The Pennsylvania State University
The Graduate School
College of Information Sciences and Technology

TOWARDS MODELS OF THE ECONOMIC VALUE OF INTERDEPENDENT PRIVACY IN SOCIAL APP ADOPTION SCENARIOS

A Dissertation in
Information Sciences and Technology
by
Yu Pu

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

May 2017

The dissertation of Yu Pu was reviewed and approved* by the following:

Jens Grossklags
Assistant Professor of Information Sciences and Technology
Dissertation Advisor, Chair of Committee

Mary Beth Rosson
Professor of Information Sciences and Technology
Associate Dean for Undergraduate and Graduate Studies, College of Information Sciences and Technology

Peng Liu
Professor of Information Sciences and Technology

S. Shyam Sundar
Distinguished Professor of Communications

Andrea H. Tapia
Associate Professor of Information Sciences and Technology
Director of Graduate Program, College of Information Sciences and Technology

*Signatures are on file in the Graduate School.

Abstract

In the context of third-party social apps, the problem of interdependency of privacy refers to users making app adoption decisions which cause the collection and utilization of personal information of users' friends. In contrast, users' friends have typically little or no direct influence over these decision-making processes.

While the issue of interdependent privacy grows in practical importance, only a limited number of research studies have appeared on this subject. To address this literature gap, in this dissertation, we discuss three studies that address the problem space of interdependent privacy in social app adoption scenarios. More specifically, this dissertation focuses on quantifying and explaining the monetary value which app users place on their friends' information, i.e., value of interdependent privacy.

In Study 1, we conduct a full-profile conjoint analysis study with two treatment conditions which vary the app data collection context (i.e., to which degree the functionality of the app makes it necessary for the app developer to collect friends' information). Analyzing the data, we are able to quantify how much monetary value app users place on their friends' and their own personal information in each context. Combining these valuations with the responses to a comprehensive survey, we apply structural equation modeling (SEM) analysis to investigate the roles of privacy concern, its antecedents, as well as app data collection context to work towards a model of interdependent privacy for the scenario of social app adoption.

Complementing Study 1, our second study aims to further explain the valuation of interdependent privacy. In particular, research indicates that social capital, which is an immaterial resource that can yield positive social outcomes, plays an important role in individuals' decision-making. Motivated by these works, we investigate the complex and still undetermined relationship between interdependent privacy value and social capital. In addition, in order to gain a comprehensive understanding of interdependent privacy valuation, our study also examines its relationships with factors such as individuals' number of friends within SNSs, and demographics.

With Study 3, we explore important contextual factors that affect the value which app users attribute to their friends' information. In particular, we focus on understanding the impact of sharing anonymity (i.e., whether disclosure of friends' information is anonymous) on the valuation of interdependent privacy. To address this research goal, we conduct a between-subject, choice-based conjoint analysis study with 4 treatments (2 sharing anonymity $\times$ 2 context relevance). Our study confirms the important role that sharing anonymity plays in interdependent privacy valuation.

Our research contributes to a better understanding of individuals' attitudes and behaviors towards interdependent privacy issues associated with social apps. Based on this understanding, we offer insights, such as implications to redesign apps' privacy notice dialogues, as well as suggestions to introduce new privacy polices, for better addressing individuals' own and their friends' privacy preferences.

Table of Contents

List of Figures **ix**

List of Tables **x**

Acknowledgments **xi**

Chapter 1
Introduction **1**
1.1 Overview of Studies . . . 3
1.1.1 Study 1 . . . 3
1.1.2 Study 2 . . . 4
1.1.3 Study 3 . . . 5
1.2 Contributions . . . 6
1.2.1 Understanding the Interdependent Privacy Problem . . . 7
1.2.1.1 Expand Privacy Literature . . . 7
1.2.1.2 Offer Implications for Privacy by Redesign . . . 8
1.2.1.3 Provide Insights on Privacy Policy Discussions . . . 9
1.2.2 Suggestions for Conducting Human Behavioral Research . . . 10
1.3 Structure of Dissertation . . . 11

Chapter 2
Background & Related Work **12**
2.1 Social Apps' Privacy Issues . . . 12
2.1.1 Social Apps on Social Network Sites . . . 12
2.1.2 Social Apps on Mobile Networks . . . 13
2.2 Interdependent Privacy . . . 15
2.3 Valuation of Privacy . . . 17
2.4 Privacy Concerns and Other Constructs . . . 19
2.5 Anonymity in Individual Decision-Making . . . 20
2.6 Resolve Interdependent Privacy Conflicts . . . 22

Chapter 3

Study 1: Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy 25

3.1 Conjoint Analysis to Determine Privacy Value . . . 27
3.1.1 Design of Conjoint Study . . . 27
3.1.1.1 Determination of Attributes and Their Levels . . . 27
3.1.1.2 Selection of Conjoint Analysis Method and Number of Stimuli . . . 30
3.1.1.3 Estimation of Conjoint Model . . . 30
3.1.2 Design of Survey Experiment . . . 31
3.1.2.1 Screening Task . . . 31
3.1.2.2 App Ranking Task and Survey Measures . . . 32
3.1.2.3 Procedures . . . 34
3.1.3 Sampling . . . 35
3.1.4 Analysis of Empirical Results . . . 37
3.2 SEM to Investigate Associations between Privacy Value and Its Antecedents . . . 39
3.2.1 Hypotheses and Research Model . . . 40
3.2.2 Measurement Scale Development . . . 45
3.2.3 Empirical Results . . . 46
3.2.3.1 Evaluation of the Measurement Model . . . 47
3.2.3.2 Tests of Path Model . . . 47
3.2.3.2.1 Tests of Model Fitness . . . 47
3.2.3.2.2 Tests of Direct Effects . . . 48
3.2.3.2.3 Tests of Moderating Effects . . . 49
3.2.4 Discussion of SEM Model . . . 52
3.3 Summary . . . 54

Chapter 4

Study 2: Interdependent Privacy Value in Social App Adoption Contexts: Its Associations with Social Capital, Data Collection Context, and Number of Friends 56

4.1 Background on Social Capital . . . 58
4.2 Research Question . . . 60
4.3 Method . . . 62
4.4 Data Description . . . 64
4.4.1 Demographics and Number of Friends . . . 64
4.4.2 Interdependent Privacy Value . . . 65
4.4.3 Measurement Value . . . 66
4.4.3.1 Bridging Social Capital . . . 67

4.4.3.2 Bonding Social Capital . . . 67
4.4.3.3 Interdependent Privacy Concern . . . 68
4.5 Results . . . 69
4.5.1 Model 1 . . . 71
4.5.2 Model 2 . . . 72
4.6 Discussion . . . 73
4.7 Summary . . . 77

Chapter 5
Study 3: Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter? 78
5.1 Conjoint Analysis to Determine Privacy Value . . . 80
5.1.1 Design of Choice-based Conjoint Study . . . 80
5.1.1.1 Determination of Apps' Attributes and Their Levels 81
5.1.1.2 Selection of Conjoint Analysis Method . . . 81
5.1.1.3 Selection of App Profiles . . . 82
5.1.1.4 Estimation of Conjoint Model . . . 83
5.1.2 Design of Survey Experiment . . . 83
5.1.2.1 Treatments . . . 83
5.1.2.2 Procedure . . . 85
5.1.2.3 Participants and Recruitment . . . 85
5.1.3 Results of Choice-based Conjoint Study . . . 86
5.1.3.1 Participant Data . . . 86
5.1.3.2 Estimations of Privacy Values . . . 87
5.1.3.3 Effects of Sharing Anonymity and Context Relevance on Privacy Valuation . . . 89
5.2 SEM to Investigate Determinants of Privacy Value . . . 91
5.2.1 Hypotheses and Research Model . . . 92
5.2.2 Measurement Scale Development . . . 96
5.2.3 Evaluation of the Measurement Model . . . 97
5.2.4 Evaluation of the Path Model . . . 98
5.2.5 Discussion of SEM Results . . . 100
5.3 Summary . . . 102

Chapter 6
Conclusions 104
6.1 Summary of Findings . . . 105
6.2 Summary of Contributions . . . 107
6.3 Limitations and Future Work . . . 109

Appendix
Appendix A: Survey Instruments **112**

Bibliography **117**

List of Figures

3.1 Screenshot of experiment interface (drag and drop interaction) . . . 33
3.2 Screenshot of experiment interface (drag and drop interaction) . . . 35
3.3 The conceptual model . . . 44

4.1 Gender distribution . . . 64
4.2 Age distribution . . . 64
4.3 Education level distribution . . . 65
4.4 Income level distribution . . . 65
4.5 Number of friends distribution . . . 66
4.6 Value of interdependent privacy . . . 66
4.7 Interaction of number of friends and treatment on interdependent privacy value . . . 72
4.8 Interaction of bonding social capital and treatment on interdependent privacy value . . . 73

5.1 Screenshot of app choice interface . . . 86
5.2 Effects of sharing anonymity and context relevance on valuation of friends' *basic* information . . . 89
5.3 Effects of sharing anonymity and context relevance on valuation of friends' *valuable* information . . . 90
5.4 Effects of sharing anonymity and context relevance on valuation of friends' *full profile* information . . . 91
5.5 SEM explaining privacy valuation . . . 92

List of Tables

2.1 Most frequently requested Facebook permissions explicitly involving information of users' friends (abbreviated table from Wang et al. [1]) 14

3.1 Summary of attributes and levels 29
3.2 Averaged part-worth utilities 38
3.3 Utility change and monetary value of change 38
3.4 Evaluations of measurement model 45
3.5 Results of path analysis 48
3.6 Results of pair-wise parameter comparisons 49

4.1 Summary statistics for bridging social capital 67
4.2 Summary statistics for bonding social capital 68
4.3 Summary statistics for interdependent privacy concern 69
4.4 Regressions explaining value of interdependent privacy 70

5.1 Summary of attributes and levels 81
5.2 Utility change and monetary value of change 88
5.3 Evaluations of measurement model 97

Acknowledgments

It seems almost unreal to believe that this journey is finally coming to an end. I still remember many details of the first time I visited State College, the hopes and fears I had about joining the Ph.D. program in IST, and the wonderful experience of presenting my research to domain experts. With so many unforgettable memories, I realize that I could not have made it without the tremendous support from so many people I am grateful to have in my life.

Foremost, I would like to express my special appreciation and thanks to my dear advisor Dr. Jens Grossklags. You led me through this wonderful journey and made me who I am today. During the past four years, I have been continuously encouraged by your research enthusiasm. You introduced me to the amazing world of privacy research, and kept honing my research skills with your generous mentorship and guidance. Meanwhile, your positive attitude towards life inspires me to keep calm when faced with difficulties, to always stay optimistic, and to work hard and play hard. Thank you, my dear advisor. I feel fortunate to be one of your students.

I would also like to thank my committee members: Dr. Mary Beth Rosson, Dr. Peng Liu, and Dr. S. Shyam Sundar. Thank you all for your brilliant comments and suggestions, thank you all for making my defense an enjoyable moment, and thank you all for your appreciation of my research.

I want to reserve my special thanks to my dear labmates for their company for many days and nights: Sadegh Farhang, Moury Bidgoli, and Jake Weidman. Thank you Sadegh, for so many encouraging conversations and your warm smiles. Thank you Moury, for your kind companionship, and many holiday cards and candies. Thank you Jake, for your endless support, and your help with my English writing and speaking. Thank you all for always staying by my side and cheering me up! I wish you all the best.

Meanwhile, I also want to thank my friends here at Pennsylvania State University. Thank you, Yaifei Wang, Shuting Wang, Lu Liu for accompanying me, and for

celebrating my important life moments. Thank you, Yibo Wu, Qian Zhang, Yi Yang, Nan Yu, and Li Qiu for all the happy time spent with you. Hongjian Wang, Fei Wu, Jian-Syuan Wong and so many others, thanks for being such wonderful friends and sources of inspiration. All the best to you.

Finally, I want to thank my parents Guoying Yu and Aiwen Pu, and my important life partner Dr. Xinyang Ge for their selfless and unconditional support. Life with them is so gorgeous!

Chapter 1
Introduction

Within the past ten years, we have witnessed the increasing popularity of social network sites (SNSs). In order to expand their functionalities, these platforms allow outside developers to interact with users through so-called third-party applications (or social apps). Those apps have met significant success in the marketplace ever since their emergence. Despite their worldwide popularity, users and consumers advocates grow increasingly concerned about the associated privacy risks arising from the collection and potential misuse of users' personal information. For example, research has demonstrated that apps request a disproportionate amount of user information [2]. For one thing, apps usually request more permissions than actually necessary for their operations [3]. For another, it has been revealed that app developers can be owners of several apps. As a result, an app developer may use different apps to request different personal information, and later aggregate all collected user data [2,4]. In addition, due to the fact that apps are highly integrated to social network platforms, app users usually have misconceptions regarding app security and privacy. In other words, users often do not understand that apps collect and accumulate their personal data [5], and hence inadvertently reveal more information to apps than they want. Further, it has also been reported that apps may transfer personal identifiable information to "fourth party" entities such as trackers and advertisers [2,6].

Furthermore, the growing importance of the interdependent privacy issue has introduced an additional layer of privacy concern towards social apps. In a nutshell, interdependency of privacy refers to the phenomenon that within a networked system, privacy of individuals not only depends on their own behaviors, but is also influenced by decisions of others [7]. The interconnected setting of SNSs has made it possible for apps to easily collect personal information about users' friends, thereby emphasizing the problem of interdependent privacy. In this situation, the affected friends typically have little influence to prevent such information flows.

The problem of interdependent privacy is common in social app marketplaces since social apps can request a broad range of information about users' friends. Such information includes but is not limited to friends' birthday information, friends' photos, friends' online presence, and friends' location data. Further, given the high frequency at which social apps are installed, the flow of friends' information to outside developers can be substantial, even if only a limited number of apps request a specific type of information [1].

While the issue of interdependent privacy grows in practical importance, only a limited number of research studies have appeared on this subject, particularly in the scenario of app adoption. Although our previous work proposes an economic approach to study how large groups of app users act in an interdependent privacy scenario [8], it addresses this problem space only from a theoretical perspective. Therefore, more empirical studies are needed to understand app users' attitudes and behaviors under the consideration of interdependent privacy. To this end, in this dissertation, we discuss three empirical studies that focus on social apps' interdependent privacy issues.

1.1 Overview of Studies

The dissertation includes three studies to empirically study the problem space of interdependent privacy under the scenario of social app adoption. Specifically, applying different methods of conjoint analysis, we first quantify the monetary value which social app users place on their friends' information. We then utilize the method of structural equation modeling (SEM) as well as regression analysis to comprehensively explore the valuation process of interdependent privacy. In particular, we analyze how factors, such as data collection context relevance (Study 1 & Study 3), online social capital (Study 2) and sharing anonymity (Study 3) impact the monetary value of interdependent privacy perceived by social app users.

1.1.1 Study 1

In this study, we aim to first quantify the value social app users place on their friends' information, and then take a step further to explore factors that influence this valuation.

To achieve these goals, we first conduct an online user study by replicating our prior work on interdependent privacy valuation [9]. Specifically, following the procedures in [9], we conduct a new full-profile conjoint analysis study with two treatment conditions which vary the *app data collection context* (context relevance), i.e., to which degree the functionality of the app makes it necessary for the app developer to collect friends' information. Analyzing the data, we are able to quantify the monetary value which app users place on their friends' and their own personal information in each context.

Next, through combining interdependent privacy valuations with the responses to a comprehensive survey, we apply SEM analysis to investigate the roles of privacy concern, its antecedents, as well as app data collection context to work towards a model of interdependent privacy for the scenario of social app adoption.

We find that individuals' past experiences regarding privacy invasions are negatively associated with their trust for social apps' proper handling of their personal information, which in turn influences their concerns for their own privacy. In addition, positive effects of users' privacy knowledge on concerns for their own privacy and concerns for friends' privacy regarding app adoption are partially supported. These privacy concerns are further found to affect how users value their own and their friends' personal information. However, we are unable to support an association between users' online social capital and their concerns for friends' privacy. Nor do we have enough evidence to show that treatment conditions moderate the association between the concern for friends' personal information and the value of such information in app adoption contexts.

1.1.2 Study 2

In Study 1, most of the factors proposed as antecedents of interdependent privacy value are not supported, but the impact of some factors is only partially examined. To complement our first study, our second study aims to better explain the valuation of interdependent privacy in contexts of social app adoption.

Specifically, the complex relationship between interdependent privacy value and social capital is yet undetermined. Broadly speaking, social capital is a resource accumulated through individuals' interactions with others [10]. In particular, there are two kinds of social capital: bridging social capital and bonding social capital [11]. Bridging social capital, which is linked to loose connections between acquaintances, helps individuals to broaden world views and opens up opportunities for information gathering [12]. Bonding social capital, which derives from close-knit relationships between family members and close friends, is associated with trust and reciprocity, and provides strong emotional or substantive support for one another [11, 12]. With regards to the association between privacy value and social capital, some believe those who have a higher level of social capital are more willing to engage in

disclosure behaviors, and hence value interdependent privacy less. Others argue that the higher the level of social capital individuals have, the more likely they carefully evaluate actions that might harm others in order to maintain social capital, and therefore place higher value on friends' information. These two contradictory views motivate us to empirically investigate how social capital influences the value of interdependent privacy in the context of social app adoption.

To address these research goals, we conduct a series of regression analyses on data obtained from Study 1 to understand the impact of social capital, data collection contexts, as well as number of friends on interdependent privacy value.

Although, we fail to find a significant association between bridging social capital and interdependent privacy value, our analysis suggests that the value app users place on their friends' information is reversely related to the level of bonding social capital they have. In addition, we find the impact of bonding social capital on interdependent privacy value varies with app data collection context. Furthermore, we detect a cross-over interaction between number of friends and data collection context on interdependent privacy value. In particular, we find when app users notice data collection about friends is useful for app performance, the more friends they have, the less value they place on all their friends' information.

1.1.3 Study 3

In Study 1 & Study 2, we quantify and briefly explain the valuation of interdependent privacy. However, the understanding of important contextual factors that influence interdependent privacy decision-making is still in its infancy. In particular, we do not yet understand how characteristics of the platform which mediates the sharing, influence human choices about others' privacy. A key aspect is to which degree transparency (between the sharer and the affected individuals) about a sharing decision influences the propensity to share information, or affects valuation of personal information of friends. In other words, Study 3 investigates whether

different modes of *anonymity* (or identifiability) influence how a sharing decision is perceived when it affects interdependent privacy valuation.

To address this research question, we quantify the value which app users attribute to their friends' information (i.e., value of interdependent privacy) and aim to understand how this valuation is affected by two factors: sharing anonymity (i.e., whether disclosure of friends' information is anonymous), and context relevance (i.e., whether friends' information is necessary for apps' functionality). Specifically, we conduct a between-subject, choice-based conjoint analysis study with 4 treatments (2 sharing anonymity $\times$ 2 context relevance), which enables us to investigate the impact of these 4 conditions on interdependent privacy valuations.

In addition, besides the factors we investigate in Study 1, we also explore how other previously unconsidered factors, such as other-regarding preference, perceived privacy control, and disposition to value privacy, affect interdependent privacy valuations by applying structural equation modeling analysis.

Our results suggest that valuation of interdependent privacy is affected not only by individuals' personal attributes and experiences, such as other-regarding preference and privacy knowledge, but also by treatment conditions. In particular, we find that anonymity plays an important role in interdependent privacy valuation. Specifically, when individuals believe sharing of friends' information is anonymous, they tend to value their friends' data significantly *less*. Similarly, we find app users place a significantly lower value on their friends' information when they believe such information is useful for an app's functionality, which is in line with the findings in Study 1.

1.2 Contributions

Our work not only advances our understanding of interdependent privacy issues, particularly in the scenario of social app adoption, but also offers useful suggestions

for conducting human behavioral studies.

1.2.1 Understanding the Interdependent Privacy Problem

1.2.1.1 Expand Privacy Literature

One of our main contributions is addressing the still insufficiently investigated research area on privacy, i.e. interdependent privacy issue in app adoption scenarios. Specifically, we present:

- **One of the first empirical studies on the topic of interdependent privacy**. Although the issue of interdependent privacy grows in practical importance, this problem space has been primarily addressed from a game-theoretic perspective in the app adoption scenario. To the best of our knowledge, no empirical research has investigated this subject in the scenario of social app adoption. Our work addresses this literature gap by contributing to a better understanding of interdependent privacy from the perspectives of individuals' perceptions, knowledge, and preferences.

- **The first work to quantify the value of interdependent privacy.** Previous studies offer multiple insights about individuals' valuations of their *own* privacy. Our study complements the privacy valuation literature by quantifying the value which individuals place on their friends' information, i.e., value of interdependent privacy.

- **The first attempt to investigate relationships between privacy values and other constructs.** A number of empirically descriptive research works have focused on the relationship between privacy and other constructs. Instead of explicitly examining the value of privacy itself, almost all of these studies use privacy concern as a measurement proxy for privacy [13]. Our

study takes a further step to investigate this relationship by taking the value of own and interdependent privacy into consideration.

- **The first work to investigate the impact of sharing anonymity on privacy valuation.** The understanding of important contextual factors that influence interdependent privacy decision-making is still in its infancy. In particular, we are unaware of any research that directly addresses the question as to which degree transparency about a sharing decision affects valuation of privacy. Our work addresses this literature gap by investigating whether modes of anonymity (or identifiability) influence how a sharing decision is perceived when it affects interdependent privacy valuation.

1.2.1.2 Offer Implications for Privacy by Redesign

Besides offering a better understanding of individuals' perceptions, knowledge and preferences regarding interdependent privacy, this dissertation also offers insightful implications to the "privacy by redesign" debate [14].

- **Design to reflect data collection context relevance.** Research has proven that presenting privacy information in a clearer fashion to users when they are making adoption decisions can assist users in choosing less privacy-invasive apps [1, 15]. Our studies demonstrate that data collection contexts affect how users value their friends' information. Therefore, in order to help app users make well-informed decisions, it would be helpful to revise apps' privacy notice dialogues so that they explicitly inform users whether apps' practices of collecting data is necessary for the app's functionality. Alternatively, technical approaches which reverse-engineer apps to infer their usage of requested information can provide outside help for users [16, 17].

- **Design to inform data sharing anonymity.** Our results highlight that informing individuals of whether or not sharing friends' information with apps

is anonymous affects how they valuate interdependent privacy. Given that, a viable way to protect friends' privacy is not only to make such information sharing observable, but also to inform app users that the behavior of sharing friends' data is identifiable. For example, certain mechanism should be proposed so that when individuals share their friends' data, their friends will be notified about these sharing behaviors. In addition, a platform provider can appropriately modify apps' authorization dialogues, so that they convey the information to app users that sharing friends' information will be later discoverable by friends.

- **Design to control flow of friends' information.** Our work indicates that app users are privacy egoists [9] not only in that they trade off their friends' information for accruing social capital, but also due to the fact that they are eager to reveal friends' data when they believe such disclosure behaviors result in better app performance. As such, relying on individuals themselves to protect their friends' privacy is likely not adequate. Therefore, affected friends of app users should be involved more directly in the decision-making process. For example, designs that enable mutual agreements regarding sharing others' data, e.g., reciprocal designs that allow one to share others' information if and only if he/she also lets others to share his/her information, should be implemented. Alternatively, we can also introduce mechanisms that empower affected friends unilaterally to decide whether or not to allow their information to be shared by others.

1.2.1.3 Provide Insights on Privacy Policy Discussions

The thesis also contributes to the policy discussion on app privacy.

- **Resolve privacy externality problems.** The central point regarding the problem of interdependent privacy is negative externality, i.e., those who

install apps that collect personal information of friends do not directly suffer from interdependent privacy harms. Much like what economists generally suggest to deal with negative externalities [18], government interventions or self-regulation need to be considered for the problem space of interdependent privacy in social app adoption scenarios. For example, it is of vital importance that policies or laws are introduced to rigorously limit apps' practice of collecting friends' data.

- **Deal with privacy egoists.** In addition, as aforementioned, it is not adequate to rely on app users to protect their friends' privacy since app users are often privacy egoists. This further emphasizes the importance of government intervention to address the issue of interdependent privacy.

- **Promote education on privacy.** Our work confirms that privacy knowledge impacts the values which app users place on friends' information. This indicates that educating app users about practices impacting interdependent privacy might be a viable way to increase their valuation of interdependent privacy. Therefore, policy makers should consider introducing policies which integrate privacy in educational programs.

1.2.2 Suggestions for Conducting Human Behavioral Research

Besides advancing our understanding of interdependent privacy in social app adoption scenarios, our work also offers useful suggestions for conducting human behavioral research.

- **Choose appropriate methods for conjoint analysis study.** We utilize the full-profile conjoint analysis, and choice-based conjoint analysis in Study 1 and Study 3, respectively, to quantify the value of interdependent privacy. Through comparing these two studies, we find that full-profile conjoint study likely poses a significant cognitive challenge to human subjects, and therefore

results in lower data quality compared with the choice-based conjoint analysis. Therefore, we suggest the use of the choice-based method when conducting conjoint analysis studies that involve complex decision-making.

- **Use screening task to improve data quality.** The inclusion of an ice-cream screening task, which is similar to the app conjoint analysis experiment, has contributed to largely increase data quality in Study 1 compared with the results in [9]. This suggests that utilizing screening tasks that are similar to the central task, which serves as a main purpose, is a viable way to increase data quality in human behavioral studies.

1.3 Structure of Dissertation

The rest of the dissertation is structured as follows. In Chapter 2, we provide necessary background information about our study and discuss related work. Chapter 3 presents the details of Study 1. Specifically, it explains how to apply the conjoint analysis approach to elicit the value that app users place on their friends' information, and details about using SEM to explore factors that affect interdependent privacy valuation. In Chapter 4, we present Study 2, which complements Study 1 by more thoroughly explaining valuation of interdependent privacy in app adoption scenarios. In Chapter 5, we discuss details of Study 3, where we present a between-subject, choice-based conjoint analysis study with 4 treatments (2 sharing anonymity $\times$ 2 context relevance) to investigate impacts of contextual factors, in particular sharing anonymity, on interdependent privacy valuations. Finally, we conclude in Chapter 6.

Chapter 2
Background & Related Work

2.1 Social Apps' Privacy Issues

2.1.1 Social Apps on Social Network Sites

Our work is primarily motivated by incidents that highlight the potential negative privacy and security consequences of social app adoption on social network sites. A selected number of studies have demonstrated that social app developers sell user information to advertising and data firms [6, 19, 20]. Given that it is usually hard to observe data practices after users authorize app developers to access their profiles, these studies are highly valuable.

From a more user-centered perspective, several studies focus on the disclosure and authorization procedures associated with social app adoption. For example, several user studies show that app users are concerned about privacy issues associated with app adoption, and that they have only an incomplete understanding or even misunderstanding about apps' practices of collecting their profiles [21–23]. In addition, another stream of user studies investigates how app users' behaviors are impacted by interface improvements of the authorization dialogues for social apps [1, 24].

A different set of studies measure aspects of the permission-based system for

social apps on social network sites [25–27], e.g., the most frequently requested permission, the average number of permissions for all apps, and specific categories of permissions requested. In particular, by investigating permission systems of the 9,411 most popular Facebook apps, Wang et al. [1] provide evidence for the significance of the interdependent privacy problem. Table 2.1, which is an abbreviated version from their study, summarizes the number of requests for the 16 types of permissions involving information of users' friends. These permissions not only cover friends' basic information such as friends' hometowns, but also involve more sensitive data such as friends' birthdays, friends' locations, or even friends' photos and videos. Wang et al. [1] report that while specific permissions are only collected by a small subset of apps, the impact of these data collection practices is nevertheless significant given the high frequency at which these apps are installed by users. For example, friends' birthday information is accessed in bulk by Facebook apps in almost 20 million cases. Taking into consideration the average number of friends of a typical user, the total amount of leaked information is considerable; i.e., a Pew Research Center survey found that users have on average over 300 friends [28].

2.1.2 Social Apps on Mobile Networks

What is also gaining increasing importance are security and privacy issues associated with social apps on mobile networks. It has been documented that app developers have been trying to utilize users' devices for spam and unwanted costly services [29]. Further, most apps are found to include permission requests that enable potentially dangerous practices [30].

