a Concept and a Social Issue - Multidimensional Developmental Theory. *Journal of Social Issues,* 33**,** 22-42.

LEVIN, I. P., JASPER, J. & FORBES, W. S. 1998. Choosing versus rejecting options at different stages of decision making. *Journal of Behavioral Decision Making,* 11**,** 193-210.

LEVIN, I. P., PROSANSKY, C. M., HELLER, D. & BRUNICK, B. M. 2001. Prescreening of choice options in 'positive'and 'negative'decision-making tasks. *Journal of Behavioral Decision Making,* 14**,** 279-293.

LEVIN, I. P., SCHREIBER, J., LAURIOLA, M. & GAETH, G. J. 2002. A tale of two pizzas: building up from a basic product versus scaling down from a fully-loaded product. *Marketing Letters,* 13**,** 335-344.

MADEJSKI, M., JOHNSON, M. & BELLOVIN, S. 2011. The failure of online social network privacy settings. *posterouscom***,** 1-20.

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**,** 336-355.

MARGULIS, S. T. 2003a. On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues,* 59**,** 411-429.

MARGULIS, S. T. 2003b. Privacy as a social issue and behavioral concept. *Journal of Social Issues,* 59**,** 243-261.

MARSDEN, P. V. & CAMPBELL, K. E. 1984. Measuring tie strength. *Soc. F.,* 63**,** 482.

MAZUMDAR, T. & JUN, S. Y. 1993. Consumer Evaluations of Multiple Versus Single Price Change. *Journal of Consumer Research,* 20**,** 441-450.

METZGER, M. J. 2007. Communication privacy management in electronic commerce. *Journal of Computer‐Mediated Communication,* 12**,** 335-361.

MOURALI, M. & NAGPAL, A. 2011. The powerful select, the powerless reject: Power's influence in decision strategies. *Journal of Business Research*.

NETER, J., WASSERMAN, W., KUTNER, M. H. & LI, W. 1996. *Applied linear statistical models,* Irwin.

NORBERG, P. A., HORNE, D. R. & HORNE, D. A. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs,* 41**,** 100-126.

OSBORNE, J. W. 2000. Advantages of hierarchical linear modeling. *Practical Assessment, Research & Evaluation,* 7**,** 1-3.

PARK, C. W., JUN, S. Y. & MACINNIS, D. J. 2000. Choosing what I want versus rejecting what I do not want: An application of decision framing to product option choice decisions. *Journal of Marketing Research***,** 187-202.

PAVLOU, P. A., LIANG, H. G. & XUE, Y. J. 2007. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly,* 31**,** 105-136.

PETRONIO, S. S. 2002. *Boundaries of privacy: Dialectics of disclosure,* State Univ of New York Pr.

PHELPS, J., NOWAK, G. & FERRELL, E. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing***,** 27-41.

PORTES, A. 1998. Social Capital: Its origins and applications in modern sociology. *Annual Review of Sociology,* 24**,** 1-24.

RAFAELI, S. & RABAN, D. R. 2005. Information sharing online: a research challenge. *International Journal of Knowledge and Learning,* 1**,** 62-79.

RAUDENBUSH, S. W. 2004. *HLM 6: Hierarchical linear and nonlinear modeling,* Scientific Software International.

SCHRAMMEL, J., KÖFFEL, C. & TSCHELIGI, M. How much do you tell?: information disclosure behaviour indifferent types of online communities. 2009. ACM, 275-284.

SMITH, H. J., DINEV, T. & XU, H. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly,* 35**,** 989-1015.

SMITH, H. J., MILBERG, S. J. & BURKE, S. J. 1996. Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly***,** 167-196.

THALER, R. 1980. Toward a positive theory of consumer choice. *Journal of Economic Behavior & Organization,* 1**,** 39-60.

TVERSKY, A. & KAHNEMAN, D. 1986. Rational choice and the framing of decisions. *Journal of business***,** 251-278.

WASKO, M. M. L. & FARAJ, S. 2005. Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly***,** 35-57.

WATSON, D., CLARK, L. A. & TELLEGEN, A. 1988. Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of Personality and Social Psychology,* 54**,** 1063.

WESTIN, A. F. 1968. Privacy and freedom. *Washington and Lee Law Review,* 25**,** 166.

XU, H. The effects of self-construal and perceived control on privacy concerns. 2007.

YANIV, I. & SCHUL, Y. 2000. Acceptance and elimination procedures in choice: Noncomplementarity and the role of implied status quo. *Organizational Behavior and Human Decision Processes,* 82**,** 293-313.

YANIV, I., SCHUL, Y., RAPHAELLI-HIRSCH, R. & MAOZ, I. 2002. Inclusive and exclusive modes of thinking: Studies of prediction, preference, and social perception during parliamentary elections. *Journal of Experimental Social Psychology,* 38**,** 352-367.

