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

Yu Pu, ***The Pennsylvania State University;*** **Jens Grossklags,** ***Technical University of Munich***

https://www.usenix.org/conference/soups2017/technical-sessions/presentation/pu

This paper is included in the Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).

July 12–14, 2017 • Santa Clara, CA, USA

ISBN 978-1-931971-39-3

Open access to the Proceedings of the Thirteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

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

Yu Pu
Security, Privacy and
Information Economics Lab (SPIEL)
The Pennsylvania State University

Jens Grossklags
Chair for Cyber Trust
Department of Informatics
Technical University of Munich

ABSTRACT

Through their third-party app installation decisions, users are frequently triggering interdependent privacy consequences by sharing personal information of their friends who are unable to control these information flows. With our study, we aim to quantify the value which app users attribute to their friends' information (i.e., value of interdependent privacy) and to understand how this valuation is affected by two factors: sharing anonymity (i.e., whether disclosure of friends' information is anonymous), and context relevance (i.e., whether friends' information is necessary for apps' functionality). Specifically, we conduct a between-subject, choice-based conjoint analysis study with 4 treatment conditions (2 sharing anonymity $\times$ 2 context relevance). Our study confirms the important roles that sharing anonymity and context relevance play in the process of interdependent privacy valuation. In addition, we also investigate how other factors, e.g., individuals' personal attributes and experiences, affect interdependent privacy valuations by applying structural equation modeling analysis. Our research findings yield design implications as well as contribute to policy discussions to better account for the problem of interdependent privacy.

1. INTRODUCTION

The vast majority of published research on privacy-decision making focuses on individual choices regarding personal privacy. However, with the accelerating usage of Social Network Sites (SNSs), mobile platforms and other digital advances with interactive tools, we observe the increasing relevance of decisions which affect others' information. These *interdependent privacy* choices involve scenarios in which a decision-maker has power over the sharing of personal information about other individuals, which are often friends, family members or colleagues. Previous work has studied this problem space from a theoretical [11, 80] and behavioral perspective [83]. A key finding is that individuals exhibit behaviors which can be interpreted as *privacy egoism*: they value their own information much higher than the information of a friend [83]. From a theoretical perspective, this phenomenon can be explained with the economic concept of negative externalities, i.e., individuals do not bear the (privacy) cost that they impose on others [11].

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

We consider the scenario of third-party app adoption on SNSs where users are presented with app offers and associated authorization dialogues which may trigger sharing decisions over their own personal information and their friends' personal information [107]. For example, an app may request to access not only users' own data, but also information about their friends. In practical settings, the ability of an affected individual to learn about others' sharing decisions is quite modest. For example, users may be subjected to social app advertisements and may indirectly learn that a friend has adopted an app which triggers the sharing of friends' information.[1] We focus on studying the impact of this veil of anonymity (as well as its counterpart full identifiability) of sharing decisions.

To address our research question, our first step is to quantify the interdependent privacy value by applying the methodology of conjoint analysis. In our previous work [83], we conducted a full-profile conjoint study to determine this value, and we use this study setup as a starting point for the current investigation. However, due to a high cognitive challenge presented by the full-profile method, alternative approaches should be taken to address low data quality (see Appendix A). To respond to this data quality concern and to improve on our previous work, we utilize a different methodology, i.e., choice-based conjoint analysis, to determine interdependent privacy valuations. Further, we introduce, in the choice-based conjoint study, four treatment scenarios which differ in whether or not sharing friends' data is anonymous (*sharing anonymity*[2]) and whether or not the requested friends' data is useful to app's functionalities (*context relevance*). This allows us to examine how sharing anonymity and context relevance affect app users' valuation towards their friends' data.

[1] In the mobile app context even such spurious cues may not exist when a user shares an address book or other data type containing friends' data. Likewise, in the context of genetic privacy there is no mechanism that automatically informs other family members about the decision by one individual to take a test [109].

[2] To clarify, sharing anonymity does not mean that an app user shares anonymized friends' data. Instead, it indicates the situation where it is hard for friends to identify the person that released their information to apps.

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

In order to comprehensively explain the valuation of friends' information, our second step is then to apply Structural Equation Modeling (SEM) analysis to investigate how interdependent privacy values are influenced by factors such as *other-regarding preferences* (see details in later sections), privacy knowledge, privacy concern, and the treatment conditions, i.e., sharing anonymity and context relevance.

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

These results offer valuable insights into the problem of interdependent privacy, which are directly applicable to privacy by design or re-design initiatives [41, 116]. More specifically, our study conveys that design features helping to raise individuals' interdependent privacy concerns will also impact individuals' valuation of friends' personal information. But additional ways to protect friends' privacy emerge which can be used by interface designers and information architects. First, making the sharing of friends' data identifiable is a viable approach to erect a psychological hurdle against unfettered bulk data sharing with third parties as often triggered by app adoption. Second, informing app users when data collection is not contextually relevant also influences privacy valuations significantly. Computer scientists work on automating the analysis of contextual relevance in the app context by identifying over-privileged apps [28, 32, 46], which makes the implementation of related design features during the app selection process viable. In addition, our research findings also emphasize the important roles of governmental interventions and privacy education in protecting friends' privacy in the context of app adoption.

Roadmap: We proceed as follows. In Section 2, we discuss related work on the role of anonymity in individual decision-making. We further summarize extant work on the value of personal information, and the modeling of privacy decision-making. In addition, we also review existing work on resolving interdependent privacy conflicts. Next, we present the choice-based conjoint analysis approach, and the associated results in Section 3. In Section 4, we discuss the development and results for the behavioral model based on SEM. Finally, we discuss our findings in Section 5, and offer concluding remarks in Section 6.

2. RELATED WORK

2.1 Anonymity in Individual Decision-Making

A set of studies in the area of experimental economic research has focused on the influence of anonymity on decision-making. In particular, the experimental literature on economic bargaining games which mostly centers on the analyses of the so-called ultimatum [42] and dictator games [60] is of high relevance. In the classical version of both games, a monetary amount (i.e., pie) is offered for allocation between two individuals. One person acts as the proposer and can suggest a split of the pie. In the ultimatum game, the recipient of the proposal can reject the offer (then the money will remain with the experimenter) or accept the split [42]. In contrast, in the dictator game the recipient has no decision-making power (and the pie is allocated according to the proposed split) [60]. A specific sub-area of this literature is addressing the impact of anonymity from two perspectives: 1) anonymity between proposer and recipient, 2) anonymity between players and experimenter (i.e., double-blind).