Similar to studies of apps on social network sites, research has documented usability problems associated with social apps on mobile networks [15, 31] by investigating their permission-based systems. In reaction to these privacy issues, several studies propose technological measures to help users to manage permissions

Table 2.1: Most frequently requested Facebook permissions explicitly involving information of users' friends (abbreviated table from Wang et al. [1])

Permission	Number of apps requesting permission	Percentage of apps requesting permission	Total times a permission is requested by apps
friends_birthday	206	2.19%	19,237,740
friends_photos	214	2.27%	13,051,340
friends_online_presence	121	1.29%	10,745,500
friends_location	104	1.11%	8,121,000
friends_hometown	21	0.22%	5,862,500
friends_work_history	86	0.91%	5,260,660
friends_education_history	14	0.15%	3,564,500
friends_activities	22	0.23%	3,448,300
friends_about_me	17	0.18%	3,328,000
friends_interests	13	0.14%	3,163,500
user_work_history	73	0.78%	2,961,900
friends_relationships	3	0.03%	2,912,000
friends_photo_video_tags	32	0.34%	2,423,340
friends_likes	36	0.38%	2,385,960
friends_checkins	6	0.06%	1,350,000
friends_relationship_details	4	0.04%	741,000
friends_videos	2	0.02%	230,400

on mobile systems. For example, a system that can disable information requests made by a mobile app and unwanted permissions is introduced by Beresford et al. [32].

Further, much like apps on social network sites, mobile apps can gain access in various ways to information of friends. For example, for apps with multi-platform functionality, if they have the ability to get access to a user's Facebook account, they will be able to share the same information in the mobile context. Besides that, mobile apps are able to share additional information that is gathered in the mobile context. These information includes but is not limited to users' SMS and MMS (i.e., personal and professional communications with other users) [33].

Auditing over 800,000 apps in the Android play store, security firm BitDefender

reports that apps frequently request information affecting users' friends or other contacts. For instance, 10% of these apps request access to users' contact lists, and a few of them even leak users' call histories [34]. The same phenomena are observable in the iOS app market as demonstrated by a survey from Zscaler [35]. For example, they discover that among the 25 most popular apps 92% request access to users' address books, and 32% include a permission to access users' calendars, which may include references to other individuals.

In aggregate, these studies document many challenges faced by users for identifying privacy consequences of social apps, as well as for implementing their privacy preferences when making app adoption decisions. In particular, these studies also highlight the problem of interdependent privacy in the scenario of app adoption, which will be comprehensively investigated in this dissertation.

2.2 Interdependent Privacy

The problem of interdependent privacy is gaining increasing importance. Several researchers have begun to study the problem of interdependent privacy primarily from theoretical perspectives. A small number of research papers have focused on this problem in domains of SNSs and social app adoption. Taking a first step, Biczók and Chia [7] define the notion of interdependent privacy, and develop a game-theoretic 2-player model to study users' app adoption decisions under the presence of this particular privacy issue. By proposing and simulating a more comprehensive app adoption model on networked systems, Pu and Grossklags [8] discover that even rational app users who care about others' well-being would likely install apps that cause high levels of interdependent privacy harm. By presenting a visual network analysis, Biasiola [36] shows the nature and scope of friends' data leakage through users' ties to an app. Symeonidis et al. [4] assess interdependent privacy consequences of app installation based on a model and a privacy scoring

formula they propose. In addition, by proposing and analyzing the complexity of an optimal inference algorithm, Olteanu et al. [37] quantify interdependent privacy risks of location data on SNSs. Some others study interdependent privacy issues within other contexts. For example, Chessa et al. [38] propose and analyze a game-theoretic model of a data analytics project that has interdependent privacy consequences. Also applying a game-theoretic approach, Humbert et al. [39] study interdependent privacy problems associated with genomic data.

The issue of interdependent privacy has also been investigated from legal perspectives. Some law articles have highlighted the existence of the interdependent privacy problem in contexts of eligibility, data mining, and social networks [40, 41]. Recognizing the problem of interdependent privacy, Fairfield and Engel [41] argue that privacy is a public good, and hence a group-focused approach should be adopted for privacy protection. In addition, through analyzing current notice-and-choice policies, MacCarthy [40] reports these polices fail to address the problem of interdependent privacy. Instead, he recommends the implementation of a unfairness framework as a way to deal with privacy externalities.

Further, a different set of studies addresses the problem space of interdependent privacy through analysis of user data or surveys. Based on users' comments posted on Facebook's official blog, Shi et al. [42] analyze SNS users' interpersonal privacy concerns when their information is leaked by others' actions. Choi and Jiang [43] develop survey instruments of collective privacy concerns, e.g., concern for the violation of collective privacy that includes an individual's, others' and a group's information privacy. Applying these instruments, they aim to identify antecedents of collective privacy concerns. Through a survey study involving 265 participants, Morlok [44] examines how factors such as external information privacy concerns and external social privacy concerns affect individuals' intentions to disclose information about others. Similarly, Alshoor and Keil [45] propose a SEM model to study the same relationships. Also utilizing a survey study, Krasnova et al. [46] elicit levels

of Facebook users' privacy concern regarding the release of 38 different information items including data about friends. In addition, research questions such as how individuals' information disclosure behaviors are influenced by disclosure actions of others and existing disclosure norms on marketplaces have also been empirically investigated [47, 48].

Although these studies highlight important aspects of the interdependent privacy problem, little empirical research has been proposed or conducted to quantify the (monetary) value of interdependent privacy, or to explain such a valuation process. To address this literature gap, we describe three studies to quantify and explain the perceived value of friends' privacy by social app users.

2.3 Valuation of Privacy

Viewing privacy as an economic good [49], the perspective of privacy calculus expects consumers to perform a risk-benefit analysis in assessing the outcomes they will receive as a result of information disclosure [13, 50–52]. This viewpoint is adopted in several works on privacy issues [50], particularly, in the domain of privacy valuation research. By putting individuals in implicit or explicit trade-off scenarios, such as surveys, field experiments, discrete choice experiments, and conjoint analyses, prior research has shed light at the value individuals place on their own personal privacy. A different perspective is adopted by Grossklags and Barradale who measure the joint preferences (i.e., not the trade-off) for privacy and security in a laboratory experiment [53].

Previous (survey and experimental) studies offer multiple insights about personal privacy perceptions. For example, researchers have developed a privacy concern score for individuals, which is calculated on a seven-point Likert-type scale, to represent how consumers value their privacy in an online context [54]. Similarly, responses from a survey including questions on disclosure of personal information

to commercial entities have been used to measure privacy values [55].

Other studies try to understand the value of privacy by conducting experiments that typically involve users' choices of selling and protecting personal information, or offering some form of recommendation or discount [56]. For example, Beresford et al. [57], Jentzsch et al. [58] and Tsai et al. [59] find that consumers are willing to pay a (typically small) premium in order to purchase more privacy-friendly products; Grossklags and Acquisti [60] demonstrate that the average amount of money users are willing to accept to reveal their information is higher than the average amount they are willing to pay for protecting their privacy. Conducting auctions is another method used to elicit the value people place on personal information. For example, Huberman et al. [61] apply second-price auctions to measure the perceived value of individuals' weight and height information. Using a related methodology, Danezis et al. [62] evaluate the value of location information for individuals from European Union countries. Acquisti and Grossklags study the robustness of monetary valuations for different types of personal information to reframing of marketers' offers [63].

A different set of studies use discrete choice experiments to understand the valuation of privacy. Applying this method, Potoglou et al. [64] estimate the value of personal information in three real-life contexts and situations. They find that while individuals have a low willingness to pay to control their personal data, the extent of personal data collection by third parties is the most important factor impacting users' online retailer choice. Using a similar method, Egelman [65] and Krasnova et al. [66] investigate concerns about users' information disclosure when presented with sign-on mechanisms such as Facebook Connect.

Conjoint analysis has been utilized to investigate individuals' privacy valuations and to explore the trade-off between the benefits and costs of revealing personal information online [67, 68]; also in the scenario of SNS [69]. These researchers also derived the monetary value of an individual's personal information [67–69].

In aggregate, these studies utilize different methods to quantify the value individuals place on different types of their own personal information. However, only few studies have addressed the monetary value of interdependent privacy. Our research applies the conjoint analysis method and extends [69]'s work to the scenario of social app adoption. Specifically, we extend their work by considering interdependent privacy as a key attribute, as well as by introducing and comparing different contextual conditions regarding data collection and data sharing.

2.4 Privacy Concerns and Other Constructs

A number of empirically descriptive research works have focused on the relationship between privacy and other constructs. Instead of explicitly examining the value of privacy itself, almost all of these studies use privacy concern as a measurement proxy for privacy [13]. Several studies focus on investigating the relationship between a number of antecedents and measures of privacy concerns. For example, Smith et al. [70] find that individuals who have experienced an invasion of their privacy tend to have stronger concerns regarding information privacy than those who did not. Privacy awareness, which indicates the extent to which an individual is informed about organizational privacy practices [71], has also been found to be one of the factors which impacts consumers' privacy concerns [72]. Researchers also discovered that personality differences, such as the "big-five" personality traits [73], and measures of introversion versus extroversion [74], have an impact on individuals' formation of privacy concerns.

In addition to these works that examine associations between antecedents and privacy concerns, other studies investigate outcomes of privacy concerns. Focusing on behavioral reactions, Eastlick et al. [75] find that privacy concern has a significant impact on online purchase intention; Metzger [76] and Xu et al. [77] argue that concern, together with trust, affect individuals' willingness to disclose information to

others. In addition, taking a policy perspective, Metzger [76] and Turow et al. [78] argue that consumers' privacy concerns should be addressed by regulation efforts due to the complexity of privacy decision-making. In addition, using a natural experiment, research also demonstrated how individuals' information disclosure behaviors are influenced by disclosure actions of other users and existing disclosure norms on marketplaces [47, 48].

Although these studies highlight associations between privacy and other constructs, their discussion is only limited to concerns for individuals' personal privacy. To the best of our knowledge, there is no published research addressing the relationship between such constructs and interdependent privacy concerns, or explaining the (monetary) value of friends' personal information. To address this gap, we construct a SEM model for the scenario of third-party social app adoption to investigate relationships among app users' privacy concerns for both themselves and their friends, antecedents of such concerns, and the economic value which users place on their own and friends' personal information.

2.5 Anonymity in Individual Decision-Making

A set of studies in the area of experimental economic research has focused on the influence of anonymity on decision-making. In particular, the experimental literature on economic bargaining games which mostly centers on the analysis of the so-called ultimatum game [79] and dictator game [80] is of high relevance. In the classical version of both games, a monetary amount (i.e., pie) is offered for allocation between two individuals. One person acts as the proposer and can suggest a split of the pie. In the ultimatum game, the recipient of the proposal can reject the offer (then the money will remain with the experimenter) or accept the split [79]. In contrast, in the dictator game the recipient has no decision-making power (and the pie is allocated according to the proposed split) [80]. A specific sub-area of

this literature is addressing the impact of anonymity from two perspectives: 1) anonymity between proposer and recipient, 2) anonymity between players and experimenter (i.e., double-blind).

Radner and Schotter compare face-to-face (F2F) bargaining with anonymous bargaining and find that the latter was associated with an increase in rejected proposals, while the former was associated with an almost uniform acceptance rate [81]. Prasnikar and Roth report similar results [82]. However, they also find that F2F communications that explicitly exclude any form of conversation about the relevant bargaining aspects and are merely social in nature, also contribute to an almost uniform acceptance rate of proposals which were later issued without additional F2F exchanges [82]. During the latter treatment, participants were required to learn the name and education level of their bargaining opponents. The finding of this social conversation treatment was interpreted to confirm that social pressures arising from F2F are influencing subjects; rather than the discussion of any pertinent aspects of the transaction [83]. Similarly, Charness and Gneezy conduct dictator and ultimatum game experiments in which they compare treatments in which participants were informed about the family names of their counterparts (or not) [84]. This manipulation strongly impacted the generosity of proposers in the dictator game, but not the initial offer of the proposers in the ultimatum game where strategic considerations seemed to prevail [84]. Hoffman et al. introduced a double-blind setup in which the experimenter could not identify the experimental participants [85]. The results indicate that this double-blind setup was associated with the most selfish offers by the proposer. Experiments have also been conducted in the field to document the negative impact of anonymity on donations for environmental causes [86] or in churches [87].

In addition, a stream of information system research investigates the impact of anonymity on individuals' self-disclosure on social network sites. These studies mainly focus on two types of anonymity: discursive anonymity and visual anonymity.

Discursive anonymity refers to the extent to which information can be linked to a particular source [88], whereas visual anonymity indicates the degree to which others can see and/or hear the person who discloses the information [88]. Although focusing on this topic for more than a decade, researchers have not reached an agreement on either the impact of discursive anonymity or the influence of visual anonymity on self-disclosure. For example, Qian and Scott [89] report a positive relationship between self-disclosure and discursive anonymity. However, this association is found to be negative by Hollenbaugh and Everett [90]. When it comes to visual anonymity, some studies claim that it is positively related to self-disclosure [90, 91], while other research fails to detect such an association [89]. These contradictory empirical findings suggest that the relationship between anonymity and self-disclosure in online social networks is still in question and should be further examined [90].

Most related to our work, some studies have begun to explore the impact of anonymity on individuals' privacy attitudes or privacy behaviors. In particular, through an empirical study involving 251 respondents, Jiang et al. [92] report that when individuals perceive themselves to be unidentifiable, they feel less concerned about their privacy. In addition, they find that individuals exhibit higher level of concerns about their own privacy when other parties' identities are anonymized. However, we are still unaware of any research that directly addresses how anonymity impacts individuals' attitudes towards others' privacy. Our study addresses this literature gap by exploring the impact of anonymity on the valuation of interdependent privacy.

2.6 Resolve Interdependent Privacy Conflicts

Privacy conflicts may arise from interdependent privacy issues, where privacy preferences of those who share others' data and those whose information is leaked are not aligned. These privacy conflicts are referred to as multi-party privacy

conflicts (MPCs) [93]. Several research projects explore how to resolve conflicts arise from interdependent privacy issues in social media, although not in the scenario of social app adoption. A stream of these studies focuses on providing computational mechanisms or external tools to deal with MPCs. For example, in the scenario of photo sharing on social network sites, a system has been proposed so that when a user is tagged in a photo, he/she can send privacy suggestions or feedback to those who upload the photo [94]. Also in the scenario of photo sharing, Ilia et al. [95] introduce a mechanism of blurring faces of individuals (who appear in photos) based on a users' access control permissions.

To provide support for users to resolve MPCs, some studies propose sharing policies based on aggregate individual privacy preferences. For example, Hu et al. [96] formulate an access control model, multi-party policy specification scheme, and a policy enforcement mechanism to facilitate collaborative management of shared data. Thomas et al. [93] demonstrate how Facebook's privacy model can be adapted to enforce multi-party privacy. Similarly, other mechanisms or access control policies have been introduced in [97, 98] to address MPCs.

Other researchers try to address MPCs from the perspective of game-theoretic analysis. For example, Hu et al. [99] study a multi-party access control model to investigate systematic approaches to identify and to resolve conflicts of collaborative data sharing. Similarly, a negotiation mechanism is introduced and examined to help users to reach an agreement under cases of MPCs [100].

There is another stream of studies which explores strategies users have utilized to resolve MPCs. Wisniewski et al. [101] demonstrate that individuals use both online strategies, such as untagging, and offline strategies, such as negotiating offline with affected others before posting photos. In addition, they also investigate how support mechanisms that are provided by social media interfaces are used by individuals for addressing MPCs [102]. They conclude that these mechanisms are ineffective, difficult to use, and not easy to be aware of, and therefore users are

more likely to apply offline coping strategies.

Through conducting a qualitative study with 17 individuals, Lampinen et al. [103] discover that users apply a range of preventive strategies to avoid causing problematic situations for others. In particular, they categorize 4 types of strategies: preventive, corrective, individual, and collaborative. Similarly, Cho and Filippova [104] identify the same types of strategies based on findings from focus-group interviews and online surveys.

In aggregate, these studies investigate different ways of resolving privacy conflicts that arise from interdependent privacy issues in social networks. However, we are unaware of any research that directly explores MPCs in the context of social app adoption. Our research provides insights for dealing with such privacy conflicts.

Chapter 3

Study 1: Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy

In the context of social apps, the problem of *interdependency of privacy* refers to users making app adoption decisions which cause the collection and utilization of personal information of users' friends. In contrast, users' friends have typically little or no direct influence over these decision-making processes. While the issue of interdependent privacy grows in practical importance, it has been primarily addressed from a game-theoretic perspective in the app adoption context [7, 8], or in data analytics or genetic privacy scenarios [38, 39]. In this chapter, we present our work that contributes to a better understanding of interdependent privacy from the perspectives of individuals' perceptions, knowledge and preferences.

More specifically, we present a survey study with an online user population. We first collect data about individuals' valuations for interdependent privacy by following a full-profile conjoint analysis study approach with an experimental manipulation. We then aim to explain the valuation of interdependent privacy by

utilizing responses to carefully designed survey measures and analyzing the data from the viewpoint of an associated set of research hypotheses. Based on this combined data, we perform SEM analysis to understand which survey measures influence directly or indirectly how users economically value the personal information of their friends in an app adoption scenario.

To be more specific, we first implement and conduct a full-profile conjoint analysis study which is a common approach to study the relative importance of different decision-making factors, for example, popularity, features and privacy aspects of product adoption [105]. Conjoint analysis studies have been previously used in the context of user privacy in electronic commerce [67, 68] and SNSs [69] to determine the economic value users place on their own personal information. We apply the conjoint analysis study approach to the app adoption context with a particular focus on the valuation of the personal information of users' friends within a SNS. Further, motivated by the principle of contextual integrity [106], we aim to study how individuals' valuations of friends' personal information are influenced by different app data collection contexts. For this purpose, we introduce two treatments in the conjoint study setup: (T1) friends' information collected by the app does *not* improve its functionality, and (T2) friends' information collected by the app improves its functionality.

We then collect participants' responses to survey measures including users' past privacy invasion experiences, privacy knowledge, trust in apps' data practices, online social capital, as well as privacy concerns for both themselves and their friends regarding app adoption. Using this data, we apply SEM analysis to discover the antecedents not only to users' own privacy concerns, but also to their concerns for friends' privacy in the specific scenario of social app adoption. In addition, we go a step further by addressing the relationship between measures of privacy concern and their antecedents on the economic value which app users place on their own and friends' information. We further aim to understand whether or not *app*

data collection context moderates the relationship between users' privacy concerns and privacy value, in particular, with respect to the value of their friends' personal information in social app adoption scenarios.

The remainder of this chapter is organized as follows. In Section 3.1, we discuss the full-profile conjoint analysis approach to elicit the values which app users place on their own and their friends' personal information in the context of social app adoption. In Section 3.2, we explain the valuation of interdependent privacy. Specifically, we describe the SEM model hypotheses, model development methodology, data analysis and findings. Finally, we offer a summary in Section 3.3.

3.1 Conjoint Analysis to Determine Privacy Value

3.1.1 Design of Conjoint Study

Conjoint analysis assumes that consumers view a product as a bundle of certain features (*attributes*), which have different values (*levels*) [107]. By asking and analyzing individuals' preferences towards different versions of products, conjoint analysis helps to derive the value individuals place on each attribute level. Applied to our context of interest, we view a social app as associated with multiple app attributes. For example, one attribute would be the interdependent privacy practices associated with an app, and its corresponding levels will be the different amounts of friends' information collected. Through analyzing how individuals evaluate versions of different apps, we are able to understand the role of each factor during the app selection process, in particular how revealing friends' personal information influences the decision-making.

3.1.1.1 Determination of Attributes and Their Levels

Following Green and Krieger's suggestions [108], we conducted semi-structured interviews with social app users to determine app attributes in our conjoint study.

We recruited a convenience sample of 18 university individuals for face-to-face interviews. Interviewees had different ethnic backgrounds, and did not have previous employment backgrounds related to privacy. 10 of them had technical expertise and 8 had non-technical backgrounds. During the interview, we asked them to identify factors that affect their decisions to install an app. 17 out of our 18 interviewees believed one of the key factors that influences their app choice is the price of an app (*price*). In addition, in line with the research finding that positive network effects are an important motivator for individuals to use technologies [109], 17 participants argued that the level of an app's popularity among friends (*network popularity*) matters to them. Further, 13 interviewees reported that when faced with the decision of installing an app, they do not only take into consideration the amount of their own information the app collects (i.e., *own privacy*), but also care about the type and procedure for the collection of friends' information by that app (i.e., *friends' privacy*).

Given the interview responses, we believe that *price, network popularity, own privacy*, and *friends' privacy* are suitable attributes for a conjoint study on app adoption.

Next, we explain the levels chosen for these four attributes; for which the interviews also provided useful input. Interviewees indicated a preference for free apps, but also a willingness-to-pay of about $2 for attractive apps. Hence, we selected two levels for *price*: "$0.00" and "$1.99". In addition, we used the percentage of a user's friends who have already installed the app to represent *network popularity*. Since most apps are only used by a subset of network users, we used 5% and 25% to indicate modest and high levels of popularity as typical cases, respectively.

We selected levels for *own privacy* and *friends' privacy* by investigating app permission systems. Wang et al. [1] found that all Facebook apps collect a users' basic information such as user name and ID, and some of them request additional

Table 3.1: Summary of attributes and levels

Attributes	Attribute Descriptions	Attribute Levels
Price	Price of the app	\$0.00 \$1.99
Network Popularity	Percentage of a user's friends who installed the app	5% 25%
Own Privacy	Information the app collects about a user	None Basic profile Full profile
Friends' Privacy	Information the app collects about a user's friends	None Basic profile Full profile

information such as user's birthday and location information. However, we did not rule out the possibility that some apps would prefer to collect no information about users. In addition to collecting users' own information, some apps frequently access data about users' friends; although not all apps engage in such practices. Based on these observations, the three levels we selected for *own privacy* are "none", "basic profile" and "full profile". Similarly, we assigned three levels to *friends' privacy*: "none", "basic profile", and "full profile". "None" for *own privacy* and *friends' privacy* indicates that the app does not collect any SNS profile data about users, and about users' friends, respectively. The "basic profile" for *own privacy* includes users' name, profile picture, gender, user ID, number of user's friends, and any other information the user made public. Similarly, "basic profile" for *friends' privacy* represents an app aiming to collect friends' names, profile pictures, gender, user IDs, number of friends' friends, and any other information friends have made public on their profiles. For *own privacy*, "full profile" means a user's email-address, birthday, all photos, location information, and all information included in the "basic profile". Similarly, besides friends' "basic profile", the "full profile" of *friends' privacy* also includes friends' email-addresses, birthdays, all photos, and location information.

We show a summary of the app attributes and levels used in the conjoint analysis in Table 3.1.

3.1.1.2 Selection of Conjoint Analysis Method and Number of Stimuli

Conjoint analyses can be conducted in several ways. Among them, the two most popular methods are full-profile conjoint analysis and choice-based conjoint analysis. For the current study, we select the full-profile method. However, we apply the method of choice-based conjoint analysis in Study 3. We will discuss the details of choice-based conjoint analysis, as well as explain why we switch to that method later in Section 5.1.1.2.

When applying the full-profile approach, respondents are asked to rank a set of product profiles (*stimuli*) [110]. Particularly, respondents in our study are required to rank different app versions that are formed by combing different levels of the four app attributes. The attributes and levels in Table 3.1 yielded a total of 36 ($2 \times 2 \times 3 \times 3$) stimuli. Clearly, ranking so many apps poses a great challenge to respondents. In order to reduce the number of app versions in the study, we utilized the SPSS Conjoint 22 package to apply a fractional factorial design. This procedure generates an orthogonal array, which is a fraction of all possible combinations of factor levels and is designed to capture main effects of each factor level. By applying this method, we reduced the design from 36 possible app profiles to 9 app profiles.

3.1.1.3 Estimation of Conjoint Model

We utilized the SPSS Conjoint 22 package to estimate the utility value associated with each attribute level. It computes the utility of each attribute level in such a way that the actual rank ordering of a certain profile equals the rank ordering of utility sums of all levels in that profile. The following equation captures the main idea of this estimation method:

$$R_j = \beta_0 + \sum_{i=1}^{T} \beta_i X_{ij} + \varepsilon_j \tag{3.1}$$

where R_j is the ranking of profile j, β_0 is a utility constant, T represents the total

number of attribute levels, and β_i is the coefficient (utility value) to be estimated for attribute level i. X_{ij} is a $\{0, 1\}$ variable that equals 1 if profile j has attribute level i, and equals 0 otherwise. ε_j is a stochastic error term.

Following this method, we estimated the utility of each attribute level on an individual basis based on each participant's ranking.

3.1.2 Design of Survey Experiment

Utilizing a combination of Qualtrics and Amazon Mechanical Turk (MTurk), we conducted a web-based, between-subject online experiment. Specifically, we recruited participants from MTurk and asked them to access our study link on Qualtrics, where we had implemented the complete survey.

3.1.2.1 Screening Task

Although compared with traditional laboratory studies, MTurk enjoys several advantages such as more diverse demographics [111, 112] and lower payments [113], prior studies indicate that there is a substantial amount of Mechanical Turk users (Turkers) who do not exercise enough care with tasks or even use automated bots to complete assignments [114]. In particular, tasks with a high level of complexity, such as full-profile conjoint analyses, may fail to attract adequate attention from some Turkers. Therefore, careful inspection and filtering are necessary for these tasks [114, 115]. Downs et al. encourage to apply a screening process to remove the subset of Turkers who do not complete tasks conscientiously [114]. Following their suggestion, we introduced a screening task to help select Turkers with higher response quality in conjoint analysis tasks, who were then invited to our app ranking task.

The screening task, which also followed the methodology of full-profile conjoint study, required participants to rank a list of 12 ice cream versions (see Figure 3.1). These 12 ice cream versions differed in five attributes: price, size, brand, whether

they were served in cones or bowls, and whether or not they were made with organic ingredients. Quality of responses in the screening task was measured based on whether they demonstrated irregular consumer behaviors. Using attributes and levels that can be objectively ordered, i.e., lower price, bigger size and organic rather than conventional production, enables us to implement check conditions that can straightforwardly detect irregular consumer preferences. For example, we introduced in this task two small-size Ben & Jerry's ice creams, say ice-cream A and ice-cream B, that were both served in bowls. However, the organic ice-cream A costs $1.00 less than the conventional production ice-cream B. We then expect a reasonable consumer to prefer ice cream A over ice cream B. If participants' ranking results indicated otherwise, we regarded these submissions as violations of normal consumer preferences; likely attributable to low effort. We introduced five such check conditions in the ice cream screening task, and evaluated the quality of submissions based on the number of check conditions they passed.

Participants' demographic information such as gender and age were also collected in the screening task. Note that, besides serving to identify higher quality submitters, the ice cream ranking task also helped participants to familiarize themselves with the ranking interface, which was also used later in our app ranking task.

