Yu Pu* and Jens Grossklags

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

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.

We conduct a 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 the monetary value which 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 third-party social app adoption.

We find that individuals' past experiences regarding privacy invasions are negatively associated with their trust for third-party social apps' proper handling of their personal information, which in turn influences their concerns for their own privacy associated with third-party social apps. 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.

Keywords: Third-party Social Apps, Interdependent Privacy, App Data Collection Context, Value of Privacy, Conjoint Analysis, Structural Equation Modeling, Online Survey Study

DOI 10.1515/popets-2016-0005
Received 2015-08-31; revised 2015-11-30; accepted 2015-12-02.

1 Introduction

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 users' personal information. For example, apps are often overprivileged in that they may request access to significantly more information than they need for the stated purposes [18, 33]. It has also been reported that popular apps may transmit users' personal information to various advertising and data tracking firms [100]. In addition, when following the currently utilized notice and consent process, users tend to reveal more information to apps than they desire since most of them have only an incomplete understanding of app permissions management and the potential consequences of granting access to their data [9, 106].

Another problem area is emerging rapidly as a result of the *interdependency of privacy* in many decision-making scenarios. In the context of third-party social apps, the interdependency arises due to users making app adoption decisions which cause the collection and utilization of personal information of their friends. At the same time, affected friends may have only little direct influence to prevent such information flows.

***Corresponding Author: Yu Pu:** College of Information Sciences and Technology, The Pennsylvania State University, E-mail: yxp134@ist.psu.edu

Jens Grossklags: College of Information Sciences and Technology, The Pennsylvania State University, E-mail: jensg@ist.psu.edu

In the broader privacy literature, multiple research projects have investigated users' privacy concerns, and focused on the relationship between users' own privacy concerns and factors such as privacy experience [98], personality differences [4, 73], and behavioral reactions [30]. In the third-party app context, studies have focused on users' understanding of the app permissions process, usability issues, and users' personal privacy preferences [9, 34, 104, 105]. However, the problem space of interdependent privacy has been primarily addressed from a game-theoretic perspective in the app adoption context [10, 89], or in data analytics or genetic privacy scenarios [17, 60]. Our work contributes to a better understanding of interdependent privacy from the perspectives of individuals' perceptions, knowledge and preferences.

To achieve this goal, we conduct a survey study with an online user population. We collect data about individuals' valuations for interdependent privacy by following a conjoint analysis study approach with an experimental manipulation. Our central objective is then 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 structural equation modeling (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.

First, we implement and conduct a 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 [43]. Conjoint analysis studies have been previously used in the context of user privacy in electronic commerce [50, 51] and social network sites [71] 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 [80], 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.

Second, we collect participants' responses to survey measures including users' past privacy invasion experiences, privacy knowledge, trust on 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 third-party 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 third-party social app adoption scenarios.

The remainder of the paper is organized as follows. In Section 2, we review prior literature on the study of privacy concerns and valuations. In Section 3, we discuss the conjoint analysis approach to elicit the values which app users place on their own and their friends' personal information in the context of third-party social app adoption. In Section 4, we describe the SEM model hypotheses, model development methodology, analysis and findings. Finally, we offer a discussion as well as concluding remarks in Section 5.

2 Related work

2.1 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 [97]. Several studies focus on investigating the relationship between a number of antecedents and measures of privacy concerns. For example, Smith et al. [98] 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 [74], has also been found to be one of the factors which impacts consumers' privacy concerns [15]. Researchers also discovered that personality differences, such as the "big-five" personality traits [4], and measures of introversion

versus extroversion [73], 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. [30] find that privacy concern has a significant impact on online purchase intention; Metzger [79] and Xu et al. [109] argue that concern, together with trust, affect individuals' willingness to disclose information to others. In addition, taking a policy perspective, Metzger [79] and Turow et al. [103] 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 [11, 12].

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.

2.2 Value of privacy

Viewing privacy as an economic good [68], 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 [21, 26, 59, 97]. This viewpoint is adopted in several works on privacy issues [26], 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 [46].

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 [16]. Similarly, responses from a survey including questions on disclosure of personal information to commercial entities have been used to measure privacy values [107].

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 [99]. For example, Beresford et al. [8], Jentzsch et al. [62] and Tsai et al. [102] find that consumers are willing to pay a (typically small) premium in order to purchase more privacy-friendly products; Grossklags and Acquisti [45] 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. [58] apply second-price auctions to measure the perceived value of individuals' weight and height information. Using a related methodology, Danezis et al. [23] 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 [2].