Radner and Schotter compare face-to-face (F2F) bargaining with anonymous bargaining and find that the latter was associated with an increase in rejected proposals, while the former was associated with an almost uniform acceptance rate [85]. Prasnikar and Roth report similar results [78]. However, they also find that F2F communications that explicitly exclude any form of conversation about the relevant bargaining aspects and are merely social in nature, also contribute to an almost uniform acceptance rate of proposals which were later issued without additional F2F exchanges [78]. During the latter treatment, participants were required to learn the name and education level of their bargaining opponents. The finding of this social conversation treatment was interpreted to confirm that social pressures arising from F2F are influencing subjects; rather than the discussion of any pertinent aspects of the transaction [89]. Similarly, Charness and Gneezy conduct dictator and ultimatum game experiments in which they compare treatments in which participants were informed about the family names of their counterparts (or not) [18]. This manipulation strongly impacted the generosity of proposers in the dictator game, but not the initial offer of the proposers in the ultimatum game where strategic considerations seemed to prevail [18]. Hoffman et al. introduced a double-blind setup in which the experimenter could not identify the experimental participants [48]. The results indicate that this double-blind setup was associated with the most selfish offers by the proposers. Experiments have also been conducted in the field to document the negative impact of anonymity on donations for environmental causes [5] or in churches [96].

In addition, a stream of research in the field of information system investigates the impact of anonymity on individuals' self-disclosure on social network sites. These studies mainly focus on two types of anonymity: discursive anonymity and visual anonymity. Discursive anonymity refers to the extent to which information can be linked to a particular source [92], whereas visual anonymity indicates the degree to which others can see and/or hear the person who discloses the information [92]. Although focusing on this topic for more than a decade, researchers have not reached an agreement on either the impact of discursive anonymity or the influence of visual anonymity on self-disclosure. For example, Qian and Scott [84] report a positive relationship between self-disclosure and discursive anonymity. However, this association is found to be negative by Hollenbaugh and Everett [49]. When it comes to visual anonymity, some studies claim that it is positively related to self-disclosure [59, 49], while other research fails to detect such an association [84]. These contradictory empirical findings suggest that the relationship between anonymity and self-disclosure in online social networks is still in question and should be further examined [49].

Closely related to our work, some studies explore the impact of anonymity on individuals' privacy attitudes or privacy behaviors. In particular, through an empirical study, Jiang et al. [57] report that when individuals perceive themselves to be unidentifiable, they feel less concerned about their privacy. In addition, they find that individuals exhibit higher levels of concern about their own privacy when other parties' identities are anonymized. However, we are still unaware of any research that directly addresses how anonymity impacts individuals' attitudes towards others' privacy. Our study addresses this literature gap by exploring the impact of anonymity on the valuation of interdependent privacy.

2.2 Economic Value of Privacy

Several research projects explore the value of personal information which is also a central aspect of our study. For example, situating individuals in a second-price auction scenario, Huberman et al. elicit monetary valuations for individuals' weight and height (which were previously recorded) [54]. They find that deviation from a perceived population standard drives higher valuations. A similar approach is used to derive how individuals value information about their location traces [24].

In various experiments, participants are presented with situations in which they trade off privacy for better recommendations [97], a discount on a product purchase [3, 105], or a pure monetary reward [79]. In contrast, the willingness to pay to protect information, or to purchase a higher-priced option with privacy-friendlier terms is often reported to be low [9, 38, 79], though there are exceptions [31]. Other research shows that individuals associate little value with their own information on social network sites (when faced with the threat of deletion) [7].

Taking a different viewpoint, Acquisti and Grossklags as well as Grossklags and Barradale investigate how privacy and security preferences relate to financial preferences (e.g., discounting behaviors) [1, 39]. Böhme and Grossklags study how privacy norms shift on a micro-lending platform, when platform mechanisms for borrower-lender matching shift away from placing focus on personal descriptions provided by borrowers [12].

Several researchers have conducted studies with conjoint analyses beginning with Hann et al. [44, 43]. More recently, Krasnova et al. used this methodology to understand privacy concerns in SNS settings [62]. Common to these works is that they also determine the monetary value of personal information.

In our previous work, we determined the monetary value of personal and interdependent privacy by applying the conjoint study methodology [81, 83, 82]. We replicate the utilized basic scenario to conduct the conjoint study in this paper [83], however, we add as an additional treatment condition whether (or not) anonymity of sharing decisions over friends' information is provided. In addition, we utilize a different methodology by applying choice-based conjoint analysis to address data quality concerns from the full-profile method applied in our previous work [83].

2.3 Explaining Value of Privacy

In our work, we also aim to develop an explanatory model for the valuation of personal and interdependent privacy as measured with the conjoint study methodology.

Several related studies have focused on utilizing concerns for personal privacy as a key construct which is also part of our explanatory model [94]. We also draw on published works about antecedents of personal privacy concerns, for example, research which utilizes past privacy invasions as an explanatory factor for personal privacy concerns [95].

A number of models focus on effects of personal privacy concerns, for example, by trying to explain purchase intentions [30] or disclosure behaviors [65]. In contrast, our paper is focused on explaining personal and interdependent privacy *valuations* as in our previous work [83]. However, our behavioral model substantially differs by considering the explanatory effects of other-regarding preferences [22], perceived control [27], and disposition to value privacy [115]; in addition, our center of interest is to build a model to explain different treatment conditions regarding anonymity. We will detail the building blocks of our model in Section 4.1.

2.4 Resolve Interdependent Privacy Conflicts

Privacy conflicts may arise in interdependent privacy scenarios, where privacy preferences of those who share others' data and those whose information is leaked are not aligned. These privacy conflicts are referred to as multi-party privacy conflicts (MPCs) [103]. Several research projects explore how to resolve conflicts arising from interdependent privacy issues in social media, although not in the scenario of social app adoption. A stream of these studies focuses on providing computational mechanisms or external tools to deal with MPCs. For example, in the scenario of photo sharing on social network sites, a system has been proposed so that when a user is tagged in a photo, he/she can send privacy suggestions or feedback to those who upload the photo [10]. Also in the scenario of photo sharing, Ilia et al. [56] introduce a mechanism of blurring faces of individuals (who appear in photos) based on a users' access control permissions.

To provide support for users to resolve MPCs, some studies propose sharing policies based on aggregated individual privacy preferences. For example, Hu et al. [51] formulate an access control model, multi-party policy specification scheme, and a policy enforcement mechanism to facilitate collaborative management of shared data. Thomas et al. [103] demonstrate how Facebook's privacy model can be adapted to enforce multi-party privacy. Similarly, other mechanisms or access control policies have been introduced in [15, 101] to address MPCs.

Other researchers try to study MPCs from the perspective of game-theoretic analysis. For example, Hu et al. [52] study a multi-party access control model to investigate systematic approaches to identify and to resolve conflicts of collaborative data sharing. Similarly, a negotiation mechanism is introduced and examined to help users to reach an agreement in scenarios with MPCs [102].

There is another stream of studies which explores strategies users have utilized to resolve MPCs. Wisniewski et al. [112] demonstrate that individuals use both online strategies, such as untagging, and offline strategies, such as negotiating offline with affected others, before posting photos. In addition, they also investigate how support mechanisms that are provided by social media interfaces are used by individuals for addressing MPCs [111]. They conclude that these mechanisms are ineffective, difficult to use, and not easy to be aware of, and therefore users are more likely to apply offline coping strategies.