3.1.2.2 App Ranking Task and Survey Measures

The app ranking task, which is the main conjoint analysis ranking task, helped us to understand the relative importance of the different attributes in the choice of a social app. Specifically, through analysis of the ranking results, we are able to derive the economic value individuals place on their own as well as their friends' privacy. Further, in order to better understand how app users' valuations of their friends privacy are affected by different app data collection contexts, we introduced the following two treatment scenarios:

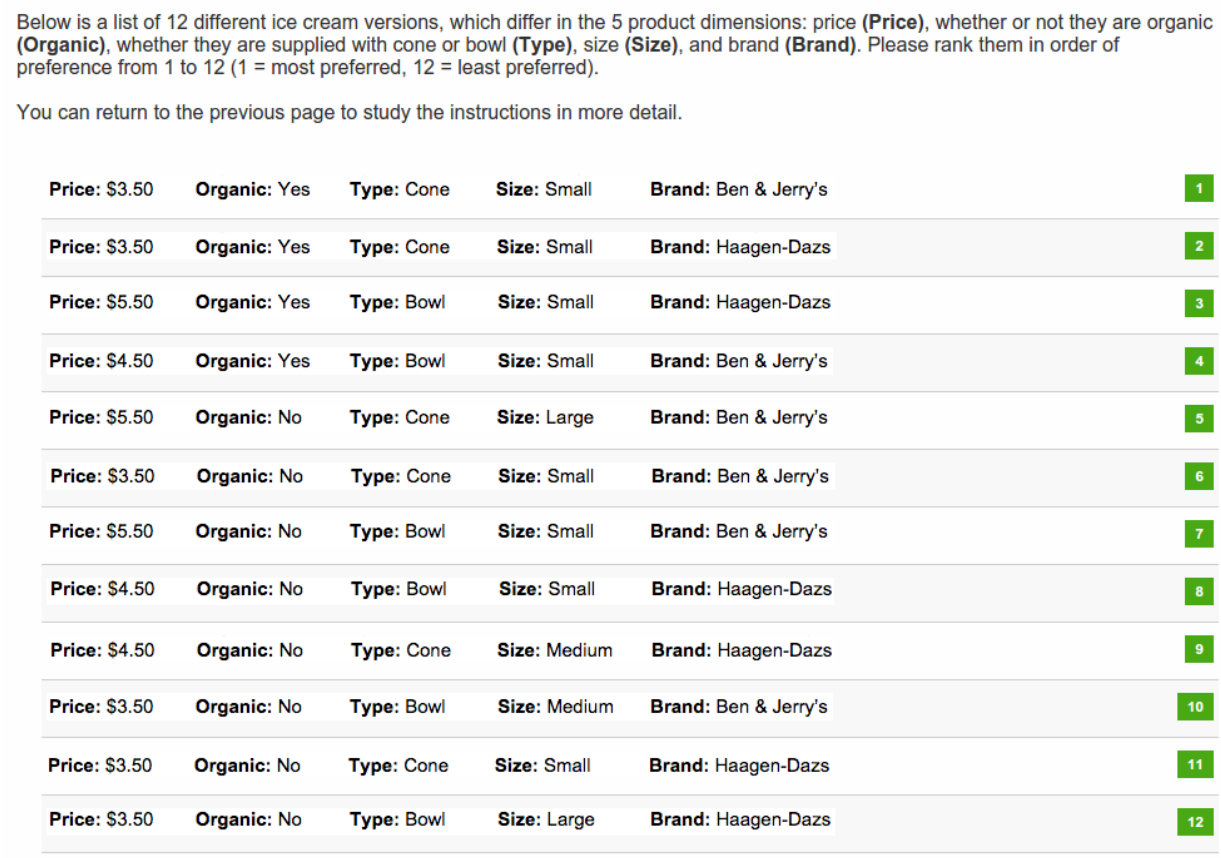

Figure 3.1: Screenshot of experiment interface (drag and drop interaction)

T1: *The information the app collects about user's friends is not useful for app's functionality.*

T2: *The information the app collects about user's friends is useful for app's functionality.*

We then randomly placed participants in one of the two treatment scenarios (which was introduced in the instructions for the app ranking task) and asked them to rank the 9 app versions. In addition, in order to evaluate the quality of participants' responses, we introduced four check conditions for the app ranking task, which were similar to what we used in the screening task and helped us to detect irregular consumer preferences.

Our work is not focused on the mere determination of the monetary value of interdependent privacy, but more importantly seeks to establish a model to comprehensively explain users' privacy evaluation processes in the social app adoption context. To this end, we developed a set of survey measures addressing individuals' past privacy invasion experiences, privacy knowledge, online social capital, trust in apps' data practices, as well as privacy concern for both themselves and their friends regarding app adoption. The responses were then used for the development of the SEM model. A detailed discussion of the hypotheses development and the measurement scales is provided in Sections 3.2.1 and 3.2.2, respectively. The exact questions are provided in Appendix A.

3.1.2.3 Procedures

The procedures of our online study were as follows: we first invited participants from MTurk to the ice cream screening task, where they were required to rank 12 ice cream versions (see Figure 3.1 for the ice cream ranking interface) and to answer demographic questions. We then evaluated the quality of responses based on how many check conditions they passed. Only those who passed all five check conditions were then invited to our main task, i.e., the app ranking task. After reading the instructions (including the treatment information), participants first ranked 9 app versions (see Figure 3.2 for the app ranking interface). Participants were then asked to complete the next study section which included the survey measures to be used in our SEM analysis.

We paid \$0.50 and \$1.00 to each participant in the screening task and the app ranking task, respectively. Our study followed a protocol reviewed and approved by the IRB of the Pennsylvania State University.

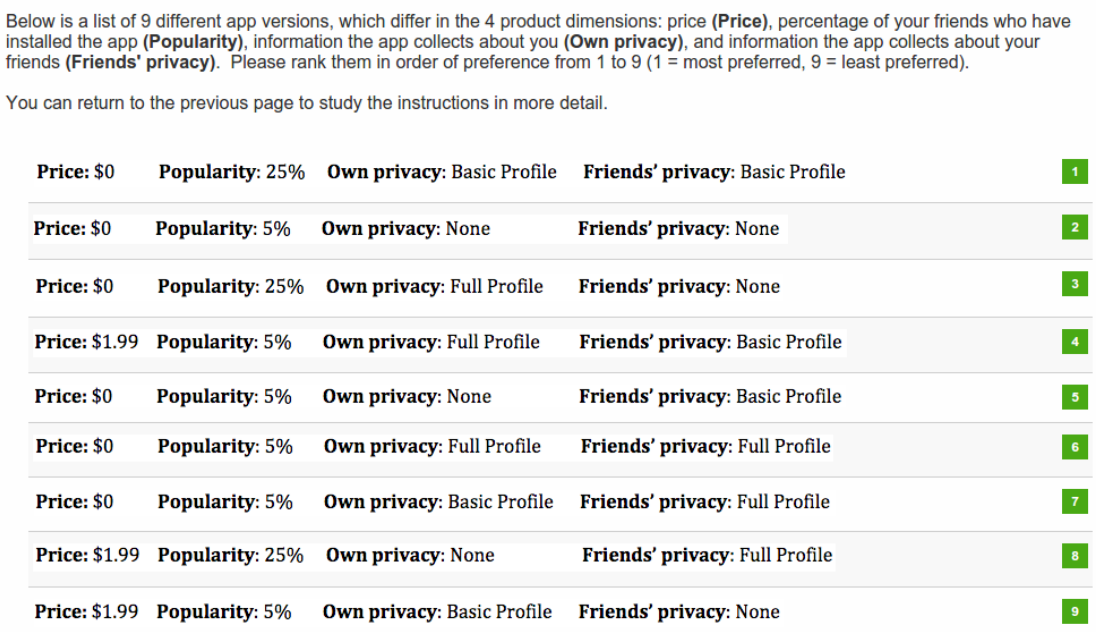

Figure 3.2: Screenshot of experiment interface (drag and drop interaction)

3.1.3 Sampling

Data collection was conducted in June 2015. We recruited a total of 1095 Turkers for the screening task. These Turkers had completed over 50 Human Intelligence Tasks (HITs) with a HIT approval rating of 95% or better, and had United States IP addresses. Among them, 497 participants passed all five check conditions. We then invited all these 497 individuals to our app ranking task. However, only 397, about 80%, Turkers responded to our invitation. Among them, 198 Turkers were assigned to T1 and 199 Turkers were assigned to T2.

As mentioned earlier, we also included four check conditions for the app ranking task, which were similar to those applied during the screening task. For example, irregular consumer preferences were measured by checking whether the ranking results showed that participants would prefer to pay a fee for an app, rather than receiving exactly the same app for free. We then counted the number of irregularities for each individual. Note here, we have previously conducted a similar app ranking

task on MTurk, however without a screening task [9]. This allows us to compare the distribution of irregularities across the two datasets. We find that the dataset with the screening task has a more than 10% higher percentage of participants without any irregular responses compared with our previous data collection. In our current study (with the ice cream screening task), the percentage of valid submissions is 72.3%, indicating that the screening task helps to select high quality submitters, but it remains an imperfect solution to the problem of shirking on Mechanical Turk.

For the current analysis, submissions with more than one irregular preference were excluded from the analysis to enhance data quality. We further excluded responses for which the monetary value of the attributes could not be estimated, as well as outliers. Through analyzing time of task execution, we were able to confirm the effectiveness of our data selection criteria since our records indicated that these excluded individuals did not exercise enough care with the completion of the ranking task and spent significantly less time on the task than included individuals ($p = 0.05$). Responses from 144 Turkers in T1, and 151 Turkers in T2 were used for analysis. Chi-square tests indicated that in both treatments, participants whose responses were excluded and participants whose responses were used did not significantly differ in age or gender.

Among 144 participants whose data were used in T1, 52.1% were male and 47.9% were female. 48.3% of the final sample in T2 were male; 51.7% were female. The average completion times for the ranking task and the survey measures were 8.5 minutes in T1 and 7.5 minutes in T2. Individuals in the final samples of T1 and T2 belonged to a wide range of age categories (from 18 to over 50). In addition, chi-square tests demonstrated that the two final samples did not significantly differ regarding either gender or age.

3.1.4 Analysis of Empirical Results

Conjoint analysis allows us to derive the final utilities (i.e., part-worths, which are represented by β_i in Equation 3.1) of each app attribute level. In Table 3.2, we show part-worths of each attribute level for both T1 and T2. Based on the part-worths, we then calculate monetary values associated with users' utility changes when an app switches from one level of an attribute to another level by following four steps: (1) calculating utility change of price level change from "$1.99" to "$0.00"; (2) calculating amount of utility change per dollar change; (3) calculating utility changes of level changes in other attributes; and (4) using the result from (2) to calculate dollar equivalents for level changes in other attributes. We show for each treatment the average values of utility changes associated with attribute level changes, as well as their dollar equivalents in the "Utility Change" column and the "Dollar Value" column in Table 3.3, respectively. Note here, for some responses, utilities associated with "$1.99" and "$0.0" are identical, indicating zero utility change associated with per-dollar change, which implies dollar equivalents for level changes in other attributes are not determinable. Therefore, as we mentioned in Section 3.1.3, we did not include such cases in our analysis.

From Table 3.3, we observe that under the scenario of social app adoption, individuals in T1 value their friends' "full profile" information at $1.01. Individuals in T2 value this information at $0.68. When it comes to users' *own privacy*, individuals in T1 and T2 value their own "full profile" information at $1.48 and $1.52, respectively.

Note here, when we refer to the economic valuations for friends' privacy, we mean the dollar value an individual places on the SNS profile information of *all* her friends. Since the value users place on the privacy of all their friends is less than the value of their own private information, social app users can be considered "privacy egoists." The observation that social app users only care a little (on average) about the privacy of each of their SNS friends can be partially explained given the previous

Table 3.2: Averaged part-worth utilities

Attributes	Attribute Levels	Part-worth Utilities	
		T1	T2
Price	\$0.00	1.78	1.80
	\$1.99	-1.78	-1.80
Network Popularity	5%	-0.56	-0.54
	25%	0.56	0.54
Own Privacy	None	0.66	0.72
	Basic profile	0.27	0.40
	Full profile	-0.93	-1.12
Friends' Privacy	None	0.46	0.31
	Basic profile	0.30	0.40
	Full profile	-0.76	-0.71

Table 3.3: Utility change and monetary value of change

Attributes	Level Change	Utility Change		Dollar Value		p-value
		T1	T2	T1	T2	
Price	\$0.00 ⇒ \$1.99	-3.56	-3.60	-1.99	-1.99	-
Network Popularity	5% ⇒ 25%	1.12	1.08	0.83	0.72	-
Own Privacy	None ⇒ Basic profile	-0.39	-0.32	-0.39	-0.30	0.26
	Basic profile ⇒ Full profile	-1.20	-1.52	-1.09	-1.22	0.28
	None ⇒ Full profile	-1.59	-1.84	-1.48	-1.52	0.46
Friends' Privacy	None ⇒ Basic profile	-0.16	0.09	-0.15	0.07	0.03
	Basic profile ⇒ Full profile	-1.06	-1.11	-0.86	-0.75	0.25
	None ⇒ Full profile	-1.22	-1.02	-1.01	-0.68	0.05

finding that most friendship ties are weak on SNSs [116].

In the next step, we examine whether there are treatment differences regarding the dollar values of *friends' privacy* and *own privacy*, i.e., we conduct one-tailed t-tests to investigate whether the app data collection context affects how individuals value privacy. We provide p-values of these tests in Table 3.3. Note here, we did not adjust p-values for the multiple testing problem since we consider our preliminary tests of the impact of collection context on privacy valuation as exploratory analysis, where multiplicity adjustments are neither mandatory, nor important [117].

From Table 3.3, we notice that the monetary values for *friends' privacy* level change from "none" to "basic profile" differ significantly between T1 and T2. We also find a borderline significant difference for the monetary values associated with *friends' privacy* level change from "none" to "full profile." However, we observe an insignificant treatment difference regarding the value of friends' sensitive information (associated with *friends' privacy* level change from "basic profile" to "full profile"). Our results suggest that an impact of data collection context on the valuation of interdependent privacy regarding app adoption is observable, but surprisingly weak. We consider this to be quite relevant for understanding the paradoxical outcome that while participants generally dislike unneeded data collection, field data shows that over-privileged apps are common [25, 118].

Complementing previous studies suggesting that privacy concern and privacy disclosure are influenced by contextual cues that are negatively related to objective dangers of disclosure [119], our findings suggest that contextual cues to some extent affect the valuation of privacy. In addition, we did not find any statistically significant differences for the valuations for *own privacy* between treatments. However, our treatment manipulation explicitly referred only to the information collected about users' friends, and seemingly did not cause any spillover effects regarding the valuation of a user's own personal information.

3.2 SEM to Investigate Associations between Privacy Value and Its Antecedents

Using conjoint analysis, we quantified the economic value users place on both their own information and their friends' information collected by social apps. We further investigated the impact of app data collection context. By applying SEM, we aim to position the conjoint study results in a broader context by asking what drives the valuation of personal and interdependent privacy. In particular, we aim to

investigate the roles of different dimensions of privacy concerns, their antecedents, as well as app data collection contexts for the valuations of users' own and their friends' information in app adoption scenarios.

Based on the existing literature, we first identify the factors that might affect a user's valuation of privacy. Next, we construct a SEM model to investigate associations between these identified factors and the measured privacy valuations. In addition, by adopting multiple group analysis [120], we are able to compare such associations among the different app data collection contexts.

3.2.1 Hypotheses and Research Model

When individuals reveal their personal information to other parties, they expect that a "social contract", which governs the behavior of those involved, is initiated [121]. One generally expected social contract is that these parties will be responsible for properly managing individuals' personal information [122]. These expectations relate to trust, which is the belief that these parties will behave in a socially responsible manner, and will fulfill the trusting party's expectations without taking advantage of any vulnerabilities [123, 124]. Prior research shows that when consumers think their personal information has been misused, they may consider this as an implied breach of contract [122, 125] and lower their trust assessment associated with the involved parties. In addition, in the electronic commerce context, it has been found that an online consumer's personal information being misused by a single online company could lead to the perception of information misuse by a larger group of online companies [126]. Further, individuals who have been victims of personal information abuse might be more aware of which actions could lead to privacy invasions [127] and what actions companies could take to misuse their information. Such awareness may further reduce their trust in online companies. Applying this to the context of our study, individuals who have privacy invasion experiences are less likely to trust other parties, including social apps,

when they handle their personal information. Therefore, we propose the following hypothesis:

Hypothesis 1: *Past privacy invasion experiences are negatively associated with individuals' trust in apps' data practices.*

In a study of online commerce, Hoffman et al. argued that trust creates positive attitudes toward Web retailers that are likely to reduce fears of retailer opportunism and attenuate infrastructure concerns [128]. Studies from other settings also argue that trust can enhance the evaluation of benefits and mitigate privacy concerns [129]. In fact, trust gives users a feeling that they will gain the benefits they expect without suffering negative consequences [129]. Applied to our context, we believe that consumers who have trust in apps' data practices would have less concerns when disclosing their own personal information to apps. Therefore, we hypothesize:

Hypothesis 2: *Trust in data practices is negatively associated with individuals' concerns for their own information privacy regarding app adoption.*

Previous studies indicate that being exposed to negative news reports regarding privacy, e.g., about the gathering and misusing of personal information, is a contributor to privacy concern [130]. Thereby, we argue that having more knowledge about privacy leads to higher concerns for both users' own and friends' privacy. Hence, we hypothesize:

Hypothesis 3: *Privacy knowledge is positively associated with individuals' concerns for their own information privacy regarding app adoption.*

Hypothesis 4: *Privacy knowledge is positively associated with individuals'*

concerns for their friends' information privacy regarding app adoption.

Previous research reported that along with computer-mediated interactions, individuals develop and maintain online social capital [131, 132]. Online social capital, which refers to immaterial resources accumulated through the relationships among people [10], often yields positive outcomes to individuals. For example, it provides emotional support for individuals [133, 134], it increases individuals' chances of exposure to diverse ideas [135], and it offers opportunities for individuals to get access to non-redundant information [136].

Putnam further classified online social capital into two categories: bridging social capital and bonding social capital [11]. These two types of social capital are not mutually exclusive and provide benefits to individuals from different perspectives [11]. According to Putnam, *bridging social capital* is created when individuals from different backgrounds connect in social networks. Although these individuals are merely acquaintances and such relationships are only tentative, bridging social capital helps them to broaden world views and opens up opportunities for information gathering or new resources [12]. In contrast, *bonding social capital* accumulates in close-knit relationships, such as families and between close friends. Such social capital provides strong emotional or substantive support for one another [12].

Through their interactions with online community members, social app users have likely developed some online social capital, both bridging and bonding social capital. In order to maintain these immaterial resources and continue to enjoy their benefits, app users would likely think twice before taking actions that are harmful to other community members. In this manner, we expect that both bridging social capital and bonding social capital motivate social app users to express concerns over their friends' privacy. Hence, we hypothesize:

Hypothesis 5: *Bridging social capital is positively associated with individuals'*

concerns for friends' information privacy regarding app adoption.

Hypothesis 6: *Bonding social capital is positively associated with individuals' concerns for friends' information privacy regarding app adoption.*

We also argue that individuals' concern for privacy is associated with their valuation for privacy. It is reasonable to assume that while keeping other factors constant, that more privacy concerned individuals exhibit higher privacy valuations. It follows that we hypothesize:

Hypothesis 7: *In app adoption scenarios, individuals' concerns for their own information privacy is positively associated with the perceived monetary value of their own information.*

Hypothesis 8: *In app adoption scenarios, individuals' concerns for their friends' information privacy is positively associated with the perceived monetary value regarding their friends' information.*

In social app adoption scenarios, the latter relationship is likely to be contingent on the context of app data collection. As discussed earlier, we introduced two treatments in the conjoint analysis survey, which manipulate the context of apps' practices of utilizing friends' information. From the analysis of the conjoint study results we know that knowledge about whether or not friends' data is relevant to an app's functionality affects how people value their friends' information. In addition, experimental studies provide substantial evidence of behavioral spillover [137, 138]. While the treatment conditions do not differ regarding the apps' practices of accessing the individuals' own personal information, we assume as a baseline hypothesis that the treatments also cause spillover effects on the relationship between own privacy concern and own privacy valuation. Therefore, we assume:

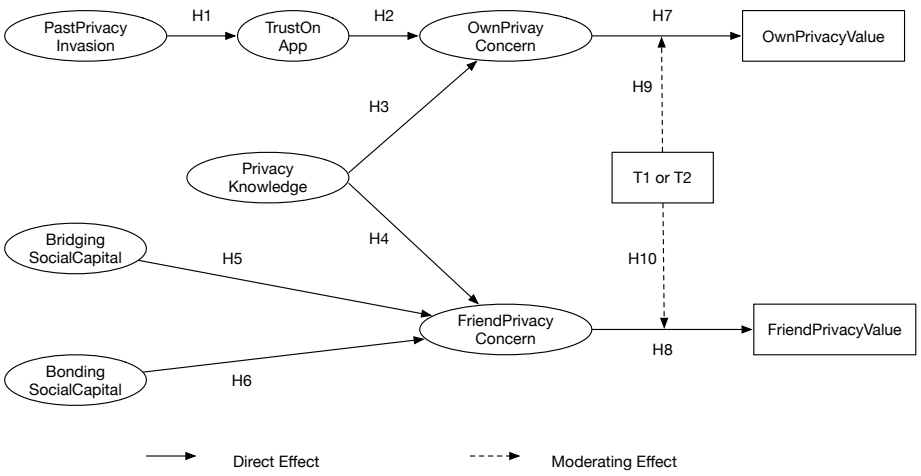

Figure 3.3: The conceptual model

Hypothesis 9: *In the context of app adoption, the association between concerns for individuals' own privacy and the valuation of their own information is variant across T1 and T2.*

Hypothesis 10: *In the context of app adoption, the association between concerns for friends' privacy and the valuation of friends' information is variant across T1 and T2.*

The research model, which is based on H1 $\sim$ H10, is presented in Figure 3.3. Paths that represent direct effects (specified by H1 $\sim$ H8) are paths for which the coefficients are estimated during the model fitting process. For those associations that represent moderating effects (specified by H9 and H10), we do not need to estimate their values. Instead, we only need to investigate the existence of such moderating effects.

Table 3.4: Evaluations of measurement model

(a) T1

	Cronbach's Alpha	Composite Reliability	Privacy Knowledge	Past Privacy Invasion	Trust OnApp	Own Privacy Concern	Friend Privacy Concern	Bridging Social Capital	Bonding Social Capital
PrivacyKnowledge	0.86	0.87	0.79						
PastPrivacyInvasion	0.75	0.75	-0.02	0.66					
TrustOnApp	0.86	0.86	-0.05	-0.34	0.78				
OwnPrivacyConcern	0.89	0.89	0.16	0.31	-0.59	0.82			
FriendPrivacyConcern	0.92	0.92	0.09	0.12	-0.03	0.22	0.86		
BridgingSocialCapital	0.79	0.79	-0.11	0.04	0.26	-0.25	0.06	0.66	
BondingSocialCapital	0.82	0.82	-0.05	0.26	0.24	-0.23	0.09	0.64	0.70

(b) T2

	Cronbach's Alpha	Composite Reliability	Privacy Knowledge	Past Privacy Invasion	Trust OnApp	Own Privacy Concern	Friend Privacy Concern	Bridging Social Capital	Bonding Social Capital
PrivacyKnowledge	0.83	0.84	0.75						
PastPrivacyInvasion	0.76	0.77	0.14	0.68					
TrustOnApp	0.85	0.85	-0.34	-0.35	0.77				
OwnPrivacyConcern	0.93	0.93	0.40	0.37	-0.45	0.87			
FriendPrivacyConcern	0.92	0.92	0.36	0.13	-0.13	0.36	0.87		
BridgingSocialCapital	0.78	0.78	0.00	-0.11	0.22	-0.05	0.06	0.65	
BondingSocialCapital	0.82	0.83	0.05	-0.20	0.13	0.01	0.03	0.51	0.71

3.2.2 Measurement Scale Development

Most of the survey measures collected are based upon or motivated by previously validated measurement scales which increases reliability. Past privacy invasion experiences were assessed based on four questions adapted from Smith et al. [70]. Note here, these items captured whether individuals subjectively perceive to have suffered from privacy invasions. We aimed to measure these experiences in a subjective way because we are interested in understanding how individuals' perceptions shape privacy concerns and valuations. The four items used to measure privacy knowledge were adopted from Park et al. [139]. To address the elements of trust in social apps, we used a shortened 4-item version of trust measures from Fogel and Nehmad [140], Krasnova and Veltri [141], and Dwyer et al. [142]. Corresponding to four questions to measure own privacy concern, which were modified from Smith et al. [70], we developed a similar set of four questions to assess individuals' concern for friends' privacy. With respect to online social capital, both bridging social

capital and bonding social capital were measured by five questions based on scales proposed by Williams [12]. Note that for the last five measurement scales, we slightly modified what appeared in the prior studies to fit the particular scenario studied here, i.e., social app adoption. All items were measured on a Likert-type scale with 1 = strongly disagree to 5 = strongly agree. Appendix A offers a detailed overview of the survey instruments. The valuations of both own privacy and friends' privacy are based on results of our conjoint analysis study.

One goal of our SEM model is to investigate whether the experimental treatments influence the association between privacy concern and privacy valuation in app adoption scenarios. Since our conjoint study results show that app data collection context significantly affects how individuals value their friends' full profile information, we limit our model to the study of the relationship between privacy concern and the value of full profile information. As such, we use the monetary valuation that is associated with the level change from "none" to "full profile" to represent own privacy valuation. Similarly, the value for friends' privacy is represented by the dollar value of the level change from "none" to friends' "full profile" information.

3.2.3 Empirical Results

We use AMOS 22.0, the standard model-fitting program, to test our SEM model which consists of a measurement model and a path model. The model is estimated by maximum likelihood (ML) estimation. ML is the default method in most SEM computer programs, and most SEMs in the literature were estimated by this method [143, 144]. In the following, we show the details for our tests of the measurement model and path model.

3.2.3.1 Evaluation of the Measurement Model

We evaluate the measurement model by examining the research instruments in terms of convergent validity and discriminant validity. Convergent validity measures the degree to which the measurement items are related to the construct they are supposed to predict [145]. In this study, two tests are used to determine the convergent validity of measured reflective constructs in a single instrument: Cronbach's alpha and composite reliability of constructs. Hair et al. [146] recommended an acceptance level of 0.7 for the composite reliability, and Nunnally [147] also proposed 0.7 as an indication of an adequate value for Cronbach's alpha. We show the test results in Table 3.4. In both treatments, Cronbach's alpha and composite reliability of all constructs exceed the suggested value of 0.7. These results support the convergent validity of our measurement model.

Discriminant validity evaluates the degree to which measures of different constructs are distinct from each other [148]. Following the criteria suggested by Fornell and Larcker [149], discriminant validity is examined: the square root of the variance shared between a construct and its measures should be greater than the correlations between the construct and any other construct in the model. Table 3.4 presents the correlations among constructs, with the square roots of variance on the diagonal. The correlations between each pair of constructs, i.e., non-diagonal elements, are less than the square roots of shared variance, i.e., diagonal elements, indicating our measurement model fulfills the requirement of discriminant validity.

3.2.3.2 Tests of Path Model

3.2.3.2.1 Tests of Model Fitness The goodness of overall model fit tests how significant the observed covariance structure differs from the covariance structure implied by the estimated model [150]. SEM relies on several statistical tests to determine the adequacy of model fit to the data. The chi-square test is a frequently reported goodness-of-fit criterion. A p-value associated with a chi-square test

Table 3.5: Results of path analysis

Hypotheses	Coefficient		Supported
	T1	T2	
H1: PastPrivacyInvasion→TrustOnApp	-0.34^{***}	-0.32^{***}	Yes
H2: TrustOnApp → OwnPrivacyConcern	-0.55^{***}	-0.45^{***}	Yes
H3: PrivacyKnowledge → OwnPrivacyConcern	0.17	0.55^{***}	Partially
H4: PrivacyKnowledge → FriendPrivacyConcern	0.12	0.69^{***}	Partially
H5: BridgingSocialCapital→FriendPrivacyConcern	0.05	0.10	No
H6: BondingSocialCapital→FriendPrivacyConcern	0.07	−0.02	No
H7: OwnPrivacyConcern → OwnPrivacyValue	0.83^{**}	0.54^{*}	Yes
H8: FriendPrivacyConcern → FriendPrivacyValue	0.49^{*}	0.38^{*}	Yes

* Significant at 5% level, ** Significant at 1% level, *** Significant at 0.1% level

exceeding 0.05 indicates the model is a good fit (i.e., significance might indicate a bad fit) [151]. Since the chi-square test is sensitive to sample size, other descriptive measures of fit are often used in addition to chi-square tests [152]. The Root Mean Square Error of Approximation (RMSEA) value, which ranges from 0 to 1, is also widely used to test model fit. Usually, acceptable model fits are indicated by an RMSEA value that is 0.06 or less [153]. The Comparative Fit Index (CFI) is another criterion of model fit with its value ranging from 0 to 1. Normally, a CFI value of 0.90 or greater indicates the model fit is acceptable [153]. In our study, we use the combination of chi-square test, RMSEA and CFI to test our model fit. The goodness of fit data of our model is $\chi^2(908) = 1358.40$, $p = 0.00; RMSEA = 0.04$; and $CFI = 0.90$. Although the chi-square value, which is sensitive to sample size, is significant, the other indices of practical fit, i.e., RMSEA and CFI, indicate that the fit of the model is acceptable.