A different set of studies use discrete choice experiments to understand the valuation of privacy. Applying this method, Potoglou et al. [88] 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 [31] and Krasnova et al. [69] 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 [50, 51]; also in the scenario of SNS [71]. These researchers also derived the monetary value of an individual's personal information [50, 51, 71].

With the current research, we extend our previous work which adopts a conjoint analysis approach to quan-

tify the value which users (who consider adopting an app) place on their own personal information, as well as their friends' personal information [90]. Compared to Pu and Grossklags [90], we improve the online survey methodology to include a screening task for improved data quality. Although the concrete measured magnitude of monetary valuations, as well as the measured effects with respect to data collection context vary slightly from the earlier work [90], our current study generally confirms our previous findings. For example, we also report that an impact of data collection context on the valuation of interdependent privacy regarding app adoption is observable, but surprisingly weak. Most importantly, our current paper is not focused on the mere determination of the monetary value of interdependent privacy. Instead, we evaluate the responses to an online survey with measures including users' past privacy invasion experiences, privacy knowledge, trust on apps' data practices, online social capital, as well as privacy concerns for both themselves and their friends regarding app adoption. By carefully developing a set of hypotheses and conducting a SEM analysis, we work towards a model to comprehensively explain users' privacy evaluation process in the third-party social app adoption context.

3 Conjoint analysis to determine privacy value

3.1 Design of conjoint study

Conjoint analysis assumes that consumers view a product as a bundle of certain features (*attributes*), which have different values (*levels*) [42]. 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 third-party 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 Determination of attributes and their levels

Following Green and Krieger's suggestions [40], we conducted semi-structured interviews with third-party 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 [47], 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 high and modest levels of popularity as typical cases.

We selected levels for *own privacy* and *friends' privacy* by investigating app permission systems. Wang et al. [104] found that all Facebook apps collect a users' basic information such as user name and ID, and some of them request additional 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",

Table 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

"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 1.

3.1.2 Selection of survey stimuli

We used a full-profile approach to conduct the conjoint analysis study which requires respondents to rank a set of product profiles (*stimuli*) [41]. 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 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.

3.1.3 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:

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

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.

3.2 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.

3.2.1 Screening task

Although compared with traditional laboratory studies, MTurk enjoys several advantages such as more diverse demographics [61, 64] and lower payments [77], 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 [28]. 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 [28, 38]. Downs et al. encourage to apply a screening process to remove the subset of Turkers who do not complete tasks conscientiously [28]. 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 the figure in Appendix A). 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.

3.2.2 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 third-party 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:

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 third-party 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 on 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 4.1 and 4.2, respectively. The exact questions are provided in Appendix C.

3.2.3 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 Appendix A 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 Appendix B 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 our university's IRB.

3.3 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. 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.

3.4 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 1) of each app attribute level. In Table 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, 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 3.3, we did not include such cases in our analysis.

From Table 3, we observe that under the scenario of third-party 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

Table 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

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 third-party 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 finding that most friendship ties are weak on SNSs [24].

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. 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 [7].

From Table 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 [18, 33].

Complementing previous studies suggesting that privacy concern and privacy disclosure are influenced by contextual cues that are negatively related to objective dangers of disclosure [63], 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.

4 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 third-party 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 [94], we are able to compare such associations among the different app data collection contexts.

4.1 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 [14]. One generally expected social contract is that these parties will be responsible for properly managing individuals' personal information [87]. These expectations relate to trust, which is the belief that these parties will behave in a socially responsible manner,

Table 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

and will fulfill the trusting party's expectations without taking advantage of any vulnerabilities [37, 78]. Prior research shows that when consumers think their personal information has been misused, they may consider this as an implied breach of contract [22, 87] 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 [85]. Further, individuals who have been victims of personal information abuse might be more aware of which actions could lead to privacy invasions [1] 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 third-party 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 [53]. Studies from other settings also argue that trust can enhance the evaluation of benefits and mitigate privacy concerns [84]. In fact, trust gives users a feeling that they will gain the benefits they expect without suffering negative consequences [84]. 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 [81]. 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 [49, 65]. Online social capital, which refers to immaterial resources accumulated through the relationships among people [19], often yields positive outcomes to individuals. For example, it provides emotional support for individuals [5, 52], it increases individuals' chances of exposure to diverse ideas [86], and it offers opportunities for individuals to get access to non-redundant information [39].