Conducting a qualitative study with 17 individuals, Lampinen et al. [64] discover that users apply a range of preventive strategies to avoid causing problematic situations for others. In particular, they categorize 4 types of strategies: preventive, corrective, individual, and collaborative. Similarly, Cho and Filippova [20] identify the same types of strategies based on findings from focus-group interviews and online surveys.

In practice, we would expect that individuals would regret many app adoption decisions, when they revisit apps' privacy practices or suffer from conflicts with their friends [34].

Finally, outside the context of SNSs, Harkous and Aberer investigate sharing practices on cloud storage platforms involving the access of third-party cloud storage apps to users' data repositories by conducting measurements and user studies [45].

In aggregate, most of these studies investigate different ways of resolving privacy conflicts that arise from interdependent privacy issues in social networks. However, we are unaware of any research

that directly explores MPCs in the context of social app adoption. Our research provides insights for dealing with such privacy conflicts.

3. CONJOINT ANALYSIS TO DETERMINE PRIVACY VALUE

3.1 Design of Choice-based Conjoint Study

Conjoint analysis is a general approach for analyzing consumer preferences for multi-attribute products and services [37]. In a conjoint analysis study, it is often assumed that consumers view a product as a bundle of certain features (*attributes*), which have different values (*levels*) [36]. Through testing and analyzing individuals' preferences for multiple versions of a product (*profiles*), researchers are able to decompose the overall utilities of different product versions, and hence understand the role which each attribute plays in individuals' decision-making [58].

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

3.1.1 Determination of Apps' Attributes and Levels

Through conducting 18 semi-structured interviews with app users, we identified in our previous work [83] four attributes that are most frequently regarded as relevant to the choice of third-party apps. In addition, the interview results also helped to determine levels of these four app attributes. To allow for a direct comparison of results, we applied these insights also to the current context. In other words, we used the same app attributes and levels [83] which are summarized in Table 1.

3.1.2 Selection of Conjoint Analysis Method

There are two popular ways to conduct conjoint analyses: full-profile conjoint analysis and choice-based conjoint analysis. Typically, in a full-profile conjoint study, participants are asked to rank several versions of a product which differ regarding multiple attributes (see an example in Appendix A). Considering that each attribute has multiple levels, ranking even a small number of product versions represents a very high cognitive challenge to respondents [36]. Therefore, as is demonstrated in our previous research [81, 83], full-profile conjoint analysis studies include a non-trivial share of participant responses with low quality.

To address this problem, we decided to apply the methodology of choice-based conjoint analysis. In a choice-based conjoint study, respondents are asked to choose an alternative from a small set (normally 2 or 3) of profiles (*choice set*) [25] (see Figure 1). Participants then repeat this task for a limited number of choice sets, thereby providing adequate data for analysis. As a result, compared with full-profile conjoint analysis, the choice-based method poses less cognitive challenges to participants. We expect that by choosing this approach, we can obtain significantly higher quality responses.

3.1.3 Selection of App Profiles

We next discuss how to determine the number of choice sets to be included in the study. While there is no clear guidance on this issue, prior studies indicate that respondents are capable of managing 17 choice sets without problems [8], and a study on the commercial use of conjoint analysis reported a median value of 16 choice sets in typical conjoint study designs [113]. Based on these results, we included 16 choice sets in our study. Note here, in order to check for consistency of participants' responses, we set two choice sets to be the same. Therefore, our study included 15 distinct choice sets.

We adapted R code provided by Burda and Teuteberg [13] to create choice scenarios (choice sets) in our study. Specifically, with the help of the Algorithmic Experimental Design R package [110], we calculated a fractional factorial design from our full factorial design ($2 \times 2 \times 3 \times 3 = 36$ stimuli) by following a 5-step procedure described in [4]. Using this method, we derived a design including 15 different app profiles which were randomly combined to form the choice sets. In addition, in order to make the scenario more realistic, we also introduced the "no choice" option in each choice set. Therefore, we generated 15 different choice sets, with each of them including two app profiles and one "no choice" option.

3.1.4 Estimation of Conjoint Model

Hierarchical Bayes (HB) estimation takes into consideration that individuals have heterogeneous preferences for product-specific attributes and is generally preferred for analyzing choice-based conjoint models [88]. Without treating all individuals alike, the HB method allows not only for estimating a conjoint model on an aggregate level, but also for calculating parameter estimates associated with specific individuals, i.e., individual-level part-worth utilities. We further utilize the R package Bayesm [87] to conduct the HB estimation and to analyze our choice-based conjoint model.

3.2 Design of Survey Experiment

3.2.1 Treatments

Prior research indicates that individuals behave differently when anonymity is preserved than under circumstances with full information; in this case, identifiability and observability. We reviewed this literature in the related work section, but briefly summarize several results here. For example, by comparing results of F2F bargaining and anonymous bargaining in a classic behavioral experiment that aims to understand how agents cooperate with each other, Radner and Schotter find that F2F bargaining captured a higher percentage of gains from trade than anonymous bargaining [85]. Similarly, in another pair of comparative experiments, Roth and Malouf observe fewer equal splits and more disagreements in anonymous bargaining than in the F2F setting [90]. Interpreting these results, Siegel and Fouraker acknowledge that small differences in the social environment (such as the provisioning of anonymous communications) might lead to a large divergence in behavior [93]. Therefore, they argue that social variables, in particular anonymity, should either be systematically studied or controlled in behavioral experiments [93].

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

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

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

In addition, previous studies reveal that individuals' privacy con-

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

Table 1: Summary of attributes and levels

cerns are influenced by whether or not information requests are context-relevant [68]. For example, Wang et al. [108] discover that while app users are typically unconcerned about giving away birthday information to a calendar app, they become uncomfortable when the app wants to collect information that is unrelated to the app's stated purpose. Motivated by the theory of contextual integrity [68] and the aforementioned empirical results, we also aim to explore how app data collection context impacts the value which app users place on their friends' information.

To this end, similar to how we account for sharing anonymity, we introduced the following 2 treatment scenarios regarding *context relevance*:

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

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

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

3.2.2 Procedure

After consenting to take part in the study, participants were randomly placed into one of the 4 treatments, and were provided with task instructions, where we offered definitions of app attributes and their corresponding levels. Next, they were presented with 16 questions (see Figure 1 for the app choice interface), which corresponded to the 16 choice sets in the conjoint analysis study. In each question, they were required to select their favorite alternative from two app versions and a "no choice" option. When participants selected a "no choice" option, it indicated that neither of the two provided app versions were preferred by them. Note here, in order to ensure that definitions of app attributes and levels were well conveyed to participants, we allowed them to revisit the instruction page during each app choice task.