3.2.3.2.2 Tests of Direct Effects We next test H1 $\sim$ H8. Our hypotheses should be tested based on the sign and statistical significance for its corresponding path in the path model. Further, the significance test is based on the ratio of each path estimate to its standard error, which is distributed as a z statistic [154]. We present the results in Table 3.5.

Our results indicate that in both treatments, past privacy invasion experiences

Table 3.6: Results of pair-wise parameter comparisons

Hypotheses	Coefficient		Critical ratio	Result
	T1	T2		
H7: OwnPrivacyConcern → OwnPrivacyValue	0.83	0.54	-0.71^{NS}	T1=T2
H8: FriendPrivacyConcern → FriendPrivacyValue	0.49	0.38	-0.38^{NS}	T1=T2

^{NS} Not significant at 5% level(one-tailed test)

are negatively and significantly associated with individuals' trust for app's proper handling of their personal information, which also has a significant and negative impact on concerns for their own personal information regarding app adoption (H1 & H2 are supported). Although the positive relationships between app users' privacy knowledge and both privacy concerns for own and friends' information are found to be significant in T2, such relationships are insignificant in T1 (H3 & H4 are partially supported in T2). We next evaluate the impact of online social capital. Bridging social capital as well as bonding social capital have a positive influence in both treatments on individuals' privacy concerns for their friends information, except for the influence of bonding social capital in T2. However, these relationships are not only weak (e.g., the highest absolute value of the coefficient is 0.10, the lowest is 0.02), but also insignificant. Therefore, H5 and H6 are not supported. In support of H7, the positive relationship between concerns for own privacy and how individuals value their own information in the context of app adoption is found to be significant in both treatments. Similarly, we find that in app adoption scenarios, individuals' concerns for friends' privacy are also significantly and positively related to the value individuals place on their friends' information in both T1 and T2 (H8 is supported).

3.2.3.2.3 Tests of Moderating Effects In this section, we aim to test hypotheses H9 and H10. In other words, we test whether the proposed impact of concerns for privacy on privacy valuations differs when information is accessed under different app data collection contexts. We first introduce the method that is

applied to test treatment differences.

SEM analysis examining hypotheses about potential group differences is commonly referred to as *multiple group analysis, multisample modeling* or *tests of model invariance* [120, 155]. This analysis starts with fitting a research model to the data for each group separately with none of the paths constrained to be equal across groups. Such an unconstrained model serves as the baseline model. Next, the model is estimated by constraining all the paths to be equal across groups [156]. The constrained model can be seen as a nested model of the baseline model. In order to determine whether or not the model is invariant across groups, the model is examined using a chi-square difference test between the baseline model and the constrained model. A statistically significant difference in χ^2 is consistent with model variances, which rejects the null hypothesis that the path values are equal across groups. If the χ^2 differences are insignificant, the parameters examined are equal across groups [157].

Once the chi-square test for the unconstrained model and constrained model is found to be statistically significant, pairwise parameter comparison is usually applied to determine whether a certain path is invariant across different treatments [158]. Critical ratios for differences between parameters, which are calculated by dividing the difference between the parameter estimates by an estimate of the standard error of the difference, are used in the pairwise parameter comparison test. The critical ratio is usually assumed to follow a standard normal distribution [158]. The critical ratio that is associated with a significant p-value demonstrates that the corresponding path is variant among the groups under examination. If the critical ratio corresponds to a p-value that is insignificant, the path of interest is the same among groups under consideration.

Using AMOS 22.0, we first apply *multiple group analysis* to test whether our model is the same across the two experimental treatments. If multiple group analysis shows that our model differs across treatments, we adopt pairwise parameter

comparisons to determine whether the paths indicated by H7 and H8 are variant across treatments. By applying both of these two methods, we are able to test H9 and H10.

Following the steps of *multiple group analysis*, we first recall the chi-square goodness of fit of the baseline model which we know from the previous section ($\chi^2(908) = 1358.40$). Next, we constrain all paths to be equal across all treatment groups. This fully constrained model has $\chi^2(982) = 1455.59$. Comparing the fully constrained model with the baseline model, we determine $\Delta\chi^2(74) = 97.19$, and $p = 0.04$. The result indicates our model differs across T1 and T2, and we therefore investigate the different paths for the treatment groups by conducting pairwise comparisons.

Since we are particularly interested in the difference of association between privacy concerns and privacy valuations among treatment groups, we conduct pairwise parameter comparisons on paths that are indicated by H7 and H8; the results are summarized in Table 3.6. We find that when it comes to individuals' own privacy regarding app adoption, although the coefficient of the relationship between concerns for such privacy and its monetary valuation in T1 is higher than the one in T2, this difference is not significant ($p = 0.24$). This indicates that our treatments do not moderate the relationship between concern for own privacy and valuation for own privacy in a substantial fashion. Therefore, H9 is unsupported.

Similarly, we observe that the regression coefficient for the relationship between concern for friends' privacy and valuation of friends' privacy is higher in T1 than it is in T2, indicating in the context of app adoption, that concerns for friends' privacy have a more salient effect on how individuals value their friends' privacy for participants in T1 than for their counterparts in T2. This is reasonable given T1 represents the case where the information collected about friends is not useful to the app's functionality, while T2 indicates otherwise. However, the treatment difference is not significant ($p = 0.35$). Accordingly, the hypothesis that in app adoption

scenarios the association between concern for friends' privacy and valuation for friends' information is variant (H10) is not supported.

3.2.4 Discussion of SEM Model

Conducting a SEM analysis, we aimed to investigate what factors, as well as how these factors, affect individuals' valuation of privacy in social app adoption scenarios. In addition, we also wanted to learn whether app data collection contexts influence the association between privacy concerns and privacy valuation. More specifically, we constructed a conceptual model that captures the role of personal privacy experiences, privacy preferences and online social capital, as well as data collection contexts and the impact of these measures on individuals' valuation of privacy regarding app adoption.

Our model suggests that individuals' trust in apps' proper handling of personal information mediates the relationship between individuals' past privacy invasion experiences and their concern for own privacy. This means that having suffered from unpleasant and potentially costly consequences of privacy invasions, individuals are less likely to trust other parties, such as social apps, to deal with their information in a responsible manner. As such, their own privacy concerns tend to increase when asked to reveal their personal information to apps.

Further, our results confirm the positive impact of concern for individuals' own privacy on individuals' valuation of own privacy in app adoption scenarios. A similar positive relationship also applies to friends' privacy, which is evident from our empirical results. This implies that privacy concerns are critical factors that shape and influence a user's economic valuation of her own personal information and friends' personal information. Given that such information is increasingly used as an economic good by marketers, it is important that individuals recognize the monetary value of personal information as well.

Although the empirical results provide support for the general applicability

of the research model, they also reveal a few unexpected relationships that are inconsistent with what we had hypothesized. Specifically, the proposed positive associations between privacy knowledge and concern for both own privacy and friends' privacy regarding app adoption are only partially confirmed in T2. One possible explanation involves the potential relationship between privacy knowledge, which in our study measures individuals' knowledge of data collection risks, and awareness of regulatory protection. In other words, we believe individuals who have higher levels of privacy knowledge are more likely to be aware of how and to which extent their privacy is protected by laws and other regulations. Since individuals have different attitudes towards the effectiveness of regulatory protection, it is possible that among those who have moderate level of privacy knowledge, some might believe privacy laws ensure adequate accountability while others consider the current regulatory framework to be insufficient to protect privacy.

As to the insignificant impact of bridging social capital and bonding social capital on concerns for both own and friends' privacy, a possible explanation is the typically large number of friends users accumulate on SNSs. Drawing on previous research, users have on average over 300 friends on SNSs [28]. Since each friend has the possibility to adopt apps with interdependent privacy harms, it is difficult to detect which individual has performed such a harmful action (in absence of tools provided by the SNS). Even upon detection, the perceived responsibility and experienced guilt may be low as the impact is diffused among all friends who have also installed such apps. Further, many app users may even be unaware of the existence of interdependent privacy (i.e., they are not aware of the fact that their information can be leaked by others' actions). Therefore, a user might believe that installing apps with interdependent privacy harm will not have a negative impact on either their personal relationships on an SNS or their online social capital. As such, individuals' level of social capital might not affect their concern for friends' privacy in app adoption scenarios.

Note that none of these three constructs (i.e., privacy knowledge, bridging social capital and bonding social capital) are significantly related to concern for friends' privacy regarding app adoption. Therefore, we believe additional research should be proposed to investigate the antecedents of friends' privacy concern in social app adoption scenarios.

As to the treatment differences in terms of association between concern for privacy and value of privacy, we find no evidence to support such an association. This demonstrates that our experimental treatments, which only differ in app data collection contexts regarding friends' information, have no spillover effects on the concern or valuation of a user's own information.

Although the coefficient of the association between concern and value of friends' privacy is higher in T1 than in T2, this difference is not significant. In other words, our treatments do not moderate the influence of concern for friends' privacy on the value of friends' privacy regarding app adoption. Since we observe a significant impact of the treatments on the valuation of friends' privacy (in the conjoint study), we believe that there are likely other factors, which also contribute to the valuation of interdependent privacy in the context of app adoption, that we did not integrate into our model. It is possible that such missing factors moderate how individuals value their friends' information. This motivates additional future work to more thoroughly understand the formation of interdependent privacy valuations in app adoption scenarios.

3.3 Summary

Our work is one of the first attempts to investigate the problem space of interdependent privacy from the quantitative-behavioral and empirical perspectives. By utilizing the results from a full-profile conjoint study, we quantify the economic value individuals place on both their own and friends' information in social app

adoption scenarios. Next, we construct a SEM model to explore how specific factors, namely past privacy invasion experiences, privacy knowledge, trust in apps' data practices, bridging social capital, bonding social capital, as well as privacy concerns, impact the process of privacy valuation in the context of app adoption. In addition, motivated by principles of contextual integrity [106], we examine the effect of app data collection context on privacy valuation, as well as its impact on the relationship between privacy concerns and privacy valuations by introducing two treatments into our study: (T1) friends' personal information cannot improve an app's functionality, and (T2) friends' personal information can improve an app's functionality.

Based on the conjoint study, we find that monetary valuations of interdependent privacy regarding app adoption are significantly higher in treatment T1 than T2, and differ in particular with respect to friends' basic information and friends' full profile information. These findings motivate us to also investigate the impact of treatments in the SEM model. As an exploratory study, our SEM model confirms a part of the hypothesized associations between our proposed factors and privacy valuations. Individuals' past privacy invasion experiences are negatively related to trust in apps' proper data practices, which in turn negatively impacts users' concerns for their own privacy. Although, privacy knowledge is found to be positively and significantly related to individuals' concerns for their own and friends' privacy in T2, such associations are not supported in T1. Surprisingly, bridging social capital and bonding social capital do both not significantly impact how individuals care about others' privacy regarding app adoption. Further, although the associations between concern for privacy and valuation for privacy are found to be significant in terms of both own privacy and friends' privacy, these relationships are not affected by variations of apps' data collection context.

Chapter 4

Study 2: Interdependent Privacy Value in Social App Adoption Contexts: Its Associations with Social Capital, Data Collection Context, and Number of Friends

In the last chapter, we described a study that quantifies and explains the value of interdependent privacy in the social app adoption scenario. However, as an exploratory study to explain users' interdependent privacy valuation, this study suffers from several limitations. Although integrated into the SEM model, factors such as social capital and data collection context are only partially examined in that study. For one thing, the relationship between social capital and interdependent privacy value is only indirectly examined through the mediation of privacy concern. For another, the only factor the study explores that interacts with app data collection context is a person's privacy concerns. However, as indicated by the

study itself, other factors that might have interactions with app data collection context are missing in the model. Therefore, additional studies are needed to more thoroughly understand the influence of data collection context and social capital on interdependent privacy valuation. To this end, in this chapter, we present a study that aims to better explain the valuation of interdependent privacy in contexts of social app adoption by not only conducting a more thorough exploration of the factors discussed in Study 1, but also taking into consideration additional factors.

In addition, the complex and yet still empirically undetermined relationship between social capital and interdependent privacy [159] is another key motivator for the work in the chapter. There are two contradictory theories regarding this relationship. On the one hand, considering the prior research finding that individuals' social capital perceptions are positively related to their disclosure behaviors [159, 160], app users who have a higher level of social capital are more willing to release information *about themselves*. However, it remains unknown as to which degree users are likely to accrue social capital through the sharing of *others' information*. In particular, we believe there is a spill-over effect such that when individuals are more open to share their own information, they are also more likely to engage in disclosure behaviors about their friends' information. As such, individuals with a higher level of social capital tend to value interdependent privacy less. On the other hand, social capital, which is accumulated through interactions with others [10], is regarded as an immaterial resource individuals gain benefits from [12, 133–135]. In order to maintain such immaterial resources, one would likely carefully evaluate actions that might harm others. From this perspective, the higher the level of social capital individuals have, the more value they place on friends' information. These two points of view are contradictory to each other, and hence motivate us to empirically investigate how social capital influences the value of interdependent privacy in the context of social app adoption.

To address these research goals, we conduct a series of regression analyses

on data obtained from an online survey study. More specifically, by performing regression analysis on responses to carefully designed survey measures, our study contributes to a better understanding of how, in a social app adoption scenario, interdependent privacy value is related to factors such as social capital, app data collection context, number of friends, concern for friends' privacy, and demographics.

This chapter is structured as follows. In Section 4.1, we provide some background on social capital. In Section 4.2, we develop and formalize our research question. In Section 4.3 and Section 4.4, we offer survey study details, and provide data descriptions, respectively. In Section 4.5, we present results of regression analyses. Finally, we discuss our results in Section 4.6 and summarize in Section 4.7.

4.1 Background on Social Capital

Broadly speaking, social capital is the resource accumulated through individuals' interactions with others [10]. It always links to a variety of positive social outcomes, such as emotional support [133, 134], chances of exposure to diverse ideas [12], and opportunities to get access to non-redundant information [135]. In addition, social capital increases individuals' commitments to a community and enhance their abilities to mobilize collection actions [136], and hence influences a wide range of significant economic and political phenomena [161].

Putnam further classifies social capital into two categories: bridging social capital and bonding social capital [11]. These two types of social capital are not mutually exclusive and provide benefits to individuals from different perspectives [11]. Bridging social capital is linked to"weak ties", which refers to the loose connections between individuals from different backgrounds [162]. Although these individuals are merely acquaintances and such relationships are only tentative, bridging social capital helps them to broaden world views and opens up opportunities for information gathering or new resources [12]. In contrast, bonding social capital

often derives from "strong ties", which are close-knit relationships between family members and close friends [163]. Prior research indicates that bonding social capital is associated with trust and reciprocity, and provides strong emotional or substantive support for one another [11, 12].

The emergence of SNSs provides individuals with many new ways to interact with a wide variety of others, ranging from close contacts to strangers [12, 164]. For example, it changes not only the costs of communication, but also the number and the character of individuals one keeps in touch with [165]. Given that, researchers have recently begun to investigate how engaging with SNSs influences one's ability to form and maintain social capital. A stream of research in the past half decade provides strong empirical support for the positive relationship between the use of SNSs and accumulation of social capital [163, 166, 167]. Even after controlling for factors such as demographics and psychological well-being, Ellison et al. [163] find students who have a more intense use of Facebook maintain a greater level of social capital. In a longitudinal study, Steinfield et al. [166] prove a causal effect of SNSs use on bridging social capital accumulation. Within an organizational setting, Steinfield et al. [167] also detect that the use of Beehive, an internal SNS in IBM, results in growth of both bonding and bridging social capital.

In contrast with studies that treat SNSs use as a monolithic activity, some others examine how SNSs affect social capital depending upon different types of SNS use. For example, by differentiating uses of SNS, Ellison et al. [168] find not all usage of Facebook results in social capital growth. Rather, students who are motivated by "social information-seeking", i.e. using SNSs to learn more about people with whom they have some form of offline connections, report higher level of social capital. Using a sample of U.S. adult Facebook users, Burke et al. [169] show that directed communication is associated with a higher level of social capital, while consuming greater levels of content actually reduces social capital perceptions. In addition, a study from Burke et al. [165] reveals only activities that involve

receiving messages from friends result in bridging social capital growth.

While the role of SNS use on social capital accumulation has been investigated in a number of studies, only a few academic works explore how privacy is related to social capital. Particularly, Ellison et al. [159] argue that in order to accumulate social capital from interactions within SNSs, one must be willing to disclose information about the self. They further reveal that the use of segmented privacy settings on Facebook, i.e. limiting specific content to groups within one's network, is positively associated with the level of social capital individuals have [159]. Extending [159]'s work, Stutzman et al. [160] demonstrate that the relationship between privacy concern and social capital is mediated by one's willingness to disclose on SNSs.

However, these studies investigate how disclosure behaviors and privacy concerns influence social capital outcomes, but not the other way around. To address this literature gap, our studies examine whether and how social capital can be used to predict privacy valuation. In particular, applied to our context of interest, we aim to uncover the impact of social capital on the value app users place on their friends' information.

4.2 Research Question

Social capital and privacy have a complex relationship [159]. When it comes to interdependent privacy, its relationship with social capital adds an additional layer of complexity. On the one hand, previous research indicates disclosure behaviors are positively related to social capital perceptions [159, 160]. In other words, the more information one releases online, the more likely he/she is going to accumulate social capital. Applied to our context of interest, app users who have a higher level of social capital might be more open to disclose information *about themselves*. However, it remains unknown as to which degree users are likely to accrue social capital through the sharing of *others' information*. In particular, we believe there

is a spill-over effect such that when individuals are more open to share their own information, they are also more likely to engage in disclosure behaviors about their friends' information. As such, app users with a higher level of social capital are more likely to value their friends' privacy less. On the other hand, social capital, which is accumulated through interactions within communities, is an immaterial resource from which individuals gain benefits such as emotional support [133, 134], opportunities of exposure to diverse ideas [12], and chances of accessing non-redundant information [135]. In order to maintain such immaterial resources and continue to enjoy their benefits, individuals, including app users in our context, would likely think twice before taking actions that are harmful to other community members. In this manner, the higher the level of social capital app users have, the less likely they are going to reveal their friends' information to apps, thus more monetary value they place on friends' privacy. These two contradictory perspectives of view make us rethink what actual role social capital, both bridging and bonding social capital, plays in the valuation process of interdependent privacy.

Prior research reveals that individuals' privacy concerns are influenced by conditions as to whether or not information requests are context-relevant [170]. For example, Wang et al. [171] find users are typically unconcerned about giving away their friends' birthday information to a birthday app, but become uncomfortable when that app also tries to get access to information unrelated to its stated purpose. Therefore, in our study, we also examine how app data collect context impacts the value social app users place on their friends' information.

When we refer to the interdependent privacy *value*, we refer to the dollar values an app user places on the profile information of all his/her friends within SNSs. Considering different app users have a different number of friends on SNSs, we are interested in investigating the impact of the number of friends on interdependent privacy valuation. Further, previous research reveals individuals' privacy concerns are significantly associated with privacy values [172]. To confirm this finding, our

study also examines this relationship. In addition, we are also curious about how interdependent privacy value differs across demographic information. Specifically, we want to understand how factors such as app users' gender, age, education level, and income level impact the dollar values they place on friends' information.

Finally, besides studying the main effects of the above mentioned factors, we are also interested in whether these factors interact in complex ways with each other when predicting the value of interdependent privacy.

To sum up, in order to better explain the valuation process of interdependent privacy in app adoption contexts, our study empirically addresses the following research question:

***RQ**:What roles do bridging and bonding social capital, app data collection context, number of friends within SNSs, concern for friends' privacy, demographics, as well as their interactions play in app users' valuation of interdependent privacy in the scenario of social app adoption?*

4.3 Method

To address our research question, we conducted an online survey study with a population of social app users to measure three dimensions of information: (1) participants' basic demographics and their number of friends on SNSs, (2) participants' value of interdependent privacy, and (3) participants' perceptions of social capital within SNSs and privacy concerns towards their friends' privacy. Therefore, our survey consisted of three parts, with each part measuring one of these three information dimensions.

In the first part, we collected participants' demographic information such as gender, age, education level, as well as income level. In addition, we also asked participants to report the number of friends they have on their primary SNS.

The second part in our survey was designed to elicit the value participants place on their friends' information. In this part, we apply the same method that is used to quantify the value of interdependent privacy in our Study 1 (See details in Section 3.1). That is, we randomly placed participants in one of the two treatment scenarios and asked them to rank 9 app versions that differ in four app features, including the information an app collects about users' friends. We then quantify the value participants place on their friends' information based on their rankings of the different app versions.

Our last part of the survey included items that measure participants' perceptions of social capital, as well as concerns for interdependent privacy. To the extent possible, most of these items are based upon or motivated by previously validated instruments in order to increase reliability. With respect to social capital, both bridging social capital and bonding social capital were measured by five questions based on scales proposed by [12]. Adapting from 4 items in [70] that measure own privacy concern, a similar set of questions was developed to assess individuals' concerns for friends' privacy. In addition, for all of these measures, we slightly modified what appeared in the prior studies to fit the particular scenario studied here, i.e., social app adoption. All items were measured on a Likert-type scale with 1 = strongly disagree to 5 = strongly agree.

Our survey study was implemented by utilizing a combination of Qualtrics, an online survey software, and Amazon Mechanical Turk (MTurk), a recruitment source that is very popular for conducting online user experiments [115]. Specifically, we constructed the survey questions on Qualtrics, and then recruited participants from MTurk to access the Qualtrics link for our survey. We paid $1.00 to each participant after completing all three parts of the survey.

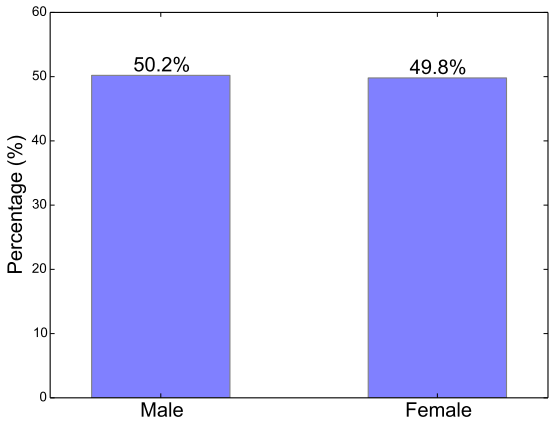

Figure 4.1: Gender distribution

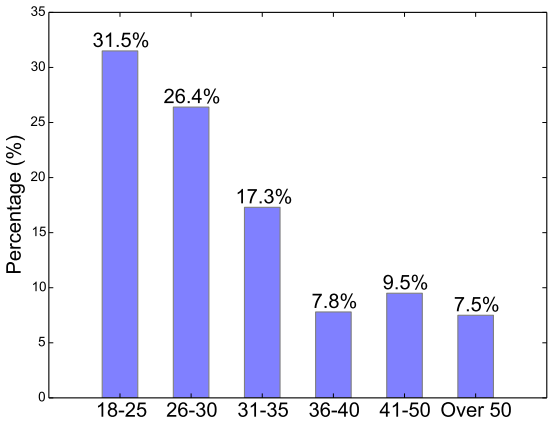

Figure 4.2: Age distribution

4.4 Data Description

Data collection was conducted in June 2015. In terms of data analysis, we first filtered out low quality responses by utilizing a screening task and several check conditions [172]. Our final sample included responses of 295 participants for data analysis. We next describe our sample data.

4.4.1 Demographics and Number of Friends

We first present basic demographic characteristics of our sample. Figure 4.1 shows the gender distribution is 50.2% male and 49.8% female, indicating we have a balanced sample in terms of gender.

We next show the age range of our participants in Figure 4.2. According to Figure 4.2, our sample covers a wide range of age categories, from 18 to over 50. In particular, with a median age range of 26-30 years, younger participants are slightly over-represented in our sample. This is in line with the fact that SNS users are generally younger [167], suggesting our sample is a good representation of the overall SNS user base.

Our sample also covers diverse education levels, ranging from less than high

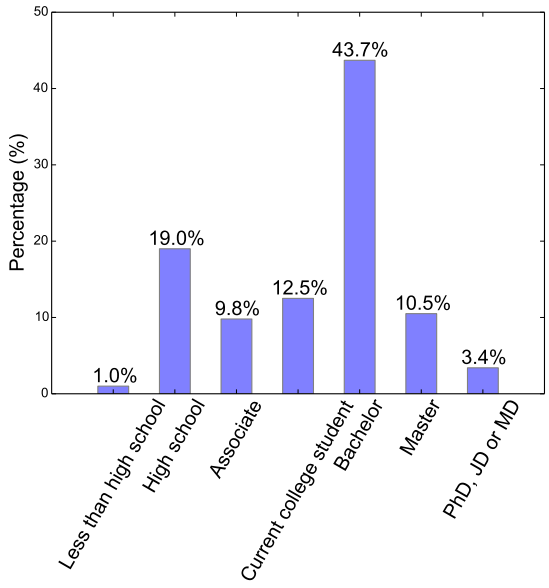

Figure 4.3: Education level distribution

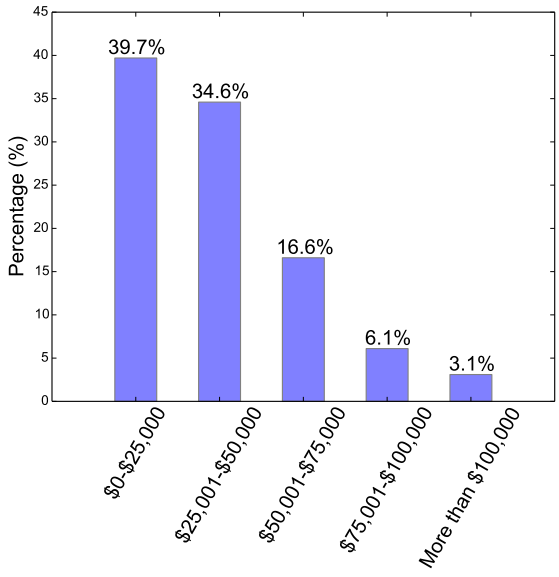

Figure 4.4: Income level distribution

school to higher education degrees such as PhD (See Figure 4.3). Among them, nearly half (43.7%) maintain a bachelor degree as their highest education level.

In terms of income level (see Figure 4.4), only a few of our participants earn a salary of more than $100,000. Rather, most of them (74.2%) have a yearly income of less than $50,000.

In addition, we show the distribution of the number of friends participants have on their primary SNS in Figure 4.5. A majority of our participants have over 100 friends. Most of them fall into the category of having 201-500 friends. This matches with published data that users have on average over 300 friends on SNSs [28], which is another indication that our sample represents SNS user populations reasonably well.

4.4.2 Interdependent Privacy Value

As discussed in the previous sections, we conducted a conjoint analysis study to quantify the value of interdependent privacy. We further introduced two treatments in order to examine the effect of app data collection context on interdependent

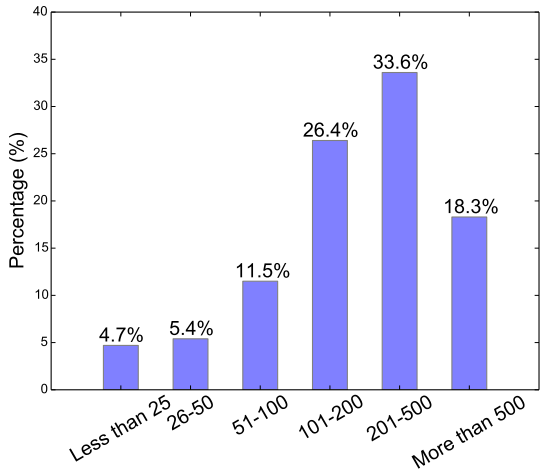

Figure 4.5: Number of friends distribution

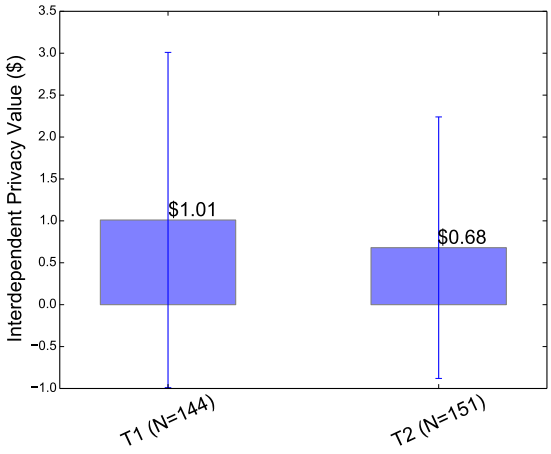

Figure 4.6: Value of interdependent privacy

privacy valuation.