Appendices

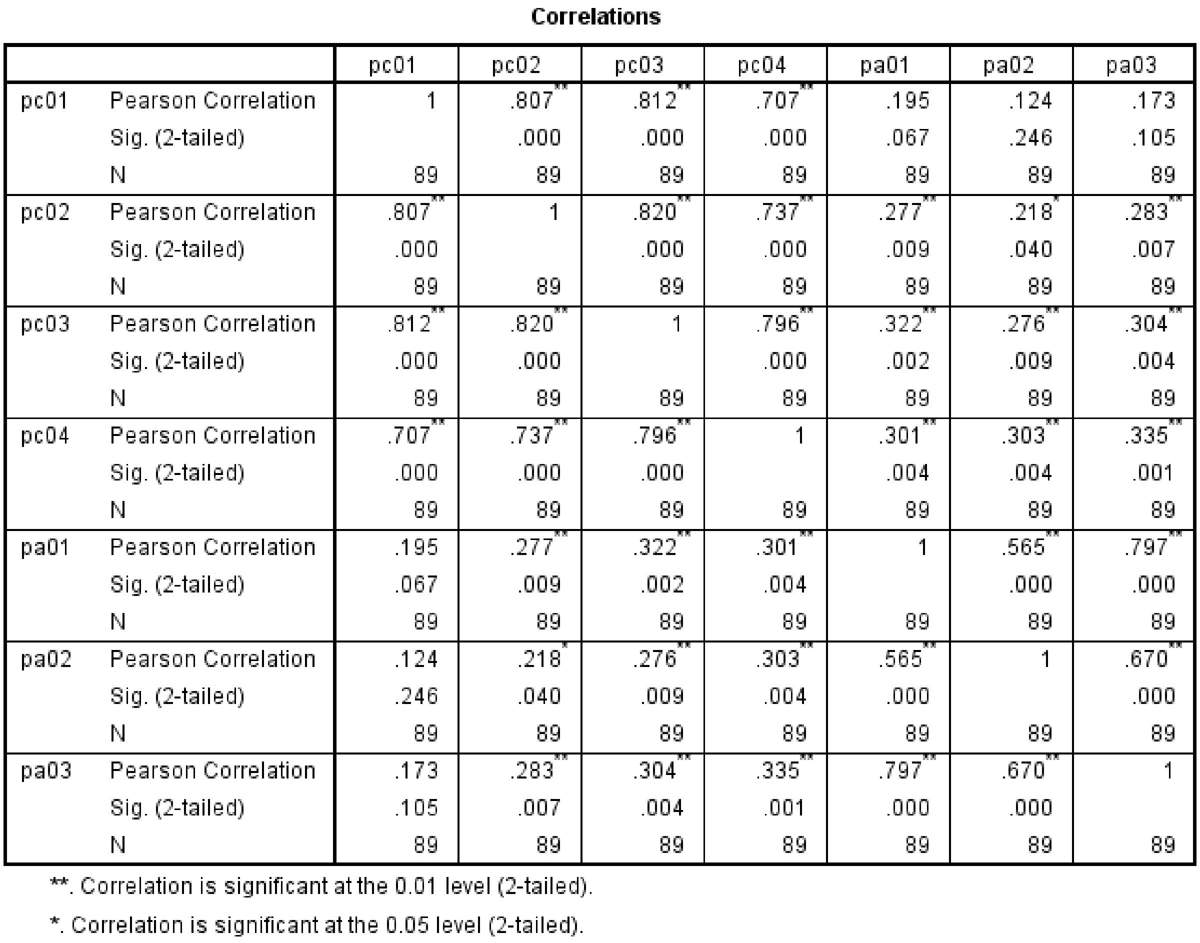
Measures, Items and their Sources

Table: Measures, Items and their Sources

Measure	**Items**	**Source**
	Social Network Tie Strength	
Social Network Tie Strengths	You have a strong relationship with this person. You feel comfortable asking this friend to loan you $100 or more. This person would be helpful if you were looking for a job. You would be upset if this person unfriended you. If you left Facebook for another social site, you would want bring this friend along.	(Gilbert and Karahalios, 2009)
	Individual Characteristics	
Privacy Concerns	I am concerned that the information I disclose to friends on Facebook could be misused.	(Dinev and Hart, 2006b)
	I am concerned that a person can find private information about me as a result of my sharing of information with friends on Facebook.	
	I am concerned about providing personal information to friends on Facebook, because of what they might do with it.	
	I am concerned about providing personal information to friends on Facebook, because it could be used in a way I did not foresee.	
Privacy Awareness	Overall, I am aware of the potential privacy issues and their negative consequences on Facebook.	Burcu et.al. 2010
	I have sufficient knowledge about the cost of potential privacy issues on Facebook.	
	I understand the issues of information privacy on Facebook and the risks they pose in general.	
Open Ended Questions	What makes this tool better for sharing personal information? What makes this tool worse for sharing personal information?	