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

3.2.3 Recruitment and Ethical Considerations

We recruited participants from Amazon Mechanical Turk, a recruitment source that is popular for conducting online user experiments [35]. We restricted participation to Turkers who had completed over 50 Human Intelligence Tasks (HITs) with a HIT approval rating of 97% or better, as well as those who had United States IP addresses. In addition, eligible participants should have previously installed at least one app on their social network sites, so that they were familiar with the scenario setting of our study. We paid $1.50 to each participant after they completed the task.

Our study followed a protocol reviewed and approved by the IRB of the Pennsylvania State University. In addition, our survey-based investigation did not raise any significant ethical issues since it was a standard consumer study with an established study methodology and hypothetical choice situations, and it did not involve any deception.

3.3 Results of Choice-based Conjoint Study

3.3.1 Participant Data

Our survey study was conducted in September 2016. We collected a total of 1007 responses. After filtering out data based on conditions such as whether participants are US citizens, whether responses pass the check conditions implemented in the survey, and whether responses result in privacy values that are not outliers[3], our final sample included responses of 931 participants for data analysis. By comparing percentages of low quality responses between the current study and our prior work [83], we believe that

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

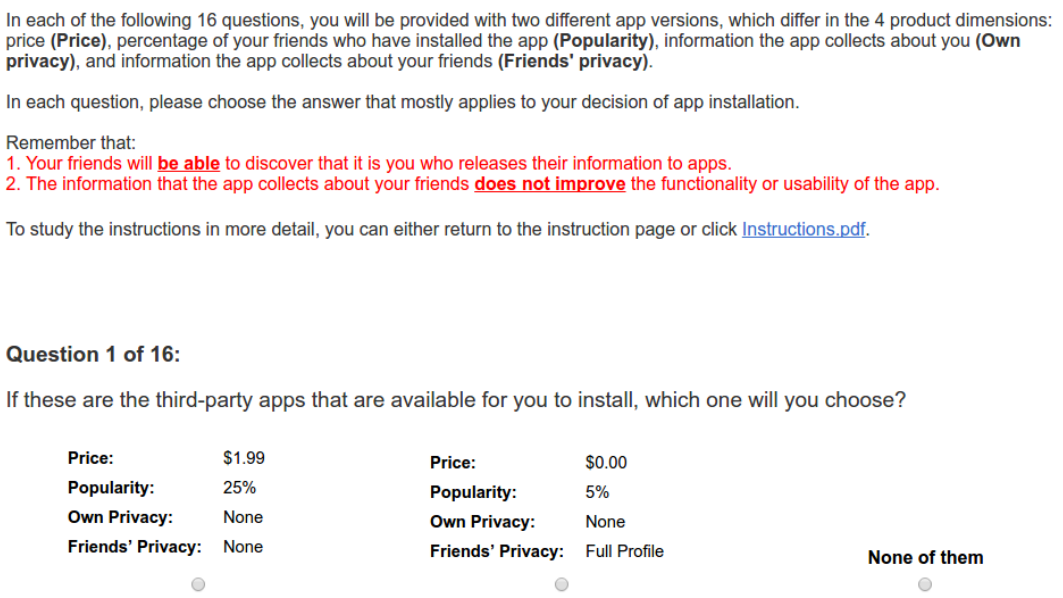

Figure 1: Screenshot of app choice interface

the choice-based conjoint method in our study has improved data quality by about 20%.

Of the 931 participants, 47.6% are male and 52.4% are female. In addition, our sample covers a wide range of age categories and education levels, ranging from 18 to over 50, and ranging from less than high school to higher education degrees such as master and PhD, respectively. In terms of income level, our participants have yearly incomes that range from less than $25,000 to more than $100,000, with a majority of them falling into the categories below $50,000.

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

3.3.2 *Estimations of Privacy Values*

In this section, we first describe goodness-of-fit of the estimated conjoint model. Then, we show how to use the estimated model parameters to quantify privacy valuations. Note here, following the practice in Burda and Teuteberg [13], we did not use "no choice" data, i.e., "None of them" responses during the app choice tasks, to analyze the model.

We conducted two tests to assess goodness-of-fit of the estimated model. A likelihood ratio (LR) test was first performed to measure how well the model and its estimated parameters perform compared with having no model [104]. The test indicated that all the four estimated models (one model for each treatment condition) are statistically valid ($p < 0.001$ for all models), i.e., the null hypothesis that the estimated model and zero model are equal can be rejected. In addition, to assess the validity of our model, we calculated the hit rate by identifying the alternative with the highest probability in all 15 choice sets for each participant [104]. Each of the four models has a hit rate of more than 90%, demonstrating all these four models are well-fitted.

Next, we calculated dollar values for privacy following the approach described by Krasnova et al. [62]. Conjoint analysis allows us to calculate individual and aggregated part-worths (utilities), which denote the attractiveness of a specific attribute level. Based on the part-worths, we calculated utility changes between various attribute levels as well as corresponding dollar values for each attribute level change (see details in Appendix B). We show these results in Table 2, where the "Utility Change" column indicates aggregated utility changes, while the "Dollar Values" column displays averages of dollar values perceived by individuals.

From Table 2, we can access the dollar values which individuals place on different dimensions of own information and of friends' information. For example, we notice that in the scenario where sharing friends' information is anonymous and where such information is irrelevant to app's functionality (T1), individuals value their friends' *basic* information (corresponding to friends' privacy level change from "None" to "Basic profile) at $0.55, friends' *valuable* information (referring to friends' privacy level change from "Basic profile" to "Full profile") at $2.36, and friends' *full* profile information (matching friends' privacy level change from "None" to "Full profile") at $3.33.

We also observed from Table 2 that in most cases, dollar values which individuals place on their friends' information are slightly larger compared to their valuation of their own information. At the first glance, this observation might be counter-intuitive. However, friends' privacy value reported here is the dollar value that an individual places on the information of *all* of his/her friends.[4] Considering that our participants self-reported to have on average 263 friends on their preferred SNS, this means that the value for a

[4]We made it clear to participants that an app might collect information of all their friends by not only using and highlighting the words "friends", but also explicitly asking for the number of their social network friends.

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

Table 2: Utility change and monetary value of change

single friend's personal information is very small (as small as a few cents) suggesting that individuals are *privacy egoists*.

3.3.3 Effects of Sharing Anonymity and Context Relevance on Privacy Valuation

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

Our analysis shows a significant main effect of sharing anonymity on the valuation of friends' basic information ($F(1,931) = 11.95$, $p = 0.001$), friends' valuable information ($F(1,931) = 6.33, p = 0.012$), and friends' full profile information ($F(1,931) = 5.03, p = 0.025$). More specifically, when sharing friends' information is anonymous, individuals value their friends' privacy significantly less than in the scenario where such sharing behavior is identifiable (see Figure 2, Figure 3, and Figure 4).