Among the 295 participants whose responses are used for data analysis, 144 were assigned to T1 and 151 were assigned to T2. Following the methodology of conjoint analysis (see details in Section 3.1), we calculated the interdependent privacy value in each treatment and show here results in Figure 4.6 [1]. From Figure 4.6, we notice that on average, participants in T1 value their friends information at \$1.01 ($SD = 2.00$), which is slightly larger than the monetary value, \$0.68 ($SD = 1.56$), their counterparts in T2 place on friends' privacy. This shows the possible influence of app data collection context on privacy valuation.

4.4.3 Measurement Value

We next discuss the measured values of bridging social capital, bonding social capital, as well as interdependent privacy concern.

[1]The interdependent privacy value here corresponds to the dollar values of friends' full profile information that are shown in Table 3.3.

Table 4.1: Summary statistics for bridging social capital

Individual Items and Scale	Mean	S.D.
Bridging social capital (Cronbach's alpha = 0.78)	**3.57**	**0.66**
Interacting with my online social network friends makes me want to try new things	3.49	0.81
Interacting with my online social network friends makes me feel like part of a larger community	3.79	0.87
Interacting with my online social network friends reminds me that everyone in the world is connected	3.97	0.86
I am willing to spend time to support general online social network community activities	3.46	0.91
On my online social network sites, I come in contact with new people all the time	3.12	1.06

Note: Individual items range from 1 = strongly disagree to 5 = strongly agree, scale is constructed by taking the mean of items

4.4.3.1 Bridging Social Capital

Bridging social capital measures the degree to which individuals are viewing themselves as a member of a broader group, and are feeling themselves to interact with a diverse set of people [167]. Adapting from [12], we grouped 5 items as shown in Table 4.1 to create a scale that measures app users' level of bridging social capital within SNSs. According to Table 4.1, this scale exhibits a high reliability (Cronbach's alpha = 0.78).

4.4.3.2 Bonding Social Capital

Bonding social capital captures one's access to emotional support and limited resources, as well as one's ability to mobilize solidarity [167]. We assess bonding social capital using five items adopted from [12], and show the items in Table 4.2.

Table 4.2: Summary statistics for bonding social capital

Individual Items and Scale	Mean	S.D.
Bonding social capital (Cronbach's alpha = 0.82)	**3.07**	**0.87**
There are several online social network friends I trust to help solve my problems	3.29	1.11
There are some online social network friends that I can turn to for advice about making very important decisions	3.43	1.10
If I need an emergency loan of $500, I know that I can turn to some of my online social network friends for help	2.35	1.20
My online social network friends would be good job references for me	3.04	1.15
I do not know my online social network friends well enough to get them to do anything important (reverse code)	3.27	1.11

Note: Individual items range from 1 = strongly disagree to 5 = strongly agree, scale is constructed by taking the mean of items

The high value of Cronbach's alpha, which is 0.82, indicates a high reliability of this scale.

4.4.3.3 Interdependent Privacy Concern

The scale of concern for interdependent privacy, which is adapted from 4 items in [70], also has high reliability (Cronbach's alpha = 0.92). Items used to assess interdependent privacy concern as well as their description data are shown in Table 4.3.

Table 4.3: Summary statistics for interdependent privacy concern

Individual Items and Scale	Mean	S.D.
Interdependent privacy concern (Cronbach's alpha = 0.92)	**4.37**	**0.72**
It usually bothers me when third-party app developers ask me for my friends' personal information	4.36	0.79
When third-party app developers ask me for my friends' personal information, I sometimes think twice before providing it	4.47	0.76
It bothers me to give my friends' personal information to so many third-party app developers	4.42	0.76
I'm concerned that third-party app developers are collecting too much personal information about my friends	4.22	0.86

Note: Individual items range from 1 = strongly disagree to 5 = strongly agree, scale is constructed by taking the mean of items

4.5 Results

In order to investigate the research question as to how the measured factors affect the value of interdependent privacy in social app adoption scenarios, we conduct a series of regression analyses. Specifically, our goal is to examine associations between the interdependent privacy value and factors such as bridging social capital, bonding social capital, app data collection context (treatments), number of friends on primary SNS, concern for interdependent privacy, and demographics. Therefore, we treat the value of interdependent privacy as the dependent variable, and the remaining factors as independent variables. In contrast with treating gender and treatment as categorical variables, we consider age, income level, education level, number of friends, privacy concern, bridging and bonding social capital as continuous variables since they are either ordinal or continuous.

Table 4.4: Regressions explaining value of interdependent privacy

Independent Variables	Coefficients	
	Model 1	Model 2
Intercept	-1.47	-1.00
Gender:		
–Male	-0.50**	-0.48**
–Female	0.50**	0.48**
Age	0.20***	0.20***
Education level	-0.01	-0.01
Income level	0.04	0.06
Number of friends	0.27**	0.30***
Treatment:		
–T1	-1.32*	-0.15
–T2	1.32*	0.15
Bridging social capital	-0.02	0.002
Bonding social capital	-0.24*	-0.47***
Interdependent privacy concern	0.30**	0.30**
Number of friends × treatment:		
–Number of friends × T1	0.39**	0.42***
–Number of friends × T2	-0.39**	-0.42***
Bonding social capital × treatment:		
–Bonding social capital × T1	–	-0.42*
–Bonding social capital × T2	–	0.42*
$N = 295$	$R^2 = 0.12$	$R^2 = 0.13$
	$F = 4.03^{***}$	$F = 3.99^{***}$

$^{*}p < 0.1$, $^{**}p < 0.05$, $^{***}p < 0.01$

$^{-}$ Variable not included in regression model

Besides studying main effects of each independent variable, we also explore the possible interactions between these variables. Therefore, in the following sections, we present two regression models, i.e. Model 1 and Model 2, with each model introducing a new interaction term. (We also test other interactions, but we do not discuss them here since they are not significant.) Results of both regression models are displayed in Table 4.4.

4.5.1 Model 1

For Model 1, besides all independent variables, the interaction between number of friends and treatment is examined.

We notice from Table 4.4 that as to the effects of demographic factors in Model 1, female participants value friends' information higher than male ($p < 0.05$); and older individuals are more likely to express a higher interdependent privacy valuation than younger ones ($p < 0.01$). However, neither education level nor income level is significantly related to the value of friends' information.

When it comes to main effects of social capital, we find both bridging and bonding social capital have negative effects on privacy valuation, indicating that the higher the level of social capital app users have, the more likely they share their friends' data to apps. However, only the impact of bonding social capital is significant ($p < 0.1$). The influence of bridging social capital on interdependent privacy valuation is not only small, i.e. $\beta = 0.20$, but also insignificant.

In addition, we also detect that interdependent privacy concern is positively and significantly associated with the value of interdependent privacy ($p < 0.05$), which is in line with the finding in [172].

For treatment and number of friends, we not only observe a significant main effect for each of them ($p < 0.1$ and $p < 0.05$, respectively), but also detect a significant interaction between them ($p < 0.05$). In other words, we find number of friends has a significantly different impact on interdependent privacy value in T1 vs. T2. To better illustrate this interaction, we plot its effect in Figure 4.7, where a larger value on the horizontal line indicates a higher number of friends an individual has. We notice that for individuals in T2 , where friends' data is irrelevant for apps' functionality, the more friends participants have, the higher the value they put on interdependent privacy. Surprisingly, in case of relevant data collection, social app users with a larger number of friends on SNSs tend to value the privacy of all their friends less.

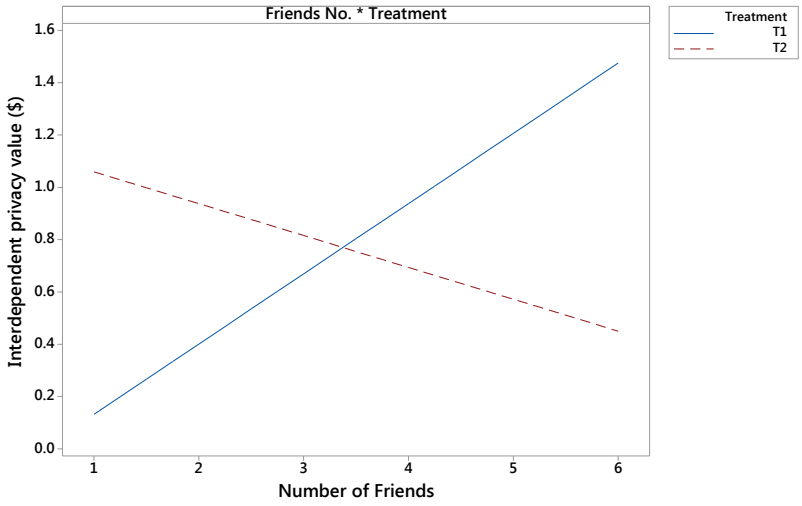

Figure 4.7: Interaction of number of friends and treatment on interdependent privacy value

4.5.2 Model 2

The significant association between bonding social capital and interdependent privacy valuation motivates us to further explore whether bonding social capital interacts in important ways with data collection context. To this end, we extend Model 1 to account for another interaction term, that is the interaction between bonding social capital and treatment. We refer to the extended model as Model 2, and we present its regression results in Table 4.4.

Compared with results in Model 1, significances of all variables except treatment remain the same when the new interaction term is included. Since the newly introduced interaction term involves treatment, we are not surprised at the change of significance associated with the treatment main effect. In terms of the direction of impact, only that of bridging social capital changes from negative to positive. Since the influence of bridging social capital on interdependent privacy value is small and not significant, we believe its direction to be influenced by chance.

As expected, the interaction between bonding social capital and treatment is significant ($p < 0.1$), indicating the relationship between bonding social capital and

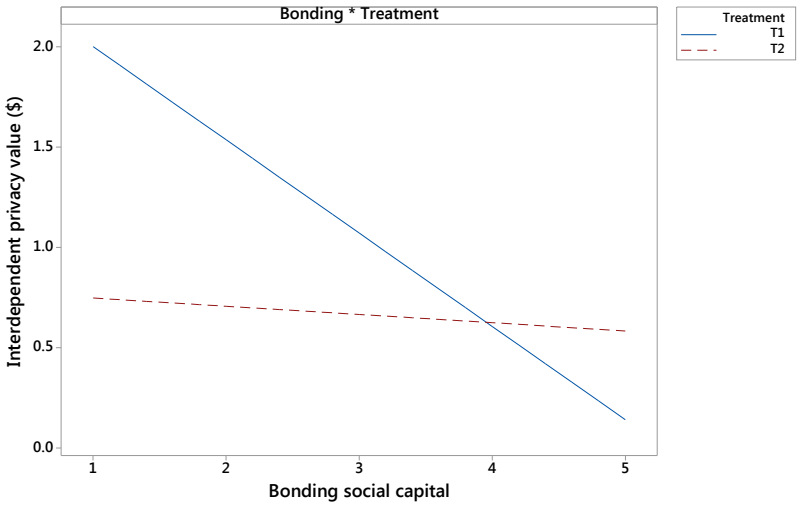

Figure 4.8: Interaction of bonding social capital and treatment on interdependent privacy value

interdependent privacy value varies based with app data collection context. We show the interaction effect in Figure 4.8. From Figure 4.8, we observe that although in both treatments, interdependent privacy value decreases with an increase of bonding social capital, the value changes more quickly in T1 than in T2. In other words, although in both treatments, social app users with a higher level of bonding social capital value their friends' information less than those with relative lower perceptions of bonding social capital, such difference is larger in T1 than it is in T2.

4.6 Discussion

Returning to our original research question, our regression analysis first helps to uncover the relationship between bonding social capital and interdependent privacy value in social app adoption contexts. Specifically, we find that the value social app users put on friends' data is reversely related to their perceptions of bonding social capital. Recall the two contradictory views, we have mentioned previously, regarding the association between interdependent privacy value and social capital.

Our finding partly supports the view that individuals with a high level of social capital, however in our case only the bonding social capital, express a lower value of interdependent privacy in that they are likely more used to and are more willing to engage in disclosure behaviors. As to the other view that individuals are reluctant to reveal information about others in order to maintain and protect social capital, we believe such reluctance either does not exist or is outweighed by individuals' eagerness to grow bonding social capital through information disclosure behaviors.

Besides the significance of its main effect, bonding social capital also significantly interacts with treatment, i.e. app data collection context. Specifically, the difference as to the value of interdependent privacy between people with a high level of bonding social capital and others is larger in T1 (irrelevant data collection) than in T2 (relevant data collection). One possible explanation of this phenomenon is that compared with app users with a high level of bonding social capital, the willingness to disclose friends' data by those with low bonding social capital perceptions is more sensitive to app data collection context. In particular, although individuals with a low level of bonding social capital are reluctant to disclose friends' data under the situation where such information is not useful to apps' functionalities, they nevertheless become willing to reveal friends' data to apps when they believe such disclosure behaviors improve app performance. However, when it comes to individuals with a high level of bonding social capital, considering that they gain bonding social capital through disclosure behaviors, they are more used to and more prone to reveal information to others. In this manner, it is highly possible that they are always open to disclose friends' data to apps no matter whether or not such information is useful to apps' functionalities. Given that, it is perhaps not surprising that when data collection about friends does not improve apps' functionalities (T1), the difference of interdependent privacy value among individuals with a low and individuals with a high level of bonding social capital is significantly larger than the difference under the case of app relevant data collection (T2).

Although bonding social capital significantly impacts the value of interdependent privacy, our work suggests that bridging social capital does not. As to the insignificant influence of bridging social capital on interdependent privacy value, a possible explanation might be that bridging social capital is valued less or can be much more easily gained than bonding social capital [163]. As such, individuals are less likely to disclose information or to sacrifice privacy for gaining weak ties that correspond to bridging social capital. In this manner, individuals with a high level of bridging social capital do not undertake too much privacy concessions. Therefore, unlike those with a high level of bonding social capital, these individuals do not necessarily place a low value on their friends' information.

Another main finding from our analysis is that the impact of number of friends on how much individuals value friends' information depends on app data collection context. Specifically, we detect a significant cross-over interaction between number of friends and treatment. Much as what we have anticipated, in T1, where data collection is not useful for apps' functionalities, the more friends individuals have, the more value they place on information of all their friends. However, we observe an opposite association in T2, i.e., individuals with more friends actually value their friends' information less. One possible explanation of this seemingly counter-intuitive finding is that under the case where data collection is relevant for apps' functionalities, individuals might believe that sharing information about more friends results in better app performance. As such, under this particular data collection context, individuals with more friends would be more willing to share all their friends' information, reducing the value they place on such information. This further indicates that people might trade off friends' privacy for benefits they gain from apps, suggesting individuals can be considered as "privacy egoists" [9]. Another explanation could be that the more friends individuals have, the more they may think that they can afford to lose friends. Since they do not care too much about losing friends, they are more likely to release friends' information when they

believe such information is useful for app's performance. Alternatively, the negative association between number of friends and how much individuals value their friends' privacy in T2 may be attributed to "diffusion of friction". When individuals have more friends, it is more likely that they believe some of their friends have already installed the app. In other words, they are more likely to perceive that their friends' information has already been accessed by the app. Therefore, under cases where friends' information contributes to app functionality, they are more willing to also release that information to the app, and hence place less value on friends' privacy.

Furthermore, as expected, our analysis confirms the positive impact of concern for friends' privacy on individuals' valuation of interdependent privacy. This implies that privacy concerns are critical factors that shape and influence a user's economic valuation of personal information. Given this result, we believe it might be a viable way to change individuals' disclosure behaviors as well as to increase their valuation about friends' information via increasing their privacy concerns towards such information.

Finally, our analysis also examines the differences of interdependent privacy value in terms of demographics. Particularly, we find females value friends' information more than males, which is consistent with the finding that females report higher privacy concerns than their male counterparts [173]. In line with the research finding that older individuals are more concerned about their privacy in comparison to younger adults [174], we observe that the value of interdependent privacy increases with an increase of age. As is suggested by previous studies, this is most likely due to the fact that older individuals are more likely to be pragmatic and privacy conscious [174], while younger ones tend to behave less carefully and take things too far with regard to the disclosure of personal information on SNSs [175]. These results indicate policy makers should consider novel ways of addressing these possible differences related to interdependent privacy value by gender and age.

Although, we believe that both education level and income level should have

significant effects on interdependent privacy valuation, our study fails to support the existence of such impacts. This suggests important topics for further exploration of the roles of education level and income level on privacy valuation.

4.7 Summary

Through conducting a series of regressions on data collected from an online survey, our work contributes to a better understanding of the valuation of interdependent privacy in social app adoption contexts. Importantly, we empirically examine the complex relationship between social capital and interdependent privacy value. Although, we fail to find a significant association between bridging social capital and interdependent privacy value, our analysis suggests that the value app users' place on their friends' information is reversely related to their perceptions of bonding social capital. In other words, the higher the level of bonding social capital individuals have, the lower they value their friends' data. In addition, we also discover that the impact of bonding social capital on interdependent privacy value varies with app data collection context. In particular, when the level of bonding social capital increases, privacy valuation decreases much more quickly in app-irrelevant data collection contexts than otherwise, suggesting that for individuals with a higher level of bonding social capital, their willingness to disclose friends' data is less sensitive to app data collection context.

Furthermore, we also detect a cross-over interaction between number of friends and data collection context on interdependent privacy value. Specifically, in the case where data collection about friends is irrelevant to apps' functionalities, individuals' value of interdependent privacy increases with a growing number of friends. However, we find surprisingly that when users believe data collection about friends is useful for app performance, the more friends individuals have, the less value they place on all their friends' information.

Chapter 5

Study 3: Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter?

Our studies in the last two chapters quantify and briefly explain the value of interdependent privacy. A key finding is that individuals exhibit behaviors which can be interpreted as privacy egoism; that is they value their own information much higher than the information of a friend. In addition, we also find that factors such as data collection context (i.e., whether friends' information is necessary for apps' functionality), the level of ones' social capital, and friends' number influence how much value individuals places on interdependent privacy.

However, the understanding of important contextual factors that influence interdependent privacy decision-making is still in its infancy. In particular, we do not yet understand how characteristics of the platform which mediates the sharing influence human choices about others' privacy. A key aspect is to which degree transparency (between the sharer and the affected individuals) about a sharing decision influences the propensity to share information, or affects valuation of personal information of friends. In other words, our central research question is whether different modes of *anonymity* (or identifiability) influence how a sharing

decision is perceived when it affects interdependent privacy valuation.

In particular, in the scenario of third-party app adoption on SNSs where users are presented with app offers and associated authorization dialogues which may trigger sharing decisions over their own personal information and their friends' personal information [1], the ability of an affected individual to learn about others' sharing decisions is quite modest. For example, users may be subjected to social app advertisements and may indirectly learn that a friend has adopted an app which triggers the sharing of friends' information.[1] We are focused on studying the impact of this veil of anonymity and its counterpart, i.e., full identifiability, of sharing decisions.

To address our research question, our first step is to quantify interdependent privacy value by applying the methodology of conjoint analysis. In Chapter 3, we discuss details of conducting a full-profile conjoint study to determine such value. However, due to a high cognitive challenge presented by full-profile conjoint method, even after implementing the screening task, Study 1 is still suffering from low quality responses and thus we have to exclude these responses from final analysis. To address this data quality concern, we utilize a different methodology, i.e., choice-based conjoint analysis, to determine interdependent privacy valuation. Further, we introduce, in the choice-based conjoint study, 4 treatment scenarios which differ in whether or not sharing friends' data is anonymous (*sharing anonymity*), and whether or not the requested friends' data is useful to app's functionalities (*context relevance*). This design not only lets us to reassess our previous findings regarding the influence of data collection contexts on valuations of interdependent privacy, but more importantly allows us to examine how sharing anonymity affect app users' valuation towards their friends' data.

In order to comprehensively explain valuation of friends' information, following

[1]In the mobile app context even such spurious cues may not exist when a user shares an address book or other data type which contains friends' data. Likewise, in the context of genetic privacy there is no mechanism that automatically informs other family members about the decision by one individual to take a test.

Study 1's research methodology, our second step is then to apply Structural Equation Modeling (SEM) analysis to investigate how interdependent privacy values are influenced by factors such as *other regarding preference* (see details in later sections), disposition to value privacy, perceived control, and treatment conditions, i.e., sharing anonymity and context relevance.

This chapter is structured as follows. In Section 5.1, we present the choice-based conjoint analysis approach, and the associated results. Afterwards, in Section 5.2, we discuss the development and results for the behavioral model based on SEM. Finally, we summarize in Section 5.3.

5.1 Conjoint Analysis to Determine Privacy Value

5.1.1 Design of Choice-based Conjoint Study

As is discussed in Study 1, conjoint analysis is a general approach for analyzing consumer preferences for multi-attribute products and services [105]. In a conjoint analysis study, it is often assumed that consumers view a product as a bundle of certain features (*attributes*), which have different values (*levels*) [107]. Through testing and analyzing individuals' preferences for multiple versions of a product (*profiles*), researchers are able to decompose the overall utilities of the different product versions, and hence understand the role which each attribute plays in individuals' decision-making [176].

Applying the methodology of conjoint analysis to our context, we assume users view a third-party app as a combination of multiple app features, which is the same idea we used in Study 1. For example, if "information an app collects about a user's friends" constitutes an attribute of an app, the respective levels will be what or how much friends' information is collected. Through analysis of how individuals evaluate versions of an app, we are able to infer how each factor, particularly revealing friends' personal information, affects a user's decision of adopting an app.

Table 5.1: Summary of attributes and levels

Attributes	Attribute Descriptions	Attribute Levels
Price	Price of the app	**$0.00**: The app is free **$1.99**: The app costs $1.99
Network Popularity	Percentage of a user's friends who installed the app	**5%**: 5% of a user's friends have installed the app **25%**: 25% of a user's friends have installed the app
Own Privacy	Information the app collects about a user	**None**: The app does not collect any information about a user **Basic profile**: The app collects a user's name, profile picture, gender, user ID, and any other information the user made public on his/her profile **Full profile**: The app collects a user's *Basic profile*, and in addition the user's valuable information, such as email address, birthday, photos, and location information
Friends' Privacy	Information the app collects about a user's friends	**None**: The app does not collect any information about a user's friends **Basic profile**: The app collects a user's friends' names, profile pictures, genders, user IDs, and any other information friends made public on their profiles **Full profile**: The app collects a user's friends' *Basic Profiles*, and in addition friends' valuable information, such as email addresses, birthdays, photos, and location information

5.1.1.1 Determination of Apps' Attributes and Their Levels

As is discussed in Study 1, through conducting 18 semi-structured interviews with app users, we identified four attributes that are most frequently regarded as relevant to the choice of third-party apps. In addition, the interview results also helped us to determine levels of these four app attributes. In this study, we used the same app attributes and levels that are used in Study 1. In Table 5.1, we summarize these app attributes and levels.

5.1.1.2 Selection of Conjoint Analysis Method

As is mentioned in Study 1, there are two popular ways to conduct conjoint analyses: full-profile conjoint analysis and choice-based conjoint analysis. In Study 1, we select the full-profile method where participants are asked to rank 9 versions of a social app that differs in four attributes. Considering that each of these four attributes has different levels, ranking 9 app versions represents a very high cognitive challenge to respondents [107]. As a result, even after implementing the screening task, Study 1 is still suffering from low quality responses and thus we have to

exclude these responses from final analysis.

To address this problem, we decided to apply the methodology of choice-based conjoint analysis. In a choice-based conjoint study, respondents are asked to choose an alternative from a small set (normally 2 or 3) of profiles (*choice set*) [177]. Participants then repeat this task for a limited number of choice sets, thereby providing adequate data for analysis. As a result, compared with full-profile conjoint analysis, the choice-based method poses less challenges to participants. We expect that by choosing this approach, we can obtain significantly higher quality responses.

5.1.1.3 Selection of App Profiles

We next discuss how to determine the number of choice sets to be included in the study. While there is no clear guidance on this issue, prior studies indicate that respondents are capable of managing 17 choice sets without problems [178], and a study on the commercial use of conjoint analysis reported a median value of 16 choice sets in typical conjoint designs [179]. Based on these results, we included 16 choice sets in our study. Note here, in order to check for consistency of participants' responses, we set two choice sets to be the same. Therefore, our study included 15 distinct choice sets.

We adapted R code provided by Burda and Teuteberg [180] to create choice scenarios (choice sets) in our study. Specifically, with the help of Algorithmic Experimental Design [181] (i.e., a R package), we calculated a fractional factorial design from our full factorial design ($2 \times 2 \times 3 \times 3 = 36$ stimuli) by following a 5-step procedure described in [182]. Using this method, we derived a design including 15 different app profiles which were randomly combined to form the choice sets. In addition, in order to make the scenario more realistic, we also introduced the "no choice" option in each choice set. Therefore, we generated 15 different choice sets, with each of them including two app profiles and one "no choice" option.

5.1.1.4 Estimation of Conjoint Model

Hierarchical Bayes (HB) estimation takes into consideration that individuals have heterogeneous preferences regarding product specific attributes and is generally preferred for analyzing choice-based conjoint models [183]. Without treating all individuals alike, HB methods allow not only for estimating a conjoint model on an aggregate level, but also for calculating parameter estimates associated with specific individuals, i.e., individual-level part-worth utilities. Finally, we utilize the R package Bayesm [184] to conduct the HB estimation and to analyze our choice-based conjoint model.

5.1.2 Design of Survey Experiment

5.1.2.1 Treatments

Prior research indicates that individuals behave differently when anonymity is preserved than under circumstances with full information and observability. We reviewed this literature in the related work section, but briefly summarize several results here. For example, by comparing results of F2F bargaining and anonymous bargaining in a classic behavioral experiment that aims to understand how agents cooperate with each other, Radner and Schotter find that F2F bargaining captured a higher percentage of gains from trade than anonymous bargaining [81]. Similarly, in another pair of comparative experiments, Roth and Malouf observe fewer equal splits and more disagreements in anonymous bargaining than in the F2F setting [185]. Interpreting these results, Siegel and Fouraker acknowledge that small differences in the social environment (such as the provisioning of anonymous communications) might lead to a large divergence in behavior [186]. Therefore, they argue that social variables, in particular anonymity, should either be systematically studied or controlled in behavioral experiments [186].

Applied to our context, we conjecture that anonymity plays a significant role in

individuals' valuations of interdependent privacy. More specifically, we argue that app users will valuate their friends' information comparatively lower when they believe sharing friends' information to apps is anonymous than in a full information scenario with observability of actions. In order to empirically investigate such an effect, we introduced the following 2 treatment scenarios regarding *sharing anonymity*:

1 *Friends will not be able to discover who releases their information to apps (anonymous sharing).*

2 *Friends will be able to discover who releases their information to apps (identifiable sharing).*

As is discussed in Study 1, previous studies reveal that individuals' privacy concerns are influenced by whether or not information requests are context-relevant [106]. For example, Wang et al. [171] discover that while app users are typically unconcerned about giving away birthday information to an app, they nevertheless become uncomfortable when the app wants to collect information that is unrelated to an app's stated purposes. Motivated by the theory of contextual integrity and the aforementioned empirical results, we also aim to explore how app data collection context impacts the value which app users place on their friends' information.