Items and their Cross loadings

Table 10: Cross Loadings for Privacy Concerns and Privacy Awareness.



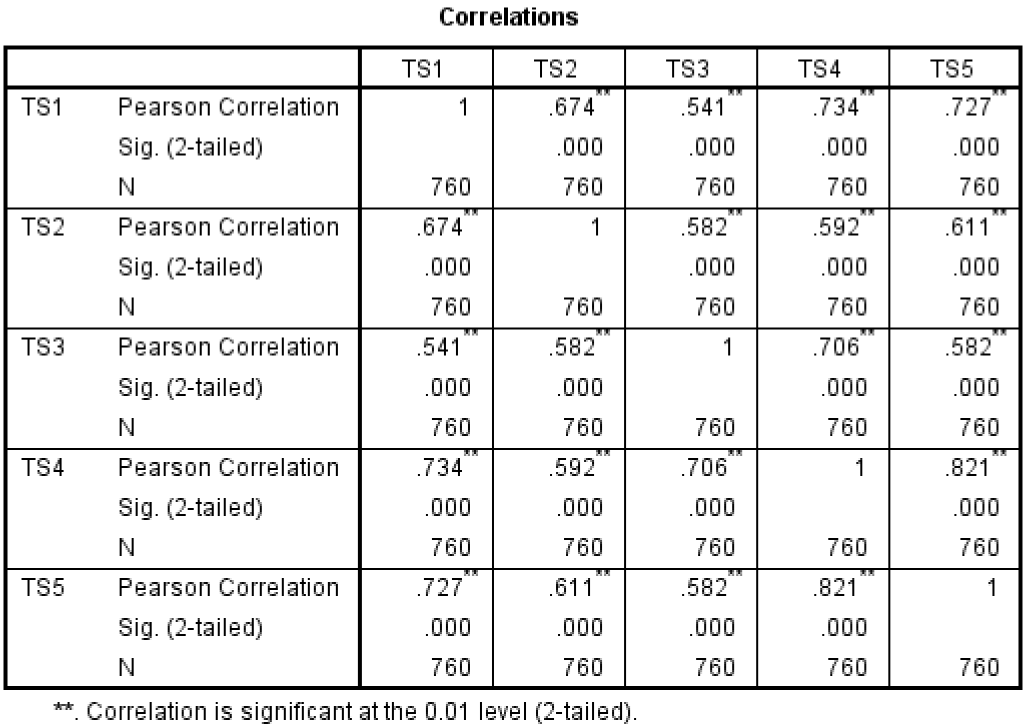
Correlations

		pc01	pc02	pc03	pc04	pa01	pa02	pa03
pc01	Pearson Correlation	1	.807**	.812**	.707**	.195	.124	.173
	Sig. (2-tailed)		.000	.000	.000	.067	.246	.105
	N	89	89	89	89	89	89	89
pc02	Pearson Correlation	.807**	1	.820**	.737**	.277**	.218*	.283**
	Sig. (2-tailed)	.000		.000	.000	.009	.040	.007
	N	89	89	89	89	89	89	89
pc03	Pearson Correlation	.812**	.820**	1	.796**	.322**	.276**	.304**
	Sig. (2-tailed)	.000	.000		.000	.002	.009	.004
	N	89	89	89	89	89	89	89
pc04	Pearson Correlation	.707**	.737**	.796**	1	.301**	.303**	.335**
	Sig. (2-tailed)	.000	.000	.000		.004	.004	.001
	N	89	89	89	89	89	89	89
pa01	Pearson Correlation	.195	.277**	.322**	.301**	1	.565**	.797**
	Sig. (2-tailed)	.067	.009	.002	.004		.000	.000
	N	89	89	89	89	89	89	89
pa02	Pearson Correlation	.124	.218*	.276**	.303**	.565**	1	.670**
	Sig. (2-tailed)	.246	.040	.009	.004	.000		.000
	N	89	89	89	89	89	89	89
pa03	Pearson Correlation	.173	.283**	.304**	.335**	.797**	.670**	1
	Sig. (2-tailed)	.105	.007	.004	.001	.000	.000	
	N	89	89	89	89	89	89	89

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 11: Correlations for Items in Tie Strength



Correlations

		TS1	TS2	TS3	TS4	TS5
TS1	Pearson Correlation	1	.674**	.541**	.734**	.727**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	760	760	760	760	760
TS2	Pearson Correlation	.674**	1	.582**	.592**	.611**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	760	760	760	760	760
TS3	Pearson Correlation	.541**	.582**	1	.706**	.582**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	760	760	760	760	760
TS4	Pearson Correlation	.734**	.592**	.706**	1	.821**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	760	760	760	760	760
TS5	Pearson Correlation	.727**	.611**	.582**	.821**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	760	760	760	760	760

**. Correlation is significant at the 0.01 level (2-tailed).