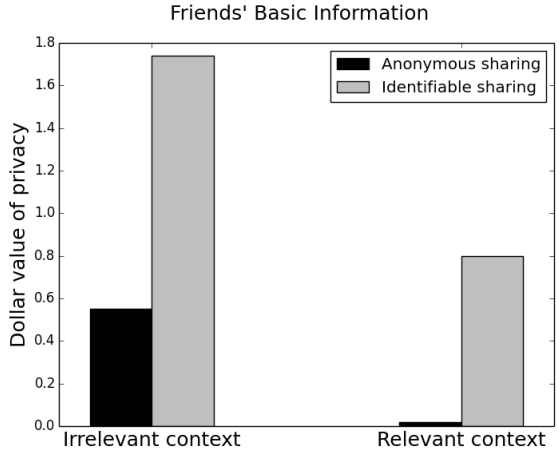

Figure 2: Effects of sharing anonymity and context relevance on valuation of friends' basic information

When it comes to the valuation of own personal privacy, we fail to detect a significant impact of sharing anonymity. In other words, the condition as to whether or not sharing friends' information is anonymous does not affect how individuals value their own basic information ($F(1,931) = 1.72, p = 0.189$), own valuable information ($F(1,931) = 0.14, p = 0.708$), or own full profile information ($F(1,931) = 0.90, p = 0.344$).

As to the condition of context relevance, we find it to significantly affect valuation of interdependent privacy. Individuals place lower values on friends' basic information ($F(1,931) = 6.61, p = 0.010$), valuable information ($F(1,931) = 7.92, p = 0.005$), and full profile

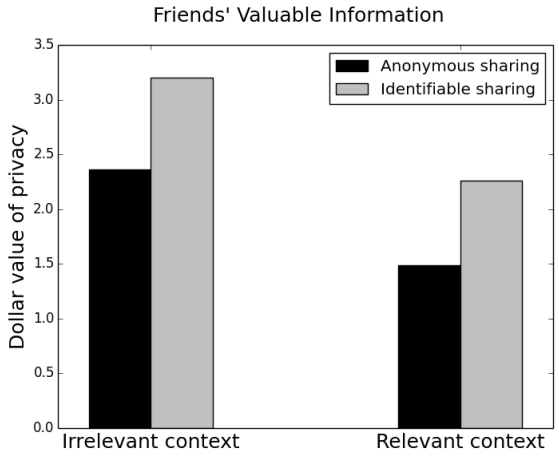

Figure 3: Effects of sharing anonymity and context relevance on valuation of friends' valuable information

information ($F(1,931) = 9.32, p = 0.002$), when they believe that information improves apps' functionality compared to the alternative scenario (see Figure 2, Figure 3, and Figure 4).

The impact of context relevance regarding the valuation of own valuable data is insignificant ($F(1,931) = 0.15, p = 0.696$); however, we observe that the treatment effect is significant for the value which individuals place on their own basic information ($F(1,931) = 3.86, p = 0.050$) and full profile information ($F(1,931) = 7.17, p = 0.008$). This might indicate that the condition of context relevance, even though only information is given to the individual about the relevance of app's usage of *friends'* personal information, has a partial spillover effect on the valuation of their *own* privacy.

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

4. INVESTIGATION OF DETERMINANTS OF PRIVACY VALUE WITH SEM

By applying choice-based conjoint analysis, we quantified the dollar values which app users place on their own and friends' privacy. We next aim to position the conjoint study results in an SEM model to investigate what drives the valuation of personal and interdependent privacy. More specifically, we seek to understand how factors such as different dimensions of privacy concerns, their antecedents, sharing anonymity, as well as context relevance affect the valuations of app users' own and their friends' information.

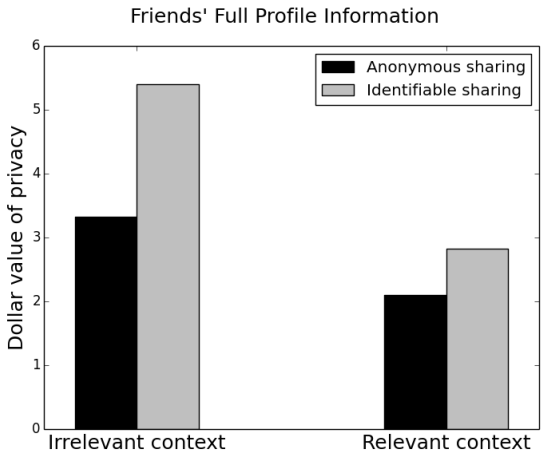

Figure 4: Effects of sharing anonymity and context relevance on valuation of friends' full profile information

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

4.1 Hypotheses and Research Model

When individuals provide their information to other parties, a *social contract*, which is generally understood as the expectation that these parties will manage personal information properly [77], is formed [16]. If individuals believe their personal information has been misused, they may consider such an implied contract breached [77, 23], and hence lower their trust assessment associated with the involved parties. In addition, prior research shows that in the electronic commerce context, an online consumer's privacy being intruded by a single online company could lead to the perception of information misuse by the entire community of online sellers [75]. In particular, individuals who have been exposed to or have been the victim of personal information abuses could be more aware of what actions other parties could take to invade privacy [2]. Such awareness might in turn lead to the reduction of their trust in online companies. Applying this to our context, we argue that the more past privacy invasion experiences individuals have, the less likely they are to trust apps' practices to protect their privacy. Therefore, we hypothesize:

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

Previous studies demonstrate trust can enhance the evaluation of benefits, and can mitigate privacy concerns [74]. In particular, Hoffman et al. [47] argue that in the setting of online commerce, trust creates positive attitudes toward Web retailers. More specifically, trust refers to individuals' feelings that they will gain the benefits they expect without suffering negative consequences [74]. In this manner, we believe that app users who trust apps' data practices are less likely to be concerned when releasing their own personal information to apps. Hence, we making the following hypothesis:

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

Disposition to value privacy is a personality attribute reflecting an individual's inherent need (or general tendencies) to manage personal information space [115]. Therefore, as opposed to individuals who tend to be more open regarding the sharing of their personal information, individuals with a higher disposition to value privacy will also express a higher level of concern when disclosing their own personal information to others. Hence, we argue:

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

Empirical evidence in numerous studies reveals that control is one of the key factors that affects privacy concerns [27, 77]. For example, it has been found that individuals' perceptions of control over dissemination of personal information are negatively related to privacy concerns [66, 114]. Additionally, research has provided evidence that, in general, individuals will have fewer privacy concerns when they believe they can control the release and dissemination of their personal information [100, 66]. To confirm these findings, we also make the following hypothesis:

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

Prior research shows that receiving negative news reports regarding privacy, such as stories about the gathering and misusing of personal information, contributes to individuals' privacy concerns [70]. Therefore, we argue that the more knowledge about privacy an individual has, the higher the level of concerns he/she will express over both own and friends' privacy. Hence, we hypothesize:

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

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

Experimental results provide substantial evidence for the existence of *other-regarding preferences* [22, 98]. In a nutshell, the theory of other-regarding preferences indicates that individuals are not purely selfish, but rather care about others' well being. However, they differ in the extent to which they care about others, which can be determined by measuring the strength of their other-regarding preferences. Applying this theory to our context, we believe individuals who have higher other-regarding preferences express higher levels of privacy concerns over their friends' information. Hence, we argue:

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

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

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

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

Recall that in the conjoint analysis study, we introduced four treatment conditions manipulating whether disclosure of friends' information is anonymous (sharing anonymity), and whether friends' information is necessary for apps' functionality (context relevance).