To this end and also to reassess the previous research findings regarding data collection context, similar to how we deal with sharing anonymity, we introduced the following 2 treatment scenarios regarding *context relevance*:

1 *The information the app collects about user's friends is not useful for app's functionality (irrelevant context).*

2 *The information the app collects about user's friends is useful for app's functionality (relevant context).*

To sum up, we included a total of 4 treatment scenarios (2 sharing anonymity $\times$ 2 context relevance) in our study. We then randomly placed participants in one of the 4 treatment scenarios, which was then introduced as part of the task instructions. In addition, we displayed a short version of the instructions with the treatment conditions above each choice-based conjoint question.

5.1.2.2 Procedure

After consenting to take part in the study, participants were randomly placed into one of the 4 treatment scenarios, and were provided with task instructions. Next, they were presented with 16 questions (see Figure 5.1 for app choice interface), which corresponded to the 16 choice sets in the conjoint analysis study. In each question, they were required to select their favorite alternative from two app versions and a "no choice" option.

After participants finished all 16 questions regarding their preferred choice of app profiles, they were asked to answer several demographic questions. In addition, since our paper aims not only to quantify the value of interdependent privacy and its dependency on sharing anonymity, but also to build a model to explain app users' privacy evaluation process, we also measured perceptual variables regarding users' privacy related attributes, beliefs and experiences (see details in later sections).

5.1.2.3 Participants and Recruitment

We recruited participants from Amazon Mechanical Turk, a recruitment source that is very popular for conducting online user experiments [115]. We restricted participants to Turkers who had completed over 50 Human Intelligence Tasks (HITs) with a HIT approval rating of 97% or better, as well as those who had United States IP addresses. In addition, eligible participants should have previously installed at least one app on their social network sites so that they were familiar with the scenario setting in our study.

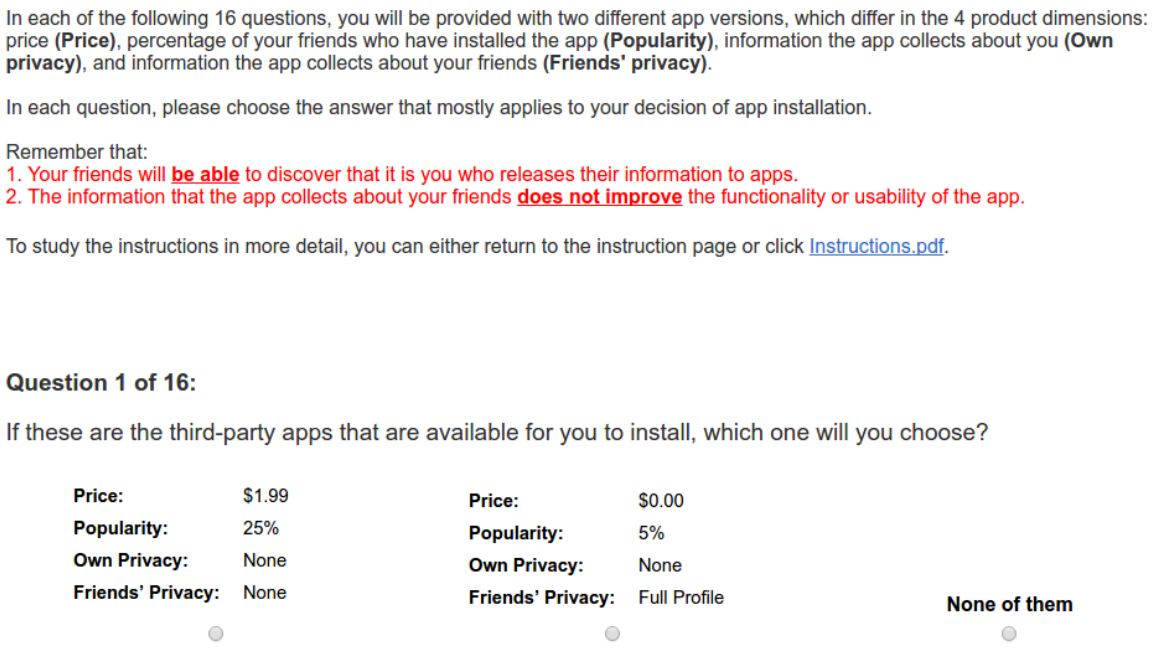

Figure 5.1: Screenshot of app choice interface

5.1.3 Results of Choice-based Conjoint Study

5.1.3.1 Participant Data

We collected a total of 1007 responses. After filtering out data based on conditions such as whether participants are US citizens, whether responses pass the check conditions implemented in the survey, and whether responses result in privacy value that are outliers[2], our final sample included responses of 931 participants for data analysis.

Of the 931 participants, 47.6% are male and 52.4% are female. In addition, our sample covers a wide range of age categories and education levels, ranging from 18 to over 50, and ranging from less than high school to higher education degrees such as master and PhD, respectively. In terms of income level, our participants have

[2]For some responses, utilities associated with "$1.99" and "$0.00" are identical or nearly identical, which indicates zero or approaching zero utility change associated with per-dollar change. Under this case, dollar equivalents for level changes in other attributes are either not determinable or abnormally large. Therefore, we did not include such responses in our analysis.

yearly incomes that range from less than $25,000 to more than $100,000, with a majority of them falling into the categories below $50,000.

Among the 931 participants, 234 were assigned to T1 (anonymous sharing & irrelevant context), 230 were assigned to T2 (identifiable sharing & irrelevant context), 239 were assigned to T3 (anonymous sharing & relevant context), and the remaining 228 were assigned to T4 (identifiable sharing & relevant context). Chi-square tests indicate that these four samples do not significantly differ regarding the demographic measures described above.

5.1.3.2 Estimations of Privacy Values

In this section, we first describe goodness-of-fit of the estimated conjoint model. Then, we show how to use the estimated model parameters to quantify privacy valuation.

We conducted two tests to assess goodness-of-fit of the estimated model. A likelihood ratio (LR) test was first performed to measure how well the model and its estimated parameters perform compared with having no model [187]. The test indicated that all the four estimated models (one model for each treatment scenario) are statistically valid ($p < 0.001$ for all models), i.e., the null hypothesis that the estimated model and zero model are equal can be rejected. In addition, to assess the validity of our model, we calculated the hit rate by identifying the alternative with the highest probability in all 15 choice sets for each participant. Each of the four models has a hit rate of more than 90%, demonstrating all these four models are well fitted.

Next, we calculated dollar values for privacy following the approach described by Krasnova et al. [69]. Conjoint analysis allows us to calculate individual and aggregated part-worths (utilities), which denote the attractiveness of a specific attribute level. Based on the part-worths, we calculated utility changes between various attribute levels as well as corresponding dollar values for each attribute level

Table 5.2: Utility change and monetary value of change

Attributes	Level Change	Utility Change				Dollar Value			
		T1	T2	T3	T4	T1	T2	T3	T4
Price	\$0.00 ⇒ \$1.99	-3.43	-2.62	-3.60	-3.36	-1.99	-1.99	-1.99	-1.99
Own Privacy	None ⇒ Basic profile	-0.35	0.24	0.37	0.53	0.016	-1.38	0.20	0.34
	Basic profile ⇒ Full profile	-3.69	-2.73	-2.51	-2.80	-2.80	-2.28	-2.27	-2.36
	None ⇒ Full profile	-4.04	-2.48	-2.14	-2.27	-2.78	-3.66	-2.07	-2.02
Friends' Privacy	None ⇒ Basic profile	-0.60	-1.31	-0.17	-1.39	-0.55	-1.74	-0.02	-0.80
	Basic profile ⇒ Full profile	-3.37	-2.33	-1.82	-2.85	-2.36	-3.20	-1.49	-2.26
	None ⇒ Full profile	-3.97	-3.64	-1.99	-4.25	-3.33	-5.40	-2.09	-2.82

change. We show these results in Table 5.2, where the "Utility Change" column indicates aggregated utility changes, while the "Dollar Values" column displays averages of dollar values perceived by individuals.

From Table 5.2, we can access dollar values which individuals place on different dimensions of own information, and of friends' information. For example, we notice that under the case where sharing friends' information is anonymous and where such information is irrelevant to app's functionality (T1), individuals value their friends' basic information (corresponding to friends' privacy level change from "None" to "Basic profile") at \$0.55, friends' valuable information (referring to friends' privacy level change from "Basic profile" to "Full profile") at \$2.36, and friends' full profile information (matching friends' privacy level change from "None" to "Full profile") at \$3.33.

We also observed from Table 5.2 that in most cases, dollar values which individuals place on their friends' information are slightly larger compared to their valuation of their own information. At the first glance, this observation might be counter-intuitive. However, friends' privacy value reported here is the dollar value that an individual places on the information of *all* of his/her friends. Considering that our participants self-reported to have on average 263 friends on their preferred SNS, this means that the value for a single friend's personal information is very small suggesting that individuals are "privacy egoists".

5.1.3.3 Effects of Sharing Anonymity and Context Relevance on Privacy Valuation

We conducted a two-way analysis of variance (ANOVA) to investigate both the effects of sharing anonymity and context relevance on personal privacy valuation and interdependent privacy valuation.

Our analysis demonstrates a significant main effect of sharing anonymity on the valuation of friends' basic information ($F(1, 931) = 11.95, p = 0.001$), friends' valuable information ($F(1, 931) = 6.33, p = 0.012$), and friends' full profile information ($F(1, 931) = 5.03, p = 0.025$). More specifically, when sharing friends' information is anonymous, individuals value their friends' privacy lower than under the case where such sharing behavior is identifiable (see Figure 5.2, Figure 5.3, and Figure 5.4).

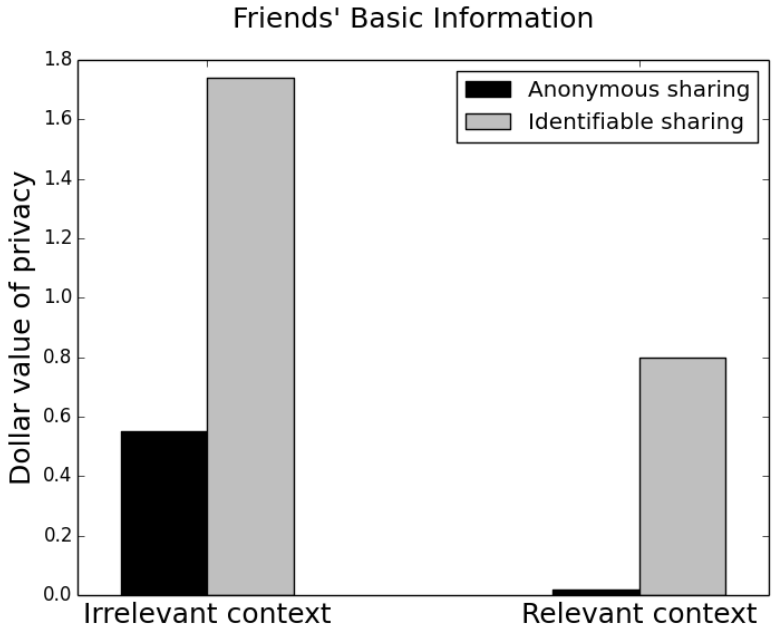

Figure 5.2: Effects of sharing anonymity and context relevance on valuation of friends' *basic* information

When it comes to the valuation of personal privacy, we fail to detect a significant impact of sharing anonymity. In other words, the condition as to whether or not

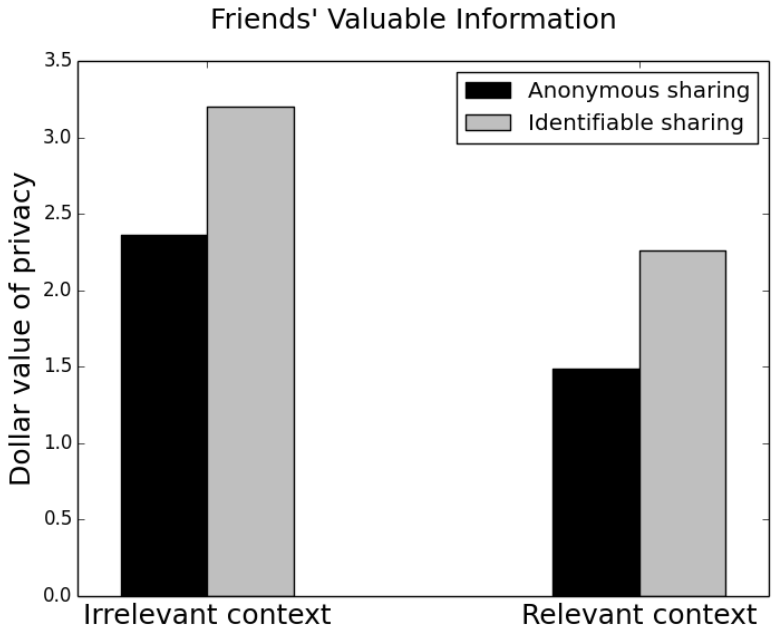

Figure 5.3: Effects of sharing anonymity and context relevance on valuation of friends' *valuable* information

sharing friends' information is anonymous does not affect how individuals value their own basic information ($F(1, 931) = 1.72, p = 0.189$), valuable information ($F(1, 931) = 0.14, p = 0.708$), or full profile information ($F(1, 931) = 0.90, p = 0.344$).

As to the condition of context relevance, we find it to significantly affect valuation of interdependent privacy. Specifically, individuals place higher values on friends' basic information ($F(1, 931) = 6.61, p = 0.010$), valuable information ($F(1, 931) = 7.92, p = 0.005$), and full profile information ($F(1, 931) = 9.32, p = 0.002$), when they believe that information improves apps' functionality compared to the alternative scenario (see Figure 5.2, Figure 5.3, and Figure 5.4).

The impact of context relevance regarding the valuation of own valuable data is insignificant ($F(1, 931) = 0.15, p = 0.696$); however, we observe that the treatment effect is significant for the value which individuals place on their own basic information ($F(1, 931) = 3.86, p = 0.050$) and full profile information

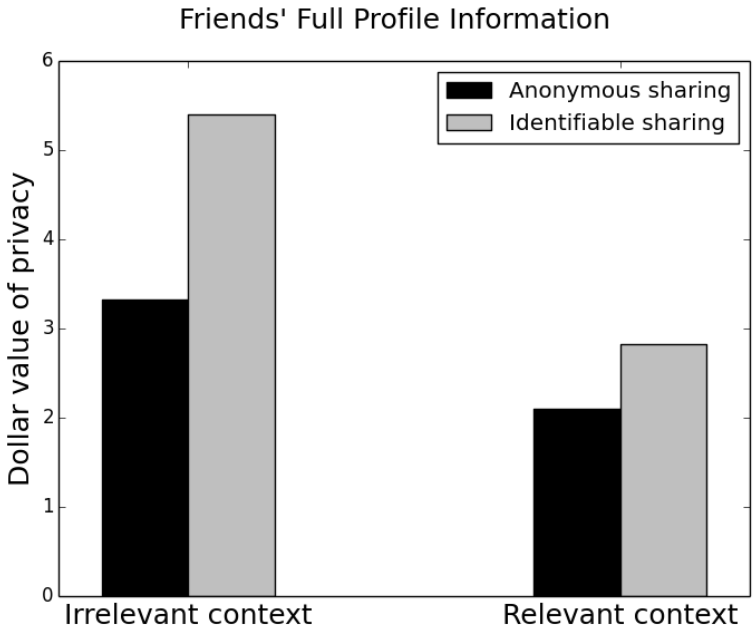

Figure 5.4: Effects of sharing anonymity and context relevance on valuation of friends' *full profile* information

($F(1, 931) = 7.17, p = 0.008$). This might indicate that the condition of context relevance, even though no information is given to the individual about the relevance of app's usage of own personal information, has a partial spillover effect on the valuation of their own privacy.

We also tested for any possible interactions between sharing anonymity and context relevance on privacy valuation. However, such effects do not exist for either own privacy valuation or interdependent privacy valuation.

5.2 SEM to Investigate Determinants of Privacy Value

Applying choice-based conjoint analysis, we quantified the dollar values which app users place on their own and friends' privacy. We next aim to position the conjoint study results in a SEM model to investigate what drives the valuation of personal and interdependent privacy. More specifically, we aim to understand how

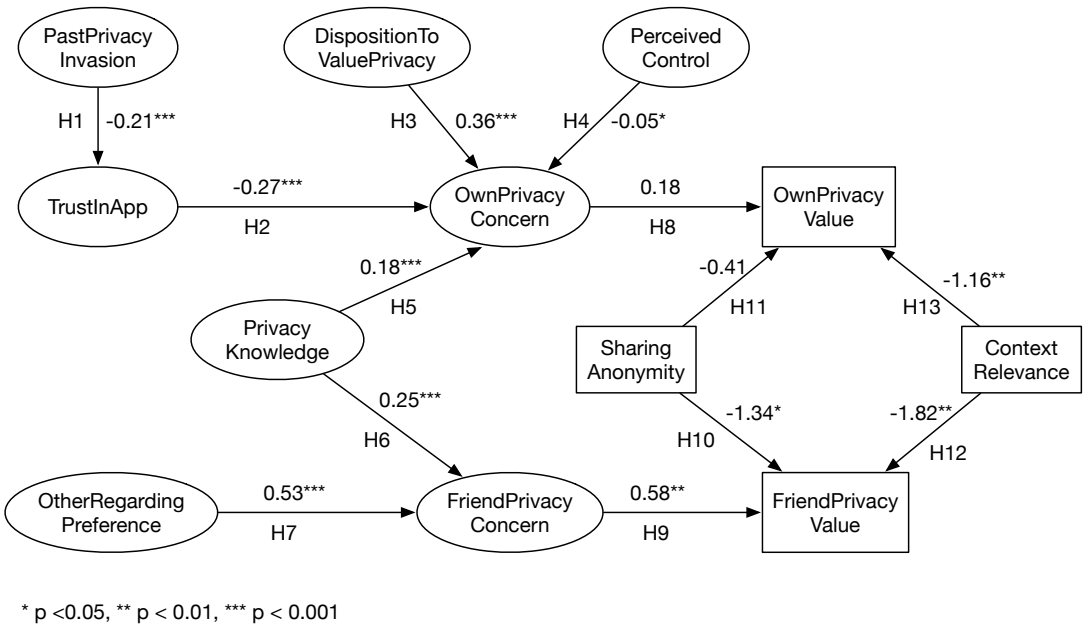

Figure 5.5: SEM explaining privacy valuation

factors such as different dimensions of privacy concerns, their antecedents, sharing anonymity, as well as context relevance affect the valuations of app users' own and their friends' information.

In this section, we first identify factors that affect users' valuations of privacy based on the existing literature. We next build a SEM model to examine relationships between these identified factors and the measured privacy valuations.

5.2.1 Hypotheses and Research Model

When individuals provide their information to other parties, a "social contract", which is generally understood as the expectation that these parties will manage personal information properly [122], is formed [121]. If individuals believe their personal information has been misused, they may consider such an implied contract breached [122, 125], and hence lower their trust assessment associated with the involved parties. In addition, prior research shows that in the electronic commerce context, an online consumer's privacy being intruded by a single online company

could lead to the perception of information misuse by the entire community of online sellers [126]. In particular, individuals who have been exposed to or have been the victim of personal information abuses could be more aware of what actions other parties could take to invade privacy [127]. Such awareness might in turn lead to the reduction of their trust in online companies. Applying this to our context, we argue that the more past privacy invasion experiences individuals have, the less likely they are to trust apps' practices to protect their privacy. Therefore, we hypothesize:

Hypothesis 1: *There is a negative relationship between individuals' past privacy invasion experiences and their trust in apps' data practices.*

Previous studies demonstrate trust can enhance the evaluation of benefits, and can mitigate privacy concerns [129]. In particular, Hoffman et al. [128] argue that in the setting of online commerce, trust creates positive attitudes toward Web retailers, such as they will not take advantage of any vulnerabilities. In other words, trust is individuals' feeling that they will gain the benefits they expect without suffering negative consequences [129]. In this manner, we believe that app users who trust in apps' data practices are less likely to be concerned when releasing their own personal information to apps. Hence, we making the following hypothesis:

Hypothesis 2: *There is a negative association between individuals' trust in apps' practices and their concerns for own information privacy.*

Disposition to value privacy is a personality attribute reflecting an individual's inherent need (or general tendencies) to manage personal information space [188]. Therefore, as opposed to individuals who tend to be more open regarding the sharing of their personal information, individuals with a higher disposition to value

privacy will also express a higher level of concern when disclosing their own personal information to others. Hence, we argue:

Hypothesis 3: *Individuals' dispositions to value privacy are positively related to their concerns for own information privacy.*

Empirical evidence in numerous studies reveals that control is one of the key factors that affects privacy concerns [122, 189]. For example, it has been found that individuals' perceptions of control over dissemination of personal information are negatively related to privacy concerns [190, 191]. Additionally, research has provided evidence that, in general, individuals will have fewer privacy concerns when they believe they can control the release and dissemination of their personal information [190, 192]. To confirm these findings, we also make the following hypothesis:

Hypothesis 4: *Individuals' perceived privacy control is negatively associated with their concerns for own information privacy.*

Prior research shows that receiving negative news reports regarding privacy, such as stories about the gathering and misusing of personal information, contributes to individuals' privacy concerns [130]. Therefore, we argue that the more knowledge about privacy an individual has, the higher the level of concerns he/she will express over both own and friends' privacy. Hence, we hypothesize:

Hypothesis 5: *Privacy knowledge is positively related to individuals' concerns for their own information privacy.*

Hypothesis 6: *Privacy knowledge is positively related to individuals' concerns for their friends' information privacy.*

Experimental studies provide substantial evidence that individuals deviate from pure self-interest in many decision-making situations [193–197]. That is, individuals exhibit other-regarding preferences [198, 199]; they care about the well-being and welfare of others. While in many decision-making scenarios individuals do not act purely based on self-interest, the strength of other-regarding preferences may vary for individuals and across contexts [193–197]. Applying these theories to our context, we believe individuals who have higher other-regarding preferences express higher levels of privacy concerns over their friends' information. Hence, we argue:

Hypothesis 7: *Individuals' other-regarding preferences are positively related to their concerns for friends' information privacy.*

In addition, it is reasonable to assume that while keeping other factors constant, more privacy concerned individuals exhibit higher privacy valuations (as measured in the conjoint study). It follows that we hypothesize:

Hypothesis 8: *Individuals' concerns for their own information privacy are positively associated with the perceived monetary value of their own information.*

Hypothesis 9: *Individuals' concerns for friends' information privacy are positively associated with the perceived monetary value of their friends' information.*

Recall that in the conjoint analysis study, we introduced four treatment conditions which manipulate whether disclosure of friends' information is anonymous (sharing anonymity), and whether friends' information is necessary for apps' functionality (context relevance). The conjoint analysis results demonstrate that both sharing anonymity and context relevance impact the value which app users place on their friends' information. When it comes to the valuation of own information,

we detect a significant impact of context relevance, but not for sharing anonymity.

Here, we integrate these effects in the SEM model not only for building a more comprehensive model of privacy valuation, but also for providing an additional method to examine significances of these effects. Therefore, we assume:

Hypothesis 10: *Under the condition of anonymous sharing, individuals place lower monetary values on their friends' information compared with identified sharing.*

Hypothesis 11: *Under the condition of anonymous sharing, individuals place lower monetary values on their own information compared with identified sharing.*

Hypothesis 12: *Under the condition of context-relevant data collection, individuals place lower monetary values on their friends' information compared with context-irrelevant data collection.*

Hypothesis 13: *Under the condition of context-relevant data collection, individuals place lower monetary values on their own information compared with context-irrelevant data collection.*

We present the research model, which is based on H1 $\sim$ H13, in Figure 5.5.

5.2.2 Measurement Scale Development

To the extent possible, we adapted measurement scales for the main constructs in this study from prior research to fit the app adoption context.

Adapting from Smith et al. [70], 4 questions were used to assess past privacy invasion experiences. Trust in apps were measured by a shortened 4-item version of trust measures from Fogel and Nehmad [140], Krasnova and Veltri [141], and Dwyer et al. [142]. To measure privacy knowledge, we used 4 items derived from Park et al. [139]. Disposition to value privacy and perceived control were measured based on the 3-item scale and 4-item scale developed in [188], respectively. With respect to other-regarding preference, we applied 5 items modified from the actively caring

Table 5.3: Evaluations of measurement model

	Cronbach's Alpha	Composite Reliability	Trust InApp	Privacy Knowledge	Past Privacy Invasion	Disposition ToValue Privacy	Other Regarding Preference	Perceived Control	Own Privacy Concern	Friend Privacy Concern
TrustInApp	0.88	0.89	0.81							
PrivacyKnowledge	0.88	0.88	-0.25	0.80						
PastPrivacyInvasion	0.78	0.78	-0.20	0.10	0.69					
DispositionToValuePrivacy	0.87	0.87	-0.14	0.08	0.24	0.84				
OtherRegardingPreference	0.71	0.74	-0.08	0.33	-0.02	0.08	0.61			
PerceivedControl	0.91	0.91	0.49	-0.28	-0.19	0.16	-0.06	0.84		
OwnPrivacyConcern	0.89	0.89	-0.41	0.25	0.21	0.60	0.20	-0.14	0.82	
FriendPrivacyConcern	0.93	0.93	-0.19	0.25	0.11	0.31	0.37	-0.10	0.58	0.88

scale in [200]. When it comes to privacy concern, four items derived from [70] are used to assess privacy concerns for one's own information. A similar set of 4 questions, which was also derived from [70], was applied to measure individuals' concern for friends' privacy. All items were measured on a Likert-type scale with 1 = strongly disagree to 5 = strongly agree. The exact questions are provided in Appendix A. In the conjoint analysis study, we measured three dimensions of privacy value: value of basic information, value of valuable information, and value of full profile information. Since the full profile information includes both basic and valuable information, we limit our model to the study of valuation of full profile information. As such, we used the monetary value that individuals place on their own full profile information to represent own privacy valuation in the SEM model. Similarly, the valuation of friends' privacy in the model is represented by the dollar value of friends' full profile information.

In addition, sharing anonymity and context relevance in the SEM model correspond to the treatment scenarios we set in the conjoint analysis survey. For example, a value of 1 of sharing anonymity indicates that sharing friends' information cannot be identified, and a value of 1 of context relevance demonstrate the friends' information collected by app improves apps' functionality.

5.2.3 Evaluation of the Measurement Model

The measurement model is evaluated in terms of both convergent validity and discriminant validity. Convergent validity measures the degree to which different

attempts to measure the same construct agree [145]. Two tests are conducted to determine the convergent validity of the scales: Cronbach's alpha and composite reliability of constructs. We present the test results in Table 3.4. As is shown in Table 5.3, the Cronbach's alpha values for all scales are larger than 0.7; an indication of adequateness proposed by Nunnally [147]. In addition, composite reliabilities of our constructs exceed Nunnally's [147] criterion of 0.7. Both of these tests support the convergent validity of our measurement model.

Discriminant validity evaluates to which degree measures of different constructs are distinct from each other [148]. Discriminant validity is achieved when the square root of the variance shared between a construct and its measures is greater than the correlations between the construct and any other constructs in the model. We show the results in Table 5.3. We observe from Table 5.3 that the correlations among constructs, i.e., non-diagonal elements, are less than the square roots of shared variance, i.e., diagonal elements, indicating our model fulfills the requirements of discriminant validity.

5.2.4 Evaluation of the Path Model

We first discuss goodness-of-fit data of the model. In SEM, the chi-square test is a frequently reported descriptive measure of fit. Usually, a chi-square test with a $p-$value exceeding 0.05 demonstrates a model is a good fit (i.e., significance might indicate a bad fit) [151]. Due to chi-square tests' sensitiveness to sample size, other goodness-of-fit criteria, such as Root Mean Square Error of Approximation (RMSEA) value and Comparative Fit Index (CFI), are also used [152]. A RMSEA value of 0.06 or less, or a CFI value of 0.90 or greater indicates the model fit is acceptable [153].

The goodness-of-fit data of our model is $\chi^2(579) = 1841.89, p = 0.00; RMSEA = 0.05$; and $CFI = 0.93$. Despite the significance of chi-square test, which is sensitive to sample size, RMSEA value and CFI together indicate that our model fit is

acceptable.