Putnam further classified online social capital into two categories: bridging social capital and bonding social capital [91]. These two types of social capital are not mutually exclusive and provide benefits to individuals from different perspectives [91]. According to Putnam, *bridging social capital* is created when individu-

als 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 [108]. 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 [108].

Through their interactions with online community members, third-party 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 third-party 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 third-party 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 [25, 93]. 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:

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 1. 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.

4.2 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. [98]. 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. [83]. To address the elements of trust in third-party social apps, we used a shortened 4-item version of trust measures from Fogel and Nehmad [35], Krasnova and Veltri [72], and Dwyer et al. [29]. Corresponding to

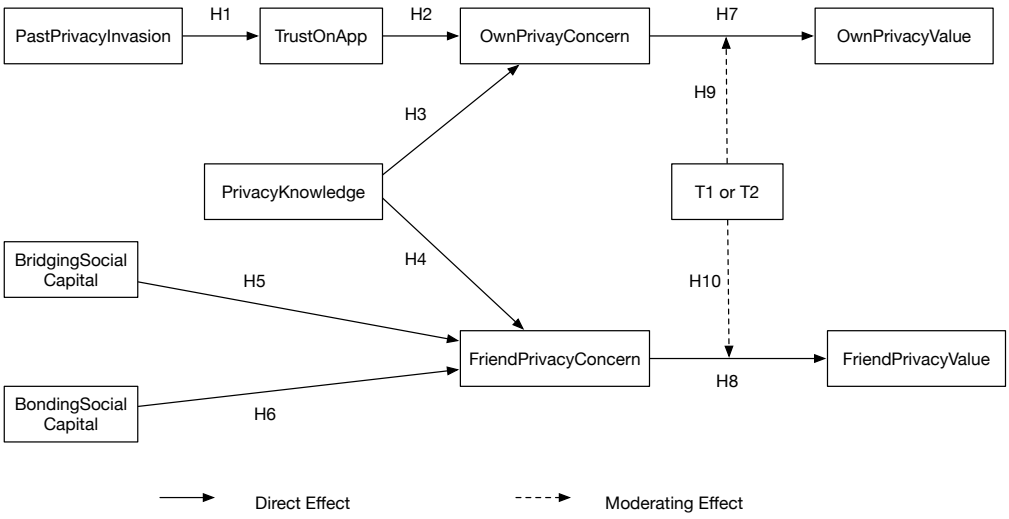


Fig. 1. The conceptual model

four questions to measure own privacy concern, which were modified from Smith et al. [98], 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 [108]. 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., third-party social app adoption. All items were measured on a Likert-type scale with 1 = strongly disagree to 5 = strongly agree. Appendix C 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.

4.3 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 [56, 67]. In the following, we show the details for our tests of the measurement model and path model.

4.3.1 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 [20]. 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. [48] recommended an acceptance level of 0.7 for the composite reliability, and Nunnally [82] also proposed 0.7 as an indication of an adequate value for Cronbach's alpha. We show the test results in Table 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

Table 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

other [13]. Following the criteria suggested by Fornell and Larcker [36], 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 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.

4.3.2 Tests of path model

4.3.2.1 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 [101]. 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 exceeding 0.05 indicates the model is a good fit (i.e., significance might indicate a bad fit) [6]. Since the chi-square test is sensitive to sample size, other descriptive measures of fit are often used in addition to chi-square tests [54]. 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 [57]. 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 [57]. In our paper, 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.

4.3.2.2 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 [55]. We present the results in Table 5.

Our results indicate that in both treatments, past privacy invasion experiences are negatively and signifi-

Table 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 supported in T2
H4: PrivacyKnowledge → FriendPrivacyConcern	0.12	0.69^{***}	Partially supported in T2
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

cantly 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).

4.3.2.3 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* [76, 94]. 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 [75]. 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 [92].

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 [3]. 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 [3]. 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,

Table 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)

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 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.

4.4 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 third-party 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 third-party 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 [96]. 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 third-party 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.

5 Conclusions

Our paper 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 conjoint study, we quantify the economic value individuals place on both their own and friends' information in third-party 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 [80], 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.