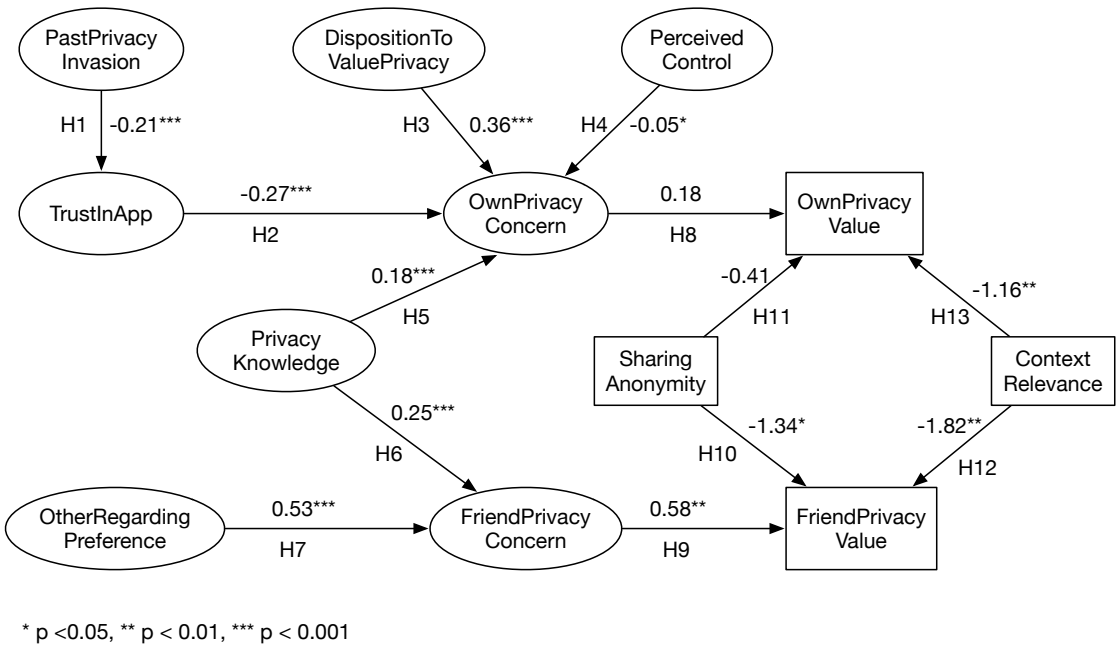

Figure 5: SEM explaining privacy valuation

The conjoint analysis results show that both sharing anonymity and context relevance impact the value which app users place on their friends' information. When it comes to the valuation of own information, we detect a (partial) significant spill-over effect of context relevance, but not for sharing anonymity.

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

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

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

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

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

We present the research model, which is based on H1 $\sim$ H13, in Figure 5.

4.1.1 Measurement Scale Development

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

Adapting from Smith et al. [95], 4 questions were used to assess past privacy invasion experiences. Trust in apps was measured by a shortened 4-item version of trust measures from Fogel and Nehmad [33], Krasnova and Veltri [63], and Dwyer et al. [29]. To measure privacy knowledge, we used 4 items derived from Park et al. [73]. Disposition to value privacy and perceived control were measured based on the 3-item scale and 4-item scale developed in [115], respectively. With respect to other-regarding preferences, we applied 5 items modified from the actively caring scale in [86]. When it comes to privacy concern, four items derived from [95] are used to assess privacy concerns for one's own information. A similar set of 4 questions, which was also derived from [95], was applied to measure individuals' concern for friends' privacy. All items were measured on a Likert-type scale with 1 = strongly disagree to 5 = strongly agree. The exact questions are provided in Appendix C.

In the conjoint analysis study, we measured three dimensions of privacy value: value of basic information, value of valuable information, and value of full profile information. Since the full profile information includes both basic and valuable information, we limit our model to the study of valuation of full profile information. As such, we used the monetary value that individuals place on their own full profile information to represent own privacy valuation in the SEM model. Similarly, the valuation of friends' privacy in the model is represented by the dollar value of friends' full profile information.

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

4.1.2 Evaluation of the Measurement Model

The measurement model is evaluated in terms of both convergent validity and discriminant validity. Convergent validity measures the degree to which different attempts to measure the same construct agree [21]. Two tests are conducted to determine the convergent validity of the scales: Cronbach's alpha and composite reliability of constructs. We present the test results in Table 3. As

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

Table 3: Evaluations of measurement model

is shown in Table 3, the Cronbach's alpha values for all scales are larger than 0.7; an indication of adequateness proposed by Nunnally [71]. In addition, composite reliabilities of our constructs exceed Nunnally's [71] criterion of 0.7. Both of these tests support the convergent validity of our measurement model.

Discriminant validity evaluates to which degree measures of different constructs are distinct from each other [14]. Discriminant validity is achieved when the square root of the variance shared between a construct and its measures is greater than the correlations between the construct and any other constructs in the model. We show the results in Table 3. We observe from Table 3 that the correlations among constructs, i.e., non-diagonal elements, are less than the square roots of shared variance, i.e., diagonal elements, indicating our model fulfills the requirements of discriminant validity.

In addition, we also conduct confirmatory factor analysis to provide an additional method to assess our measurement model. Specifically, Mean Square Error of Approximation (RMSEA) value and Comparative Fit Index (CFI) are used here. A RMSEA value of 0.06 or less, or a CFI value of 0.90 or greater indicates the model fit is acceptable [53]. Our measurement model has $RMSEA = 0.04$ and $CFI = 0.93$; further indicating that our measurement model is of high quality.

4.1.3 Evaluation of the Path Model

We first discuss goodness-of-fit data of the model. In SEM, the chi-square test is a frequently reported descriptive measure of fit. Usually, a chi-square test with a $p-$value exceeding 0.05 demonstrates a model is a good fit (i.e., significance might indicate a bad fit) [6]. Due to chi-square tests' sensitiveness to sample size, other goodness-of-fit criteria, i.e., RMSEA and CFI, are also used [50].

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

We next test H1 $\sim$ H13, which should be evaluated based on the sign and statistical significance (assessed by z-test) for corresponding paths in the model. We show the test results in Figure 5.

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

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

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

4.1.4 Discussion of SEM Results

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

Our results suggest that individuals' interdependent privacy valuations are partly determined by their personal attributes and experiences, which is similar to findings in [67]. For example, through raising privacy concerns for friends' information, app users' inherent other-regarding preferences play an important role in shaping how they value others' privacy. Similarly, through the mediation of concerns towards friends' privacy, privacy knowledge impacts the values which app users place on friends' information. This indicates that educating app users about practices impacting interdependent privacy might be a viable way to increase their valuation of interdependent privacy.