We next test H1 $\sim$ H13, which should be evaluated based on the sign and statistical significance for corresponding paths in the model. We show the test results in Figure 5.5.

Our results support most of the associations we hypothesized. Individuals' past privacy invasion experiences are found to be significantly and negatively associated with their trust in apps' data practices (H1 is supported), which in turn has a significant and negative impact on concerns for own personal privacy (H2 is supported). In support of H3 and H4, the positive relationship between individuals' disposition to value privacy and concerns for own privacy, and the negative association between individuals' perceived control and own privacy concerns, are both found to be significant. In addition, individuals' privacy knowledge is found to significantly impact concerns for both personal and friends' information privacy (H5 and H6 are supported). Further, the proposed impact of other-regarding preferences on concerns towards friends' information privacy is also significant (H7 is supported).

When it comes to the relationship between privacy concerns and monetary value of personal privacy, we do not find such an association which is statistically significant (H8 is not supported). In contrast, we observe a significant effect explaining the relationship between concerns for others' privacy and the valuation of friends' information (H9 is supported).

H10 $\sim$ H13 postulate the impacts of treatment conditions (sharing anonymity and context relevance) on privacy valuation. In support of H12 and H13, the negative impact of context relevance on both own privacy valuation and valuation towards friends' information are found to be significant. In addition, sharing anonymity is also significantly and negatively associated with the value which individuals place on their friends' privacy (H10 is supported). However, the proposed negative impact of sharing anonymity on how app users valuate their own personal information is insignificant (H11 is not supported). These results are in line with the findings we

have discussed earlier in the conjoint analysis study.

5.2.5 Discussion of SEM Results

Through conducting a SEM analysis, we explore factors that drive the valuations of own privacy and interdependent privacy. In particular, we examine how conditions such as sharing anonymity and context relevance affect privacy valuations.

Our results suggest that individuals' interdependent privacy valuations are partly determined by their personal attributes or experiences. For example, through raising privacy concerns for friends' information, app users' inherent other-regarding preferences play an important role in shaping how they value others' privacy. Similarly, through the mediation of concerns towards friends' privacy, privacy knowledge impacts the values which app users place on friends' information. This indicates that educating app users about practices impacting interdependent privacy might be a viable way to increase their valuation of interdependent privacy.

Our results further demonstrate that individuals' valuations of their friends' privacy can also be influenced by environmental settings. In particular, the value of interdependent privacy is found to be sensitive to the treatment regarding anonymity. It appears that when individuals believe their actions of disclosing friends' information to apps can be identified, they will think twice before taking such actions. Similarly, when friends' information collected by apps is irrelevant to apps' stated purposes, individuals will be more reluctant to share such information. Therefore, besides raising individuals' interdependent privacy concerns, an alternative way to protect those who might suffer from interdependent privacy is to manipulate exogenous conditions, e.g., by making the sharing of friends' data identifiable or by informing app users whether data collection is context relevant.

Similar to their concerns about friends' privacy, users' concerns towards their own privacy is affected by their personal beliefs and experiences. In particular, we find individuals' inherent needs to manage personal information space, and beliefs

regarding whether or not they are able to control privacy influence how concerned they are about their personal privacy.

When it comes to users' valuation of personal privacy, our results suggest that the condition as to whether friends' information collected by an app is relevant to the app's functionality also has a significant impact. Given that context relevance does not differ in terms of apps' practices of accessing users' own personal information, this suggests a spillover effect of this condition [137,138]. In other words, individuals might believe that their own information also contributes to app's functionality when they know this is the case for friends' information.

Although the empirical results provide overall support for the research model, they also reveal a few unexpected relationships that are inconsistent with what we have hypothesized. Specifically, the proposed positive associations between privacy concern for personal information and the perceived value of such information is not confirmed. This seemingly counter-intuitive result might be attributed to the nature of conjoint analysis. As discussed earlier, conjoint analysis is a method to uncover the hidden rules individuals use to make trade-off decisions. In other words, the conjoint methodology analyzes how individuals make trade-offs over different attributes. Applied to our context, the results we derive from conjoint analysis study are reflections of trade-offs participants make among app attributes, which include both personal privacy and friends' privacy. One thing to note here is that in the conjoint analysis survey, we highlighted treatment scenarios, i.e., 4 conditions regarding sharing anonymity and context relevant, not only during task instructions, but also at the beginning of each conjoint analysis question. Such emphasis might lead our participants to pay more attention to friends' privacy, and therefore affects their valuation for their own privacy. In this manner, even if users express high privacy concerns for their personal information, it does not necessarily correspond to high valuations for such information.

The insignificance of sharing anonymity in reducing users' perceived value of

their own information makes sense since we would not expect a spillover effect in this case. As individuals in our study setup know that they are sharing their own information, the condition of sharing anonymity would not play a role in app users' valuation of their own privacy. (Of course, in practice users may not always pay attention to privacy conditions associated with an adoption decision, or may not fully understand these terms as they are presented in user-unfriendly ways.)

5.3 Summary

To the best of our knowledge, this paper is one of the first formal studies to investigate the impact of anonymity on privacy decision-making and, in particular, on the valuation of interdependent privacy. Through conducting a choice-based conjoint analysis study with different treatment scenarios, we quantify the economic value app users place on both their own and friends' information, and also examine the impact of treatment conditions on privacy valuation. We also build and estimated a SEM model to explore how factors such as individuals' personal beliefs, attributes, experiences, as well as environment settings, i.e., sharing anonymity and context relevance, impact individuals' perceived value of both personal and friends' privacy.

Our results suggest that valuation of interdependent privacy is affected not only by individuals' personal attributes and experiences, such as other-regarding preference and privacy knowledge, but also by treatment conditions. In particular, we find that through raising concerns towards friends' privacy, individuals' other regarding preferences, and knowledge on privacy indirectly contribute to valuations of interdependent privacy.

When it comes to treatment conditions, our study shows that anonymity plays an important role in interdependent privacy valuation. In particular, when individuals believe sharing of friends' information is anonymous, they tend to value their friends'

data significantly *less*. Similarly, we find app users place a significantly lower value on their friends' information when they believe such information is useful for an app's functionality.

These results provide valuable insights for protecting friends' privacy in the context of app adoption. More specifically, our study conveys that besides raising individuals' interdependent privacy concerns, additional ways to protect friends' privacy are making the sharing of friends' data identifiable, and informing app users when data collection is not contextually relevant.

Chapter 6
Conclusions

Third-party social applications (social apps) have become a major growth factor for social network sites (SNS), and greatly increase the variability and breadth of interaction possibilities. Despite the benefits, however, users and consumer advocates grow increasingly concerned about the associated privacy risks arising from the collection and potential misuse of personal information. In particular, a newly discovered privacy issue associated with social apps is the *interdependency of privacy*. In the context of third-party social apps, the problem of *interdependency of privacy* refers to users making app adoption decisions which cause the collection and utilization of personal information of users' friends. In contrast, users' friends have typically little or no direct influence over these decision-making processes.

Although the problem of interdependent privacy is common in social app marketplaces, only a limited number of research studies have appeared on this subject. In this dissertation, we discuss one of the first attempts to investigate the problem space of interdependent privacy from the quantitative-behavioral and empirical perspectives. Specifically, in Study 1, by utilizing the results from a full-profile conjoint analysis, we quantify the economic value which individuals place on both their own and friends' information in social app adoption scenarios. We also construct a SEM model to explore how specific factors, such as data collection context (context relevance), privacy knowledge, and trust in apps, impact the process of privacy

valuation. Complementing Study 1 by more thoroughly explaining the valuation of interdependent privacy, Study 2 investigates in particular the relationship between social capital and interdependent privacy value through conducting a series of regression analyses. With Study 3, we explore important contextual factors that influence interdependent privacy decision-making. In particular, we investigate how different modes of anonymity (or identifiability) influence how a sharing decision is perceived when it affects interdependent privacy valuation. In addition, in order to address the concern of low data quality that results from full-profile conjoint analysis study, in Study 3, we utilize a different methodology, i.e., choice-based conjoint analysis, to quantify interdependent privacy valuations.

6.1 Summary of Findings

In a nutshell, the primary goal of the dissertation is to advance the understanding, as well as to explain valuations of interdependent privacy in social app adoption contexts. Most of our findings are consistent throughout the dissertation:

First of all, we find that although individuals somewhat care about their friends' privacy, i.e., place monetary value on interdependent privacy, they can be considered as "privacy egoists". For one thing, given the self-reported number of friends, the value associated with the profile of an average single friend is a very small fraction of the value associated with a user's own personal information. For another, users not only trade off their friends' information for accruing social capital, but are eager to reveal friends' data when they believe such disclosure behaviors result in better app performance.

In addition, when it comes to explain values for interdependent privacy, all of our three studies indicate that contextual factors play important roles in shaping interdependent privacy valuations. In particular, we confirm the impact of data collection context (context relevance), and the influence of sharing anonymity on

users' valuation towards their friends' data.

Further, our results in all the three studies suggest that valuations of interdependent privacy are also affected by individuals' personal attitudes and experience. For example, in both Study 1 & Study 3, we find significant associations between individuals' past privacy invasion experiences, their trust regarding apps' privacy practices, their knowledge about privacy, and interdependent privacy valuations. In addition, we observe in Study 2 that one's level of social capital, number of friends, and demographics such as gender and age also influence how people care about their friends' privacy. Finally, we observe in Study 3 that individuals' interdependent privacy valuations are also determined by other factors, such as one's disposition to value privacy, perceived control of privacy, and other-regarding preference.

Although there is a high level of consistency of research findings throughout the three studies, we also observe a few differences:

To begin with, in Study 3, we discover a spill-over effect of context relevance, i.e., the condition as to whether or not friends' information collected is useful for app's functionality also impacts how individuals value their own information. However, we fail to detect the same effect in Study 1. One possible explanation for this conflict might be related to the ways of conveying treatment scenarios to participants. Compared with the full-profile conjoint survey in Study 1, we emphasized more the treatments conditions, including conditions of context relevance, in Study 3. Specifically, in the choice-based conjoint survey, we not only highlighted the treatment conditions during task instructions, but also at the beginning of each conjoint analysis question. It is very likely that such emphasis triggered participants to think more about the data collection context so that they may have believed their own information also impacts apps' functionality.

In addition, although the empirical result in Study 1 supports the positive relationship between an individual's concern towards own information privacy and the value of such information, such association is not confirmed in Study 3.

This conflict might be attributed to the nature of conjoint analysis. As discussed earlier, conjoint analysis is a method to uncover the hidden rules individuals use to make trade-off decisions. In other words, the conjoint methodology analyzes how individuals make trade-offs over different attributes. Applied to our context, the results we derive from the conjoint analysis study are reflections of trade-offs participants make among app attributes, which include both personal privacy and friends' privacy. As is discussed earlier, we put more emphasis on the treatment scenarios in Study 3 than in Study 1. Such emphasis might lead participants in Study 3 to pay more attention to friends' privacy, which in turn affects their valuation for their own privacy. In this manner, even if users in Study 3 express high privacy concerns for their personal information, it does not necessarily correspond to high valuations for such information.

Both of these two conflicts indicate trade-offs we should consider when choosing ways of conveying treatment conditions to participants in human behavioral studies.

6.2 Summary of Contributions

The contributions of this thesis fall into two categories: advancing our understanding of interdependent privacy issues, and providing suggestions for conducting human behavioral research.

When it comes to the problem space of interdependent privacy, our research makes contributions to the privacy literature, privacy by redesign initiatives and the policy discussion on privacy.

First of all, we address the still inadequately investigated research area on privacy. Specifically, we expand the privacy literature by offering (1) one of the first empirical studies on the topic of interdependent privacy; (2) the first work to quantify the value of interdependent privacy; (3) the first attempt to explain associations between privacy values and other constructs; and (4) the first work to

investigate the impact of sharing anonymity on privacy decision-making.

Secondly, our study also offers insightful implications for "privacy by redesign". Research has proven that presenting privacy information in a clearer fashion to users when they are making adoption decisions can assist users in choosing less privacy-invasive apps [1, 15]. Our results highlight that contextual factors, such as context relevance and sharing anonymity, play important roles in interdependent privacy valuations. Therefore, in order to help app users make well-informed decisions, it would be helpful to revise apps' privacy notice dialogues so that they explicitly inform users whether apps' practices of collecting data are necessary for the app's functionalities. Further, conveying the information to app users whether sharing friends' information will be later discoverable by friends also helps.

In addition, our work indicates that app users are privacy egoists [9] not only in that they trade off their friends' information for accruing social capital, but also due to the fact that they are eager to reveal friends' data when they believe such disclosure behaviors result in better app performance. As such, relying on individuals themselves to protect their friends' privacy is likely not adequate. Therefore, affected friends of app users should be involved more directly in the decision-making process. For example, designs that enable mutual agreements regarding the sharing of others' data, e.g., reciprocal designs that allow one to share others' information if and only if he/she also lets others share his/her information, should be implemented. Alternatively, we can also introduce mechanisms that empower affected friends to unilaterally decide whether or not to allow their information to be shared by others.

Finally, our research fills important voids in the policy discussions on app privacy. As previously mentioned, it is inadequate to rely on app users themselves to protect their friends' privacy since app users behave like privacy egoists. This further emphasizes the importance of government intervention to limit the data sharing of friends' information.

In addition, we also find that privacy knowledge impacts the values which app users place on friends' information. This indicates that educating app users about practices impacting interdependent privacy might be a viable way to increase their valuation of interdependent privacy. Therefore, policy makers should consider introducing policies which integrate privacy in educational programs.

With regards to methodological contributions, our work offers useful suggestions for conducting human behavioral research.

For one thing, we conduct and compare the results of two conjoint analysis methods: full-profile conjoint analysis, and choice-based conjoint analysis. We find that full-profile conjoint study likely poses a significant cognitive challenge to human subjects, and thereby results in lower data quality compared with the choice-based conjoint analysis. Therefore, we suggest the selection of the choice-based method when conducting conjoint analysis studies that involve complex decision-making.

For another, the inclusion of an ice-cream screening task, which is similar to the app conjoint analysis experiment, has contributed to largely increase data quality in Study 1 compared with the results in [9]. This suggests that utilizing a screening task that is similar to the central task, which serves as a main purpose, is a viable way to increase data quality in human behavioral studies.

6.3 Limitations and Future Work

There are several limitations of our work, some of which present useful opportunities for further research.

First, our investigation about the influence of context on privacy valuations is limited to the measurable impact of app data collection context (context relevance) and sharing anonymity. However, other factors that might have considerable impact on users' privacy concerns and behaviors [106], such as app category, are not part of the study. To better understand the relationship between other contextual factors

and privacy valuations, more context dimensions should be evaluated in follow-up research.

Second, privacy concerns were given more prominence in our experiment than they would likely receive in practical decision-making scenarios. It is possible that this pronounced focus elevated the measured monetary valuations. Taking this into account, the very low valuations for an individual friend's personal information stand out even more. Recent research focused on the idea to measure privacy in survey settings *without asking about it* [201]. We consider it as a fruitful research direction to implement similar ideas in experiments and trade-off scenarios such as conjoint studies.

Third, in the choice-based conjoint analysis survey, we make the treatment scenarios salient by not only emphasizing them during task instructions, but also highlighting them in each conjoint choice question. Given that these treatment scenarios are highly related to the collection of friends' information, this implementation may give additional emphasis to the importance of interdependent privacy, and thereby reduce the perceived importance of personal privacy. Therefore, one should proceed with care when comparing the absolute values for personal privacy and friends' privacy. And one should reason deliberately when choosing ways of conveying treatment conditions to participants in human behavioral studies.

Fourth, although our paper empirically detects the negative association between interdependent privacy value and bonding social capital, additional work is needed to further examine the general relationship between social capital and privacy valuation. To this end, it would be useful to also investigate the impact of social capital on the value users place on their own privacy.

Fifth, the problem of interdependent privacy is also common in other contexts such as SNSs [42, 46] and email service [202]. Our focus on the app adoption setting might limit the generalizability of our findings to other settings. This pertains in particular to contextual factors (e.g., type of information collectors, the nature and

amount of information collected, technical characteristics of information collection). Therefore, a more comprehensive examination of interdependent privacy in other settings is needed.

Further, as with other studies in a specific geographical setting, our research focuses on individuals living in the United States. However, according to prior research [59, 141], individuals in different regions approach privacy issues differently. Therefore, it is necessary to further evaluate the robustness of our results by conducting a cross-cultural study that involves participants with different nationalities.

Finally, our results also provide motivation for extending our previously proposed economic model of app adoption to better understand the impact of interdependent privacy on user behaviors [8]. For example, one can integrate the factors of sharing anonymity and context relevance into the model, as well as simulate the model with empirical data, such as the value of interdependent privacy.

Appendix

Appendix A: Survey Instruments

PrivacyKnowledge: (Used in Study 1 & Study 3)

1. Companies today have the ability to place online advertisements that target you based on information collected about your web browsing behavior.
2. When you go to a website, it can collect information about you even if you do not register.
3. Popular search engine sites, such as Google, track the sites you come from and go to.
4. Many of the most popular third-party apps reveal users' information to other parties, such as advertising and Internet tracking companies.

PastPrivacyInvasion: (Used in Study 1 & Study 3)

1. How often have you personally been victim online of what you felt was an invasion of privacy?
2. How often have you personally been victim offline of what you felt was an invasion of privacy?
3. How often have you noticed others being victims online of what you felt was an invasion of privacy?

4. How often have you noticed others being victims offline of what you felt was an invasion of privacy?

TrustOnApp: (Used in Study 1 & Study 3)

1. Third-party app developers tell the truth about the collection and use of personal information.

2. Third-party app developers can be relied on to keep their promises.

3. I trust that third-party app developers will not use users' information for any irrelevant purposes.

4. I can count on third-party app developers to take security measures to protect customers' personal information from unauthorized disclosure or misuse.

OwnPrivacyConcern: (Used in Study 1 & Study 3)

1. It usually bothers me when third-party app developers ask me for personal information.

2. When third-party app developers ask me for personal information, I sometimes think twice before providing it.

3. It bothers me to give my personal information to so many third-party app developers.

4. I'm concerned that third-party app developers are collecting too much personal information about me.

FriendPrivacyConcern: (Used in Study 1 & Study 3)

1. It usually bothers me when third-party app developers ask me for my friends' personal information.

2. When third-party app developers ask me for my friends' personal information, I sometimes think twice before providing it.

3. It bothers me to give my friends' personal information to so many third-party app developers.

4. I'm concerned that third-party app developers are collecting too much personal information about my friends.

BridgingSocialCapital: (Used in Study 1)

1. Interacting with my online social network friends makes me want to try new things.

2. Interacting with my online social network friends makes me feel like part of a larger community.

3. Interacting with my online social network friends reminds me that everyone in the world is connected.

4. I am willing to spend time to support general online social network community activities.

5. On my online social network sites, I come in contact with new people all the time.

BondingSocialCapital: (Used in Study 1)

1. There are several online social network friends I trust to help solve my problems.

2. There are some online social network friends that I can turn to for advice about making very important decisions.

3. If I needed an emergency loan of $500, I know that I can turn to some of my online social network friends for help.

4. My online social network friends would be good job references for me.

5. I do not know my online social network friends well enough to get them to do anything important.

DispositionToValuePrivacy: (Used in Study 3)

1. Compared to others, I am more sensitive about the way personal information is handled.

2. Keeping information private is the most important thing to me.

3. Compared to others, I tend to be more concerned about threats to information privacy.

PerceivedControl: (Used in Study 3)

1. I believe I have control over who can get access to my personal information collected by third-party app developers.

2. I think I have control over what my personal information is released by third-party app developers.

3. I believe I have control over how my personal information is used by third-party app developers.

4. I believe I can control my personal information provided to third-party app developers.

OtherRegardingPreference: (Used in Study 3)

1. I have recently helped a person with a problem.

2. I should go out of my way to help people more often.

3. If a member of my "social group" comes to me with a personal problem, I'm willing to listen without being judgmental.

4. If a member of my "social group" needs help on a task, I am willing to help even if it causes me some inconvenience.

5. I am willing to help a "social group" member I don't know.

Bibliography

[1] Wang, N., J. Grossklags, and H. Xu (2013) "An online experiment of privacy authorization dialogues for social applications," in *Proceedings of the 16th ACM Conference on Computer Supported Cooperative Work (CSCW)*, pp. 261–272.

[2] Huber, M., M. Mulazzani, S. Schrittwieser, and E. Weippl (2013) "Appinspect: Large-scale evaluation of social networking apps," in *Proceedings of the First ACM Conference on Online Social Networks*, ACM, pp. 143–154.

[3] Frank, M., B. Dong, A. P. Felt, and D. Song (2012) "Mining permission request patterns from Android and Facebook applications," in *2012 IEEE International Conference on Data Mining*, IEEE, pp. 870–875.

[4] Symeonidis, I., F. Shirazi, G. Biczók, C. Perez-Sola, and B. Preneel (2016) "Collateral damage of Facebook apps: Friends, providers, and privacy interdependence," in *International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*.

[5] King, J., A. Lampinen, and A. Smolen (2011) "Privacy: Is there an app for that?" in *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS)*.

[6] Krishnamurthy, B. and C. Wills (2009) "On the leakage of personally identifiable information via online social networks," in *Proceedings of ACM SIGCOMM Workshop on Online Social Networks (WOSN)*, pp. 7–12.

[7] Biczók, G. and P. Chia (2013) "Interdependent privacy: Let me share your data," in *Financial Cryptography and Data Security* (A.-R. Sadeghi, ed.), vol. 7859 of *Lecture Notes in Computer Science*, Springer, pp. 338–353.

[8] Pu, Y. and J. Grossklags (2014) "An economic model and simulation results of app adoption decisions on networks with interdependent privacy consequences," in *Decision and Game Theory for Security* (R. Poovendran and W. Saad, eds.), Springer, pp. 246–265.

[9] ——— (2015) "Using conjoint analysis to investigate the value of interdependent privacy in social app adoption scenarios," in *Proceedings of the International Conference on Information Systems (ICIS)*.

[10] Coleman, J. (1988) "Social capital in the creation of human capital," *American Journal of Sociology*, **94**, pp. S95–S120.

[11] Putnam, R. (2001) *Bowling alone: The collapse and revival of American community*, Simon and Schuster.

[12] Williams, D. (2006) "On and off the Net: Scales for social capital in an online era," *Journal of Computer-Mediated Communication*, **11**(2), pp. 593–628.

[13] Smith, J., T. Dinev, and H. Xu (2011) "Information privacy research: An interdisciplinary review," *MIS Quarterly*, **35**(4), pp. 989–1016.

[14] Cavoukian, A. and M. Prosch (2011) "Privacy by ReDesign: Building a better legacy," *Information Privacy Commissioner Ontario*, pp. 1–8.

[15] Kelley, P., L. Cranor, and N. Sadeh (2013) "Privacy as part of the app decision-making process," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 3393–3402.

[16] Do, Q., B. Martini, and K. Choo (2014) "Enhancing user privacy on Android mobile devices via permissions removal," in *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*, pp. 5070–5079.

[17] Enck, W., P. Gilbert, S. Han, V. Tendulkar, B. Chun, L. Cox, J. Jung, P. McDaniel, and A. Sheth (2014) "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Transactions on Computer Systems*, **32**(2), pp. 5:1–5:29.

[18] Stiglitz, J. E. (2000) *Economics of the public sector*, W.W. Norton & Company.

[19] Book, T. and D. Wallach (2013) "A case of collusion: A study of the interface between ad libraries and their apps," in *Proceedings of the 3rd Annual ACM CCS Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM)*, pp. 79–86.

[20] Steel, E. and G. Fowler (2010) "Facebook in privacy breach," *The Wall Street Journal*.

[21] Besmer, A. and H. Richter Lipford (2010) "Users' (mis)conceptions of social applications," in *Proceedings of Graphics Interface (GI)*, pp. 63–70.

[22] King, J., A. Lampinen, and A. Smolen (2011) "Privacy: Is there an app for that?" in *Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS)*, pp. 12:1–12:20.

[23] Tam, J., R. Reeder, and S. Schechter (2010) *I'm allowing what? Disclosing the authority applications demand of users as a condition of installation*, *Tech. Rep. MSR-TR-2010-54*, Microsoft Research.

[24] Wang, N., H. Xu, and J. Grossklags (2011) "Third-party apps on Facebook: Privacy and the illusion of control," in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT)*, pp. 4:1–4:10.

[25] Chia, P. H., Y. Yamamoto, and N. Asokan (2012) "Is this app safe? A large scale study on application permissions and risk signals," in *Proceedings of the 21st International World Wide Web Conference (WWW)*, pp. 311–320.

[26] Shehab, M., S. Marouf, and C. Hudel (2011) "ROAuth: Recommendation based open authorization," in *Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS)*, pp. 11:1–11:12.

[27] Wang, N. (2012) "Third-party applications' data practices on Facebook," in *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems, Extended Abstracts (CHI EA)*, pp. 1399–1404.

[28] Smith, A. (2014), "6 new facts about Facebook," `http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/`, accessed: 2015-09-09.

[29] Felt, A., M. Finifter, E. Chin, S. Hanna, and D. Wagner (2011) "A survey of mobile malware in the wild," in *Proceedings of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, pp. 3–14.

[30] Felt, A., K. Greenwood, and D. Wagner (2011) "The effectiveness of application permissions," in *Proceedings of the 2nd USENIX Conference on Web Application Development (WebApps)*.

[31] Felt, A., E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner (2012) "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS)*, pp. 3:1–3:14.

[32] Beresford, A., A. Rice, N. Skehin, and R. Sohan (2011) "MockDroid: Trading privacy for application functionality on smartphones," in *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (HotMobile)*, pp. 49–54.

[33] Woollaston, V. (2014) "Is Facebook reading your TEXTS? Android update lets app access your written and picture messages," *Daily Mail Online*.

[34] Karambelkar, D. (2014) "Spyware: A bird's-eye view," *Gulf News*.

[35] Robertson, J. (2014) "Google+, 'Candy Crush' show risk of leakiest apps," *Bloomberg Technology*.

[36] Biasiola, S. (2013) "What friends are for: How network ties enable invasive third party applications on Facebook," in *Proceedings of Measuring Networked Privacy Workshop at Conference on Computer Supported Cooperative Work and Social Computing*.

[37] Olteanu, A.-M., K. Huguenin, R. Shokri, M. Humbert, and J.-P. Hubaux (2016) "Quantifying interdependent privacy risks with location data," *Rapport LAAS n16018*.

[38] Chessa, M., J. Grossklags, and P. Loiseau (2015) "A Game-theoretic study on non-monetary incentives in data analytics projects with privacy implications," in *Proceedings of the 2015 IEEE 28th Computer Security Foundations Symposium (CSF)*, pp. 90–104.

[39] Humbert, M., E. Ayday, J.-P. Hubaux, and A. Telenti (2015) "On non-cooperative genomic privacy," in *Financial Cryptography and Data Security* (R. Böhme and T. Okamoto, eds.), vol. 8975 of *Lecture Notes in Computer Science*, Springer, pp. 407–426.

[40] MacCarthy, M. (2011) "New directions in privacy: Disclosure, unfairness and externalities," *I/S: A Journal of Law and Policy for the Information Society*, **6**(3), pp. 425–512.

[41] Fairfield, J. and C. Engel (2015) "Privacy as a public good," *Duke Law Journal*, **65**, pp. 385–457.

[42] Shi, P., H. Xu, and Y. Chen (2013) "Using contextual integrity to examine interpersonal information boundary on social network sites," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 35–38.

[43] Choi, C. F. and Z. Jiang (2013) "Trading friendship for value: An investigation of collective privacy concerns in social application usage," in *Proceedings of the International Conference on Information Systems (ICIS)*.

[44] Morlok, T. (2016) "Sharing is (not) caring - The role of external privacy in users' information disclosure behaviors on social network sites," in *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*.

[45] Alashoor, T., M. Keil, L. Liu, and J. Smith (2015) "How values shape concerns about privacy for self and others," in *Proceedings of the International Conference on Information Systems (ICIS)*.

[46] Krasnova, H., N. Eling, O. Schneider, H. Wenninger, and T. Widjaja (2013) "Does this App ask for too much data? The role of privacy perceptions in user behavior towards Facebook applications and permission dialogs," in *Proceedings of the European Conference on Information Systems (ECIS)*.