There are several limitations of this study, some of which present useful opportunities for further research. The first limitation relates to our SEM model. As mentioned earlier, the three factors that we hypothesized as antecedents of interdependent privacy concerns regarding app adoption, namely privacy knowledge, bridging and bonding social capital, are either only partly confirmed or unconfirmed. As such, additional work is needed to further identify and investigate factors that contribute to the concern for friends' privacy in this particular scenario. Further, our model offers insufficient explanations about the formation of the valuation of interdependent privacy in the context of app adoption. In other words, besides privacy concerns for friends' data, other potentially important factors that might affect how individuals value their friends' information are missing in our current research framework, and hence need further investigation. Future work should also consider direct behavioral measures of interdependent privacy valuations to account for a potential discrepancy between survey measures and actual behaviors [1, 99]. Secondly, the problem of interdependent privacy is also common in other contexts such as SNSs [70, 95] and email service [44]. However, 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. Finally, as with other studies in a specific geographical setting, our research focuses on individuals living in the United States. However, according to prior research [72, 102], 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.

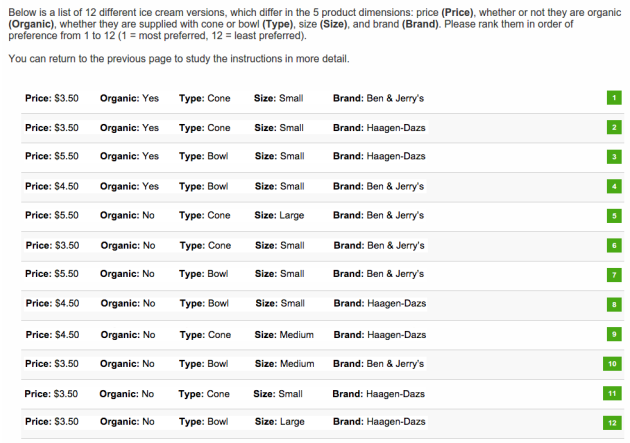
Our results also provide motivation for extending our previously proposed economic model of app adoption to better understand the impact of interdependent privacy on user behaviors [89]. For example, we plan to integrate the factor of app data collect context into the model, as well as to simulate the model with empirical data, such as the value of interdependent privacy.

We believe our study fills an important void in the broader technology policy discussion on privacy, and more specifically regarding the interdependent privacy consequences of third-party social app adoption decisions. Presenting privacy information in a cleaner fashion to users when they are making adoption decisions can assist users in choosing less privacy-invasive apps [66, 104]. Therefore, privacy advocates should push app developers to revise apps' privacy notice dialogues so that they explicitly inform users whether apps' practices of collecting data, especially the data about friends' full profiles, 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 [27, 32]. In addition, our work suggests online social capital does not contribute to the formation of interdependent privacy concerns. In other words, how individuals care about others is not impacted by individuals' fear of losing reputation or online social capital, which might in turn further reduce individuals' incentives to care about their friends' privacy. As such, relying on SNS users to protect their friends' privacy is likely not adequate. Thus, it may be necessary to limit the data sharing of friends' information, or to increase the involvement of users in the decision-making process over information sharing initiated by others.

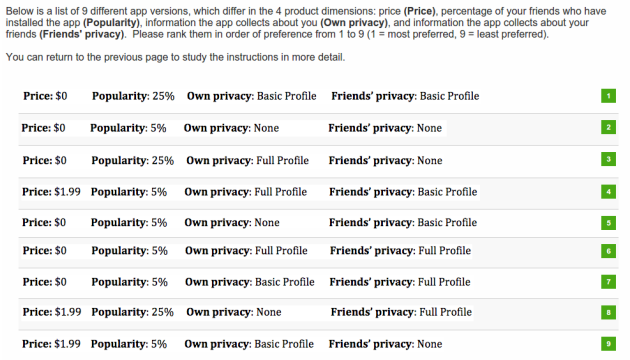
Acknowledgments

We appreciate the detailed comments of the anonymous reviewers, Dali Kaafar (our shepherd), and the PETS program chairs. We further thank Mary Beth Rosson and Mary Beth Oliver for their feedback during an earlier stage of the research. We also thank for the support through a seed grant of the College of Information Sciences and Technology at the Pennsylvania State University.

Appendix A Ice Cream Ranking Interface



Appendix B App Ranking Interface



Appendix C Survey Instrument

PrivacyKnowledge:

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:

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:

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:

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.