Our results further demonstrate that individuals' valuations of their friends' privacy can also be influenced by environmental settings. In particular, the value of interdependent privacy is found to be sensitive to the treatment regarding anonymity. It appears that when individuals believe their actions of disclosing friends' information to apps can be identified, they will think twice before taking such actions. Similarly, when friends' information collected by apps is irrelevant to apps' stated purposes, individuals will be more reluctant to share such information. Therefore, besides raising individuals' interdependent privacy concerns, an alternative way to protect

those who might suffer from interdependent privacy is to manipulate exogenous conditions, e.g., by making the sharing of friends' data identifiable or by informing app users whether data collection is context relevant.

Similar to their concerns about friends' privacy, users' concerns towards their own privacy is affected by their personal beliefs and experiences. In particular, we find individuals' inherent needs to manage personal information space, and beliefs regarding whether or not they are able to control privacy influence how concerned they are about their personal privacy.

When it comes to users' valuation of personal privacy, our results suggest that the condition as to whether friends' information collected by an app is relevant to the app's functionality also has a significant impact. Given that context relevance does not differ in terms of apps' practices of accessing users' own personal information (as per the experimental instructions), this suggests a spillover effect [26, 91]. In other words, individuals might believe that their own information also contributes to app's functionality when they know this is the case for friends' information.

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

The insignificance of sharing anonymity in reducing users' perceived value of their own information makes sense since we would not expect a spillover effect in this case. As individuals in our study setup know that they are sharing their own information, the condition of sharing anonymity would not play a role in app users' valuation of their own privacy. (Of course, in practice users may not always pay attention to privacy conditions associated with an adoption decision, or may not fully understand these terms as they are often presented in user-*un*friendly ways [40].)

5. DISCUSSION

In this section, we present the emerging themes and practical design implications of our study. In addition, we also offer policy suggestions that are motivated by our research findings.

5.1 Implications for Privacy by Redesign

Our study contributes to a better understanding of individuals' perceptions, knowledge and preferences regarding interdependent privacy, thereby yielding implications for the "privacy by redesign" debate [17]:

5.1.1 Design to inform about data sharing anonymity

Our results highlight that informing individuals about whether or not sharing friends' information with apps is anonymous affects how they value interdependent privacy. Given that, a viable way to protect friends' privacy is not only to make such information sharing observable, but also to inform app users that the behavior of sharing friends' data is identifiable. For example, concrete mechanisms should be proposed so that when individuals share their friends' data, their friends will be notified about these sharing behaviors, or at least can access a permanent and easily accessible record of such actions (e.g., see the logging mechanism for mobile app behaviors proposed in Petracca et al. [76]). In addition, apps' authorization dialogues can be appropriately modified, so that they convey the information to app users that sharing friends' information will be later discoverable by friends.

We are cautiously optimistic that platform providers would be inclined to assist users in limiting the unwanted flow of information to an *outside* party, i.e., app developers. While a platform provider like Facebook benefits from business relationships with third-party developers (like Zynga), it should be cautious about bulk data transfers of their most valuable asset, i.e., user data. As the notification interfaces and authorization dialogues are provided by the platform, we see potential for improvements and limits to bulk data sharing.

5.1.2 Design to reflect data collection relevance

Research has proven that presenting privacy information in a clearer fashion to users, when they are making adoption decisions, can assist users in choosing less privacy-invasive apps [61, 107]. Our study demonstrates that data collection context affects how users value their friends' information. Therefore, in order to help app users make well-informed decisions, it would be useful to revise apps' privacy notice dialogues so that they explicitly inform users whether an app's practice of collecting data is necessary for an app's functionality. The input for such dialogues can stem from technical approaches which reverse-engineer apps to infer their usage of requested information [28, 32].

5.1.3 Design to control flow of friends' information

Our work indicates that app users are privacy egoists [81] not only in that they place on average less than a few cents on full profile information of a single friend, but also due to the fact that they are eager to reveal friends' data when they believe such disclosure behaviors result in better app performance. As such, relying on individuals themselves to protect friends' privacy is likely not adequate. Therefore, affected friends of app users should be involved more directly in the decision-making process. For example, designs that enable mutual agreements regarding sharing others' data, e.g., reciprocal designs that allow a user to share others' information if and only if he/she also lets others to share his/her information, should be implemented. Alternatively, we can also introduce easy-to-use mechanisms that empower affected individuals to unilaterally decide whether or not to allow their information to be shared by others.

5.2 Insights into Privacy Policy Discussions

Our study also contributes to policy discussions on app privacy, particularly on the problem of interdependent privacy.

5.2.1 Emphasize the role of government interventions

The central aspect of the problem of interdependent privacy is the existence of negative externalities, i.e., those who install apps that

collect personal information of friends do not directly suffer from interdependent privacy harms. Similar to what economists generally suggest to deal with negative externalities [99], regulatory interventions should be put into place to deal with the problem space of interdependent privacy (including social app adoption scenarios). For example, policies or laws (e.g., privacy baseline regulations [106]) need to be introduced to rigorously limit apps' practice of collecting friends' data in bulk.

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

5.2.2 Promote education on privacy

Our work confirms that privacy knowledge impacts the values which app users place on friends' information. This indicates that educating app users about practices impacting interdependent privacy might be a viable way to increase their valuation of interdependent privacy. Therefore, policy makers should consider introducing policies which integrate privacy in educational programs. We have previously tested the introduction of relatively advanced measurement methodologies for online tracking in the context of an educational program with overall positive results [69].

6. CONCLUSIONS

To the best of our knowledge, this paper is one of the first formal studies to investigate the impact of anonymity on privacy decision-making and, in particular, on the valuation of interdependent privacy. Through conducting a choice-based conjoint analysis study with different treatment scenarios, we quantify the economic value app users place on both their own and friends' information, and also examine the impact of treatment conditions on privacy valuation. We also built and estimated an SEM model to explore how factors such as individuals' personal beliefs, attributes, experiences, as well as environmental factors, i.e., sharing anonymity and context relevance, contribute to individuals' perceived value of both personal and friends' privacy. Our research findings yield valuable insights, such as implications for the redesign of apps' privacy notice and permission dialogues, as well as suggestions to introduce new privacy polices, for better addressing individuals' own and their friends' privacy preferences.

Several limitations should be considered. In the conjoint analysis survey, we make the treatment scenarios salient by not only emphasizing them during task instructions, but also highlighting them in each conjoint choice question. Given that these treatment scenarios are highly related to the collection of friends' information, this implementation may give additional emphasis to the importance of interdependent privacy, and thereby reduce the perceived importance of personal privacy. Therefore, the low valuations for the data of individual friends are particularly notable. Nevertheless, one should proceed with care when comparing the absolute values for personal privacy and friends' privacy, and we recommend to use the results across the slightly different settings and methodologies in our related works as a joint basis for evaluations [81, 83, 82].