[47] Böhme, R. and J. Grossklags (2011) "Vanishing signals: Trading agent kills market information," in *Proceedings of the 6th Workshop on the Economics of Networks, Systems and Computation (NetEcon)*.

[48] ——— (2013) "Trading agent kills market information: Evidence from online social lending," in *Proceedings of the 9th Conference on Web and Internet Economics (WINE)*, pp. 68–81.

[49] Klopfer, P. and D. Rubenstein (1977) "The concept privacy and its biological basis," *Journal of Social Issues*, **33**(3), pp. 52–65.

[50] Dinev, T. and P. Hart (2006) "An extended privacy calculus model for E-commerce transactions," *Information Systems Research*, **17**(1), pp. 61–80.

[51] Hui, K.-L., B. Tan, and C.-Y. Goh (2006) "Online information disclosure: Motivators and measurements," *ACM Transactions on Internet Technology*, **6**(4), pp. 415–441.

[52] Culnan, M. (1993) "'How did they get my name?': An exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, **17**(3), pp. 341–363.

[53] Grossklags, J. and N. Barradale (2014) "Social status and the demand for security and privacy," in *Privacy Enhancing Technologies* (E. De Cristofaro and S. Murdoch, eds.), vol. 8555 of *Lecture Notes in Computer Science*, Springer, pp. 83–101.

[54] Chellappa, R. and R. Sin (2005) "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management*, **6**(2-3), pp. 181–202.

[55] Wathieu, L. and A. Friedman (2007) "An empirical approach to understanding privacy valuation," *HBS Marketing Research Paper*, (07-075).

[56] Spiekermann, S., J. Grossklags, and B. Berendt (2001) "E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, pp. 38–47.

[57] Beresford, A., D. Kübler, and S. Preibusch (2012) "Unwillingness to pay for privacy: A field experiment," *Economics Letters*, **117**(1), pp. 25–27.

[58] Jentzsch, N., S. Preibusch, and A. Harasser (2012) "Study on monetising privacy: An economic model for pricing personal information," *ENISA, Feb.*

[59] Tsai, J., S. Egelman, L. Cranor, and A. Acquisti (2011) "The effect of online privacy information on purchasing behavior: An experimental study," *Information Systems Research*, **22**(2), pp. 254–268.

[60] Grossklags, J. and A. Acquisti (2007) "When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information." in *Proceedings of the Workshop on the Economics of Information Security (WEIS)*.

[61] Huberman, B., E. Adar, and L. Fine (2005) "Valuating privacy," *IEEE Security & Privacy*, **3**(5), pp. 22–25.

[62] Danezis, G., S. Lewis, and R. Anderson (2005) "How much is location privacy worth?" in *Proceedings of the Workshop on the Economics of Privacy (WEIS)*.

[63] Acquisti, A. and J. Grossklags (2012) "An online survey experiment on ambiguity and privacy," *Communications & Strategies*, **88**(4), pp. 19–39.

[64] Potoglou, D., S. Patil, C. Gijón, J. F. Palacios, and C. Feijóo (2013) "The value of personal information online: Results from three stated preference discrete choice experiments in the UK," in *Proceedings of the European Conference on Information Systems (ECIS)*.

[65] Egelman, S. (2013) "My profile is my password, verify me!: The privacy/convenience tradeoff of Facebook Connect," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 2369–2378.

[66] Krasnova, H., N. Eling, O. Abramova, and P. Buxmann (2014) "Dangers of 'Facebook login' for mobile apps: Is there a price tag for social information?" in *Proceedings of the International Conference on Information Systems (ICIS)*.

[67] Hann, I.-H., K.-L. Hui, T. Lee, and I. Png (2002) "Online information privacy: Measuring the cost-benefit trade-off," in *Proceedings of the International Conference on Information Systems (ICIS)*.

[68] Hann, I.-H., K.-L. Hui, S.-Y. T. Lee, and I. Png (2007) "Overcoming online information privacy concerns: An information-processing theory approach," *Journal of Management Information Systems*, **24**(2), pp. 13–42.

[69] Krasnova, H., T. Hildebrand, and O. Guenther (2009) "Investigating the value of privacy in online social networks: Conjoint analysis," in *Proceedings of the International Conference on Information Systems (ICIS)*.

[70] Smith, J., S. Milberg, and S. Burke (1996) "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly*, **20**(2), pp. 167–196.

[71] Malhotra, N., S. Kim, and J. Agarwal (2004) "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research*, **15**(4), pp. 336–355.

[72] Cespedes, F. and J. Smith (1993) "Database marketing: New rules for policy and practice," *Sloan Management Review*, **34**(4).

[73] Bansal, G., F. Zahedi, and D. Gefen (2010) "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, **49**(2), pp. 138–150.

[74] Lu, Y., B. Tan, and K.-L. Hui (2004) "Inducing customers to disclose personal information to Internet businesses with social adjustment benefits," in *Proceedings of the International Conference on Information Systems (ICIS)*.

[75] Eastlick, M., S. Lotz, and P. Warrington (2006) "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," *Journal of Business Research*, **59**(8), pp. 877–886.

[76] Metzger, M. (2004) "Privacy, trust, and disclosure: Exploring barriers to electronic commerce," *Journal of Computer-Mediated Communication*, **9**(4).

[77] Xu, H., H.-H. Teo, and B. Tan (2005) "Predicting the adoption of location-based services: The role of trust and perceived privacy risk," in *Proceedings of the International Conference on Information Systems (ICIS)*.

[78] Turow, J., C. Hoofnagle, D. Mulligan, N. Good, and J. Grossklags (2007) "The FTC and consumer privacy in the coming decade," *I/S: A Journal of Law and Policy for the Information Society*, **3**(3), pp. 723–749.

[79] Güth, W., R. Schmittberger, and B. Schwarze (1982) "An experimental analysis of ultimatum bargaining," *Journal of Economic Behavior & Organization*, **3**(4), pp. 367–388.

[80] Kahneman, D., J. Knetsch, and R. Thaler (1986) "Fairness and the assumptions of economics," *Journal of Business*, **59**(4), pp. S285–S300.

[81] Radner, R. and A. Schotter (1989) "The sealed-bid mechanism: An experimental study," *Journal of Economic Theory*, **48**(1), pp. 179–220.

[82] Prasnikar, V. and A. Roth (1992) "Considerations of fairness and strategy: Experimental data from sequential games," *The Quarterly Journal of Economics*, **10**(3), pp. 865–888.

[83] Roth, A. (1995) "Bargaining experiments," in *The Handbook of Experimental Economics* (J. Kagel, A. Roth, and J. Hey, eds.), Princeton University Press, pp. 253–348.

[84] Charness, G. and U. Gneezy (2008) "What's in a name? Anonymity and social distance in dictator and ultimatum games," *Journal of Economic Behavior & Organization*, **68**(1), pp. 29–35.

[85] Hoffman, E., K. McCabe, K. Shachat, and V. Smith (1994) "Preferences, property rights, and anonymity in bargaining games," *Games and Economic Behavior*, **7**(3), pp. 346–380.

[86] Alpizar, F., F. Carlsson, and O. Johansson-Stenman (2008) "Anonymity, reciprocity, and conformity: Evidence from voluntary contributions to a national park in Costa Rica," *Journal of Public Economics*, **92**(5), pp. 1047–1060.

[87] Soetevent, A. (2005) "Anonymity in giving in a natural context - A field experiment in 30 churches," *Journal of Public Economics*, **89**(11–12), pp. 2301–2323.

[88] Scott, C. (2004) "Benefits and drawbacks of anonymous online communication: Legal challenges and communicative recommendations," *Free Speech Yearbook*, **41**(1), pp. 127–141.

[89] Qian, H. and C. Scott (2007) "Anonymity and self-disclosure on weblogs," *Journal of Computer-Mediated Communication*, **12**(4), pp. 1428–1451.

[90] Hollenbaugh, E. and M. Everett (2013) "The effects of anonymity on self-disclosure in blogs: An application of the online disinhibition effect," *Journal of Computer-Mediated Communication*, **18**(3), pp. 283–302.

[91] Joinson, A. (2001) "Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity," *European Journal of Social Psychology*, **31**(2), pp. 177–192.

[92] Jiang, Z., C. S. Heng, and B. C. Choi (2013) "Research note - Privacy concerns and privacy-protective behavior in synchronous online social interactions," *Information Systems Research*, **24**(3), pp. 579–595.

[93] Thomas, K., C. Grier, and D. Nicol (2010) "unfriendly: Multi-party privacy risks in social networks," in *International Symposium on Privacy Enhancing Technologies*, Springer, pp. 236–252.

[94] Besmer, A. and H. Richter Lipford (2010) "Moving beyond untagging: Photo privacy in a tagged world," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 1563–1572.

[95] Ilia, P., I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis (2015) "Face/off: Preventing privacy leakage from photos in social networks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 781–792.

[96] Hu, H., G.-J. Ahn, and J. Jorgensen (2013) "Multiparty access control for online social networks: Model and mechanisms," *IEEE Transactions on Knowledge and Data Engineering*, **25**(7), pp. 1614–1627.

[97] Carminati, B. and E. Ferrari (2011) "Collaborative access control in on-line social networks," in *2011 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, IEEE, pp. 231–240.

[98] Such, J. and N. Criado (2016) "Resolving multi-party privacy conflicts in social media," *IEEE Transactions on Knowledge and Data Engineering*, **28**(7), pp. 1851–1863.

[99] Hu, H., G.-J. Ahn, Z. Zhao, and D. Yang (2014) "Game theoretic analysis of multiparty access control in online social networks," in *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies*, ACM, pp. 93–102.

[100] Such, J. and M. Rovatsos (2016) "Privacy policy negotiation in social media," *ACM Transactions on Autonomous and Adaptive Systems*, **11**(1), pp. 4:1–4:29.

[101] Wisniewski, P., H. Lipford, and D. Wilson (2012) "Fighting for my space: Coping mechanisms for SNS boundary regulation," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 609–618.

[102] Wisniewski, P., N. Islam, H. Richter Lipford, and D. Wilson (2016) "Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users," *Communications of the Association for Information Systems*, **38**(1), pp. 235–258.

[103] Lampinen, A., V. Lehtinen, A. Lehmuskallio, and S. Tamminen (2011) "We're in it together: Interpersonal management of disclosure in social network services," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 3217–3226.

[104] Cho, H. and A. Filippova (2016) "Networked privacy management in Facebook: A mixed-methods and multinational study," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, ACM, pp. 503–514.

[105] Green, P. and V. Srinivasan (1990) "Conjoint analysis in marketing: New developments with implications for research and practice," *The Journal of Marketing*, **54**(4), pp. 3–19.

[106] Nissenbaum, H. (2009) *Privacy in context: Technology, policy, and the integrity of social life*, Stanford University Press.

[107] Green, P. and V. Srinivasan (1978) "Conjoint analysis in consumer research: Issues and outlook," *Journal of Consumer Research*, **5**(2), pp. 103–123.

[108] Green, P. and A. Krieger (1991) "Segmenting markets with conjoint analysis," *The Journal of Marketing*, **55**(4), pp. 20–31.

[109] Gupta, S. and C. Mela (2008) "What is a free customer worth? Armchair calculations of nonpaying customers' value can lead to flawed strategies," *Harvard Business Review*, **86**(11), pp. 102–9.

[110] Green, P. and V. Rao (1971) "Conjoint measurement for quantifying judgmental data," *Journal of Marketing Research*, **8**(3), pp. 355–363.

[111] Ipeirotis, P. (2010) *Demographics of Mechanical Turk*, *Tech. rep.*, Social Science Research Network, Technical Report No. 1585030.

[112] Kam, C., J. Wilking, and E. Zechmeister (2007) "Beyond the "narrow data base": Another convenience sample for experimental research," *Political Behavior*, **29**(4), pp. 415–440.

[113] Mason, W. and S. Suri (2012) "Conducting behavioral research on Amazon's Mechanical Turk," *Behavior Research Methods*, **44**(1), pp. 1–23.

[114] Downs, J., M. Holbrook, S. Sheng, and L. F. Cranor (2010) "Are your participants gaming the system?: Screening Mechanical Turk workers," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 2399–2402.

[115] Goodman, J., C. Cryder, and A. Cheema (2013) "Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples," *Journal of Behavioral Decision Making*, **26**(3), pp. 213–224.

[116] De Meo, P., E. Ferrara, G. Fiumara, and A. Provetti (2014) "On Facebook, most ties are weak," *Communications of the ACM*, **57**(11), pp. 78–84.

[117] Bender, R. and S. Lange (2001) "Adjusting for multiple testing - When and how?" *Journal of Clinical Epidemiology*, **54**(4), pp. 343–349.

[118] Felt, A. and D. Evans (2008) "Privacy protection for social networking APIs," in *Proceedings of the 2008 Workshop on Web 2.0 Security and Privacy (W2SP)*.

[119] John, L., A. Acquisti, and G. Loewenstein (2011) "Strangers on a plane: Context-dependent willingness to divulge sensitive information," *Journal of Consumer Research*, **37**(5), pp. 858–873.

[120] Schumacker, R. and G. Marcoulides (1998) *Interaction and nonlinear effects in structural equation modeling*, Lawrence Erlbaum Associates Publishers.

[121] Caudill, E. and P. Murphy (2000) "Consumer online privacy: Legal and ethical issues," *Journal of Public Policy & Marketing*, **19**(1), pp. 7–19.

[122] Phelps, J., G. Nowak, and E. Ferrell (2000) "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing*, **19**(1), pp. 27–41.

[123] Gefen, D. (2000) "E-commerce: The role of familiarity and trust," *Omega*, **28**(6), pp. 725–737.

[124] Mayer, R., J. Davis, and D. Schoorman (1995) "An integrative model of organizational trust," *Academy of Management Review*, **20**(3), pp. 709–734.

[125] Culnan, M. (1995) "Consumer awareness of name removal procedures: Implications for direct marketing," *Journal of Direct Marketing*, **9**(2), pp. 10–19.

[126] Pavlou, P. and D. Gefen (2005) "Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role," *Information Systems Research*, **16**(4), pp. 372–399.

[127] Acquisti, A. and J. Grossklags (2005) "Privacy and rationality in individual decision making," *IEEE Security & Privacy*, **3**(1), pp. 26–33.

[128] Hoffman, D., T. Novak, and M. Peralta (1999) "Building consumer trust online," *Communications of the ACM*, **42**(4), pp. 80–85.

[129] Pavlou, P. (2003) "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *International Journal of Electronic Commerce*, **7**(3), pp. 101–134.

[130] Nowak, G. and J. Phelps (1992) "Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs," *Journal of Direct Marketing*, **6**(4), pp. 28–39.

[131] Hampton, K. and B. Wellman (2003) "Neighboring in Netville: How the Internet supports community and social capital in a wired suburb," *City and Community*, **2**(4), pp. 277–311.

[132] Kavanaugh, A., J. Carroll, M. Rosson, T. Zin, and D. Reese (2005) "Community networks: Where offline communities meet online," *Journal of Computer-Mediated Communication*, **10**(4).

[133] Bargh, J. and K. McKenna (2004) "The Internet and social life," *Annual Review of Psychology*, **55**, pp. 573–590.

[134] Helliwell, J. and R. Putnam (2004) "The social context of well-being," *Philosophical Transactions of the Royal Society B - Biological Sciences*, **359**(1449), pp. 1435–1446.

[135] Paxton, P. (1999) "Is social capital declining in the United States? A multiple indicator assessment," *American Journal of Sociology*, **105**(1), pp. 88–127.

[136] Granovetter, M. (1973) "The strength of weak ties," *American Journal of Sociology*, **78**(6), pp. 1360–1380.

[137] Dickinson, D. and R. Oxoby (2011) "Cognitive dissonance, pessimism, and behavioral spillover effects," *Journal of Economic Psychology*, **32**(3), pp. 295–306.

[138] Savikhin, A. and R. Sheremeta (2013) "Simultaneous decision-making in competitive and cooperative environments," *Economic Inquiry*, **51**(2), pp. 1311–1323.

[139] Park, Y., S. Campbell, and N. Kwak (2012) "Affect, cognition and reward: Predictors of privacy protection online," *Computers in Human Behavior*, **28**(3), pp. 1019–1027.

[140] Fogel, J. and E. Nehmad (2009) "Internet social network communities: Risk taking, trust, and privacy concerns," *Computers in Human Behavior*, **25**(1), pp. 153–160.

[141] Krasnova, H. and N. Veltri (2010) "Privacy calculus on social networking sites: Explorative evidence from Germany and USA," in *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*.

[142] Dwyer, C., S. Hiltz, and K. Passerini (2007) "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

[143] Kline, R. (2010) *Principles and practice of structural equation modeling (3rd ed.)*, Guilford Press.

[144] Hoyle, R. (2000) "Confirmatory factor analysis," *Handbook of Applied Multivariate Statistics and Mathematical Modeling*, pp. 465–497.

[145] Cook, T., D. Campbell, and A. Day (1979) *Quasi-experimentation: Design & analysis issues for field settings*, vol. 351, Houghton Mifflin.

[146] Hair, J., W. Black, B. Babin, R. Anderson, and R. Tatham (2006) *Multivariate data analysis*, Pearson Prentice Hall.

[147] Nunnally, J. (1967) *Psychometric theory*, McGraw-Hill.

[148] Campbell, D. and D. Fiske (1959) "Convergent and discriminant validation by the multitrait-multimethod matrix." *Psychological Bulletin*, **56**(2), p. 81.

[149] Fornell, C. and D. Larcker (1981) "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, **18**(1), pp. 39–50.

[150] Suhr, D. (2006) "The basics of structural equation modeling," *University of North Colorado*.

[151] Barrett, P. (2007) "Structural equation modelling: Adjudging model fit," *Personality and Individual Differences*, **42**(5), pp. 815–824.

[152] Hooper, D., J. Coughlan, and M. Mullen (2008) "Structural equation modelling: Guidelines for determining model fit," *Electronic Journal of Business Research Methods*, **6**(1), pp. 53–60.

[153] Hu, L. and P. Bentler (1999) "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A Multidisciplinary Journal*, **6**(1), pp. 1–55.

[154] Hoyle, R. (1995) *Structural equation modeling: Concepts, issues, and applications*, Sage Publications.

[155] Marcoulides, G. and R. Heck (1993) "Organizational culture and performance: Proposing and testing a model," *Organization Science*, **4**(2), pp. 209–225.

[156] Marcoulides, G., C. Emrich, and L. Marcoulides (2008) "Testing for multigroup invariance of the computer anxiety scale," *Educational and Psychological Measurement*, **68**(2), pp. 325–334.

[157] Raykov, T. and G. Marcoulides (2012) *A first course in structural equation modeling*, Routledge.

[158] Arbuckle, J. (2013) *IBM® SPSS® AMOS 22 User's Guide*, IBM.

[159] Ellison, N., J. Vitak, C. Steinfield, R. Gray, and C. Lampe (2011) "Negotiating privacy concerns and social capital needs in a social media environment," in *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web*, Springer, pp. 19–32.

[160] Stutzman, F., J. Vitak, N. Ellison, R. Gray, and C. Lampe (2012) "Privacy in interaction: Exploring disclosure and social capital in Facebook." in *Proceedings of the 6th Annual International Conference on Weblogs and Social Media (ICWSM)*.

[161] Glaeser, E. L., D. I. Laibson, J. A. Scheinkman, and C. L. Soutter (2000) "Measuring trust," *Quarterly Journal of Economics*, **115**(3), pp. 811–846.

[162] Granovetter, M. (1983) "The strength of weak ties: A network theory revisited," *Sociological Theory*, **1**, pp. 201–233.

[163] Ellison, N., C. Steinfield, and C. Lampe (2007) "The benefits of Facebook "friends": Social capital and college students' use of online social network sites," *Journal of Computer-Mediated Communication*, **12**(4), pp. 1143–1168.

[164] Resnick, P. (2001) "Beyond bowling together: Sociotechnical capital," in *HCI in the New Millennium* (J. Carroll, ed.), Addison-Wesley, pp. 247–272.

[165] Burke, M., R. Kraut, and C. Marlow (2011) "Social capital on Facebook: Differentiating uses and users," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 571–580.

[166] Steinfield, C., N. Ellison, and C. Lampe (2008) "Social capital, self-esteem, and use of online social network sites: A longitudinal analysis," *Journal of Applied Developmental Psychology*, **29**(6), pp. 434–445.

[167] Steinfield, C., J. DiMicco, N. Ellison, and C. Lampe (2009) "Bowling online: Social networking and social capital within the organization," in *Proceedings of the International Conference on Communities and Technologies (C&T)*, pp. 245–254.

[168] Ellison, N., C. Steinfield, and C. Lampe (2011) "Connection strategies: Social capital implications of Facebook-enabled communication practices," *New Media & Society*, **13**(6), pp. 873–892.

[169] Burke, M., C. Marlow, and T. Lento (2010) "Social network activity and social well-being," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 1909–1912.

[170] Nissenbaum, H. (2004) "Privacy as contextual integrity," *Washington Law Review*, **79**(1).

[171] Wang, N., P. Wisniewski, H. Xu, and J. Grossklags (2014) "Designing the default privacy settings for Facebook applications," in *Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pp. 249–252.

[172] Pu, Y. and J. Grossklags (2015) "Towards a model on the factors influencing social App users' valuation of interdependent privacy," *Proceedings on Privacy Enhancing Technologies*, **2016**(2), pp. 61–81.

[173] Sheehan, K. B. (1999) "An investigation of gender differences in on-line privacy concerns and resultant behaviors," *Journal of Interactive Marketing*, **13**(4), pp. 24–38.

[174] Van den Broeck, E., K. Poels, and M. Walrave (2015) "Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood," *Social Media + Society*, **1**(2), pp. 1–11.

[175] Hoofnagle, C. J., J. King, S. Li, and J. Turow (2010) "How different are young adults from older adults when it comes to information privacy attitudes and policies?" *Available at SSRN: http://ssrn.com/abstract=1589864*.

[176] Johnson, R. (1974) "Trade-off analysis of consumer values," *Journal of Marketing Research*, pp. 121–127.

[177] DeSarbo, W. S., V. Ramaswamy, and S. H. Cohen (1995) "Market segmentation with choice-based conjoint analysis," *Marketing Letters*, **6**(2), pp. 137–147.

[178] Bech, M., T. Kjaer, and J. Lauridsen (2011) "Does the number of choice sets matter? Results from a web survey applying a discrete choice experiment," *Health Economics*, **20**(3), pp. 273–286.

[179] Wittink, D. and P. Cattin (1989) "Commercial use of conjoint analysis: An update," *The Journal of Marketing*, **53**(3), pp. 91–96.

[180] Burda, D. and F. Teuteberg (2014) "Understanding the benefit structure of cloud storage as a means of personal archiving–A choice-based conjoint analysis," in *Proceedings of the European Conference on Information Systems (ECIS)*.

[181] Wheeler, R. (2010), "Package AlgDesign: Algorithmic experimental design," .

[182] Aizaki, H. and K. Nishimura (2008) "Design and analysis of choice experiments using R: A brief introduction," *Agricultural Information Research*, **17**(2), pp. 86–94.

[183] Rossi, P. and G. Allenby (2003) "Bayesian statistics and marketing," *Marketing Science*, **22**(3), pp. 304–328.

[184] Rossi, P. (2015) "bayesm: Bayesian inference for marketing/micro-econometrics," *URL http://CRAN. R-project. org/package= bayesm. R package version*.

[185] Roth, A. and M. Malouf (1982) "Scale changes and shared information in bargaining: An experimental study," *Mathematical Social Sciences*, **3**(2), pp. 157–177.

[186] Siegel, S. and L. Fouraker (1960) *Bargaining and group decision making: Experiments in bilateral monopoly*, McGraw-Hill.

[187] Train, K. (2002) *Discrete choice methods with simulation*, vol. 8, Cambridge University Press.

[188] Xu, H., T. Dinev, J. Smith, and P. Hart (2011) "Information privacy concerns: Linking individual perceptions with institutional privacy assurances," *Journal of the Association for Information Systems*, **12**(12), p. 798.

[189] Dinev, T. and P. Hart (2004) "Internet privacy concerns and their antecedents-measurement validity and a regression model," *Behaviour & Information Technology*, **23**(6), pp. 413–422.

[190] Milne, G. and M.-E. Boza (1999) "Trust and concern in consumers' perceptions of marketing information management practices," *Journal of Interactive Marketing*, **13**(1), pp. 5–24.

[191] Xu, H. (2007) "The effects of self-construal and perceived control on privacy concerns," *Proceedings of the International Conference on Information Systems (ICIS)*.

[192] Stone, E. and D. Stone (1990) "Privacy in organizations: Theoretical issues, research findings, and protection mechanisms," *Research in Personnel and Human Resources Management*, **8**(3), pp. 349–411.

[193] Güth, W., R. Schmittberger, and B. Schwarze (1982) "An experimental analysis of ultimatum bargaining," *Journal of Economic Behavior & Organization*, **3**(4), pp. 367–388.

[194] Kahneman, D., J. Knetsch, and R. Thaler (1986) "Fairness and the assumptions of economics," *Journal of Business*, **59**(4), pp. S285–S300.

[195] Forsythe, R., J. Horowitz, N. Savin, and M. Sefton (1994) "Fairness in simple bargaining experiments," *Games and Economic Behavior*, **6**(3), pp. 347–369.

[196] Fehr, E., G. Kirchsteiger, and A. Riedl (1993) "Does fairness prevent market clearing? An experimental investigation," *The Quarterly Journal of Economics*, **108**(2), pp. 437–459.

[197] Berg, J., J. Dickhaut, and K. McCabe (1995) "Trust, reciprocity, and social history," *Games and Economic Behavior*, **10**(1), pp. 122–142.

[198] Cooper, D. and J. Kagel (forthcoming), "Other regarding preferences: A selective survey of experimental results," `http://myweb.fsu.edu/djcooper/research/otherregard.pdf`.

[199] Itoh, H. (2004) "Moral hazard and other-regarding preferences," *Japanese Economic Review*, **55**(1), pp. 18–45.

[200] Randall, P. (2013) "Actively caring about the actively caring survey: Evaluating the reliability and validity of a measure of dispositional altruism," *Electronic Theses and Dissertations*.

[201] Braunstein, A., L. Granka, and J. Staddon (2011) "Indirect content privacy surveys: Measuring privacy without asking about it," in *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS)*, ACM.

[202] Greene, K. (2015), "Google faces new privacy class claims over email scanning," `http://www.law360.com/articles/699961`, accessed: 2015-09-11.

Vita

Yu Pu

Yu Pu enrolled in the Ph.D. program in Information Sciences and Technology at the Pennsylvania State University in August 2013. She received the B.S. degree in Economics from Nanjing University, China in June 2012, and the M.S. degree in Information Sciences and Technology from the Pennsylvania State University in August 2015.

Her research has primarily focused on human behavior and behavioral economics, usable privacy and security, third-party apps' privacy issues, online anonymity, and privacy enhancing technologies. Her publications during the Ph.D. study include:

1. **Yu Pu**, and Jens Grossklags. Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter? 2016 (under review).

2. Le Guan, Sadegh Farhang, **Yu Pu**, Jens Grossklags, and Peng Liu. Password Vault + Input Method Editor: Securely Auto-correcting Password Typos for Mobile Phones. 2016 (under review).

3. **Yu Pu**, and Jens Grossklags. Sharing is Caring, or Callous? In *15th International Conference on Cryptology and Network Security (CANS)*, 2016.

4. **Yu Pu**, and Jens Grossklags. Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy. In *16th Privacy Enhancing Technologies Symposium (PETS)*, 2016.

5. **Yu Pu**, and Jens Grossklags. Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios. In *Proceedings of the 36th International Conference on Information Systems (ICIS)*, 2015. (***Media Coverage**: Penn State News*)

6. **Yu Pu**, and Jens Grossklags. An Economic Model and Simulation Results of App Adoption Decisions on Networks with Interdependent Privacy Consequences. In *Proceedings of the 5th Conference on Decision and Game Theory for Security (GameSec)*, 2014.