OwnPrivacyConcern:

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:

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:

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.

References

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

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

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

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

[5] J. Bargh and K. McKenna. The Internet and social life. *Annual Review of Psychology*, 55:573–590, 2004.

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

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

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

[9] A. Besmer and H. Lipford. Users' (mis)conceptions of social applications. In *Proceedings of Graphics Interface (GI)*, pages 63–70, 2010.

[10] G. Biczók and P. Chia. Interdependent privacy: Let me share your data. In A.-R. Sadeghi, editor, *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 338–353. Springer, 2013.

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

[12] R. Böhme and J. Grossklags. Trading agent kills market information: Evidence from online social lending. In *Proceedings of the 9th Conference on Web and Internet Economics (WINE)*, pages 68–81, 2013.

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

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

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

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

[17] M. Chessa, J. Grossklags, and P. Loiseau. 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)*, pages 90–104, 2015.

[18] P. Chia, Y. Yamamoto, and N. Asokan. 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)*, pages 311–320, 2012.

[19] J. Coleman. Social capital in the creation of human capital. *American Journal of Sociology*, 94:S95–S120, 1988.

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

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

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

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

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

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

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

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

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

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

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

[31] S. Egelman. 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)*, pages 2369–2378, 2013.

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

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

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

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

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

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

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

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

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

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

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

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

[44] K. Greene. Google faces new privacy class claims over email scanning. http://www.law360.com/articles/699961, 2015. Accessed: 2015-09-11.

[45] J. Grossklags and A. Acquisti. 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)*, 2007.

[46] J. Grossklags and N. Barradale. Social status and the demand for security and privacy. In E. De Cristofaro and S. Murdoch, editors, *Privacy Enhancing Technologies*, volume 8555 of *Lecture Notes in Computer Science*, pages 83–101. Springer, 2014.

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

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

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

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

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

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

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

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

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

[56] R. Hoyle. Confirmatory factor analysis. *Handbook of Applied Multivariate Statistics and Mathematical Modeling*, pages 465–497, 2000.

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

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

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

[60] M. Humbert, E. Ayday, J.-P. Hubaux, and A. Telenti. On non-cooperative genomic privacy. In R. Böhme and T. Okamoto, editors, *Financial Cryptography and Data Security*, volume 8975 of *Lecture Notes in Computer Science*, pages 407–426. Springer, 2015.

[61] P. Ipeirotis. Demographics of Mechanical Turk. Technical report, Social Science Research Network, Technical Report No. 1585030, 2010.

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

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

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

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

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

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

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

[69] H. Krasnova, N. Eling, O. Abramova, and P. Buxmann. 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)*, 2014.

[70] H. Krasnova, N. Eling, O. Schneider, H. Wenninger, and T. Widjaja. 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)*, 2013.

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

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

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

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

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

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

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

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

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

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

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

[82] J. Nunnally. *Psychometric theory*. McGraw-Hill, 1967.

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

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

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

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

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

[88] D. Potoglou, S. Patil, C. Gijón, J. F. Palacios, and C. Feijóo. 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)*, 2013.

[89] Y. Pu and J. Grossklags. An economic model and simulation results of app adoption decisions on networks with interdependent privacy consequences. In R. Poovendran and W. Saad, editors, *Decision and Game Theory for Security*, pages 246–265. Springer, 2014.

[90] Y. Pu and J. Grossklags. 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)*, 2015.

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

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

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

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

[95] P. Shi, H. Xu, and Y. Chen. 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)*, pages 35–38, 2013.

[96] A. Smith. 6 new facts about Facebook. http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/, 2014. Accessed: 2015-09-09.

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

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

[99] S. Spiekermann, J. Grossklags, and B. Berendt. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, pages 38–47, 2001.

[100] E. Steel and G. Fowler. Facebook in privacy breach. http://www.wsj.com/articles/SB10001424052702304772804575558484075236968, 2010. Accessed: 2015-09-13.

[101] D. Suhr. The basics of structural equation modeling. *University of North Colorado*, 2006.

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

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

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

[105] N. Wang, P. Wisniewski, H. Xu, and J. Grossklags. 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*, pages 249–252, 2014.

[106] N. Wang, H. Xu, and J. Grossklags. 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)*, pages 4:1–4:10, 2011.

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

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

[109] H. Xu, H.-H. Teo, and B. Tan. 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)*, 2005.