In addition, in our conjoint analysis study, the choice of an app is still at a hypothetical level, where participants did not really "gamble with their own money". Therefore, compared with real world scenarios where real costs can be incurred, the monetary value which participants put on others' data might be overestimated in the current study. However, given that even in the hypothetical scenario where individuals could show themselves from a desirable side at no cost, they prefer to disclose others' data when the scenario states they will not suffer directly from such behaviors, the problem of interdependent privacy may stand out even more in real world situations.

Further, we restrict the investigation of interdependent privacy valuation to the scenario of app adoption. However, other contexts, such as data analytics [19], location privacy [72], and genetic privacy [55, 109], also emphasize the issue of interdependent privacy. Therefore, it is prudent to also study interdependent privacy valuation in these settings in order to contribute to the generalizability of our findings.

Acknowledgments: We thank S. Shyam Sundar for insightful discussions during the design stage for this research study. We also thank Mary Beth Rosson, Peng Liu and the anonymous reviewers for their detailed suggestions for improvements of the manuscript. We further acknowledge the comments we received for our presentation at the Federal Trade Commission PrivacyCon 2017 conference. The research activities of Jens Grossklags are supported by the German Institute for Trust and Safety on the Internet (DIVSI).

7. REFERENCES

[1] A. Acquisti and J. Grossklags. Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *Proceedings of the 2nd Annual Workshop on Economics and Information Security*, 2003.

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

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

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

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

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

[7] C. Bauer, J. Korunovska, and S. Spiekermann. On the value of information - What Facebook users are willing to pay. *Proceedings of the European Conference on Information Systems (ECIS)*, 2012.

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

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

[10] A. Besmer and H. Richter Lipford. Moving beyond untagging: Photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1563–1572, 2010.

[11] 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.

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

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

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

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

[17] A. Cavoukian and M. Prosch. Privacy by redesign: Building a better legacy. *Information Privacy Commissioner Ontario*, pages 1–8, 2011.

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

[19] 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.

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

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

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

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

[24] 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.

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

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

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

[28] 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.

[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, A. P. Felt, and D. Wagner. Choice architecture and smartphone privacy: There's a price for that. In *The Economics of Information Security and Privacy*, pages 211–236. Springer, 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] J. Fogel and E. Nehmad. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1):153–160, 2009.

[34] N. Good, J. Grossklags, D. Thaw, A. Perzanowski, D. Mulligan, and J. Konstan. User choices and regret: Understanding users' decision process about consensually acquired spyware. *I/S: A Journal of Law and Policy for the Information Society*, 2(2):283–981, 2006.

[35] 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.

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

[37] 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.

[38] 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.

[39] 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.

[40] J. Grossklags and N. Good. Empirical studies on software notices to inform policy makers and usability designers. In S. Dietrich and R. Dhamija, editors, *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007*, pages 341–355. Springer, 2007.

[41] S. Gürses, C. Troncoso, and C. Diaz. Engineering privacy by design. In *Proceedings of the Conference on Computers, Privacy & Data Protection*, 2011.

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

[43] 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.

[44] 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.

[45] H. Harkous and K. Aberer. "If you can't beat them, join them": A usability approach to interdependent privacy in cloud apps. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, pages 127–138, 2017.

[46] H. Harkous, R. Rahman, B. Karlas, and K. Aberer. The curious case of the PDF converter that likes Mozart: Dissecting and mitigating the privacy risk of personal cloud apps. *Proceedings on Privacy Enhancing Technologies*, 2016(4):123–143, 2016.

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

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

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

[50] 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.

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

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

[53] 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.

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

[55] 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.

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

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

[58] R. Johnson. Trade-off analysis of consumer values. *Journal of Marketing Research*, pages 121–127, 1974.

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

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

[61] P. Kelley, L. 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.

[62] 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.

[63] 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.

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

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

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

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

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

[69] A. Nochenson, J. Grossklags, and K. Lambert. Conducting an internet measurement project in an interdiscipinary class context: A case study. In *Proceedings of the 6th International Conference of Education, Research and Innovation*, pages 6938–6947, 2013.

[70] 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.

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

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

[73] 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.

[74] 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.

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

[76] G. Petracca, A.-A. Reineh, Y. Sun, J. Grossklags, and

T. Jaeger. Aware: Preventing abuse of privacy-sensitive sensors via operation bindings. In *Proceedings of the 26th USENIX Security Symposium*, 2017.

[77] 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.

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

[79] S. Preibusch. The value of privacy in web search. In *Proceedings of the Twelfth Workshop on the Economics of Information Security (WEIS)*, 2013.

[80] 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.

[81] 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.

[82] Y. Pu and J. Grossklags. Sharing is caring, or callous? In *International Conference on Cryptology and Network Security*, pages 670–680. Springer, 2016.

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

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

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

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

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

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

[89] A. Roth. Bargaining experiments. In J. Kagel, A. Roth, and J. Hey, editors, *The Handbook of Experimental Economics*, pages 253–348. Princeton University Press, 1995.

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

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

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

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

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

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

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

[97] 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.

[98] D. Stahl and E. Haruvy. Other-regarding preferences: Egalitarian warm glow, empathy, and group size. *Journal of Economic Behavior & Organization*, 61(1):20–41, 2006.

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

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

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

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

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

[104] K. Train. *Discrete choice methods with simulation*, volume 8. Cambridge University Press, 2002.

[105] 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.

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

[107] 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.

[108] 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.

[109] J. Weidman, W. Aurite, and J. Grossklags. Understanding interdependent privacy concerns and likely use factors for genetic testing: A vignette study. In *Proceedings of the 3rd International Workshop Genome Privacy and Security (GenoPri)*, 2016.

[110] R. Wheeler. Package algdesign: Algorithmic experimental design, 2010.

[111] P. Wisniewski, N. Islam, H. Richter Lipford, and D. Wilson. Framing and measuring multi-dimensional interpersonal

privacy preferences of social networking site users. *Communications of the Association for Information Systems*, 38(1):235–258, 2016.

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

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

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

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

[116] H. Xu, N. Wang, and J. Grossklags. Privacy by redesign: Alleviating privacy concerns for third-party apps. In *Proceedings of the 33rd International Conference on Information Systems*, 2012.

APPENDIX

A. A TYPICAL TASK IN FULL-PROFILE CONJOINT ANALYSIS STUDY

Figure 6 shows a task participants are expected to complete, if we implement our study by utilizing a full-profile conjoint analysis method [83]. Specifically, in this task, participants are required to rank 9 versions of an app according to their own preferences. Given that these app versions differ in 4 attributes, which further have multiple levels, this full-profile conjoint analysis task represents a higher cognitive challenge compared to the task we used in the current study (see Figure 1).

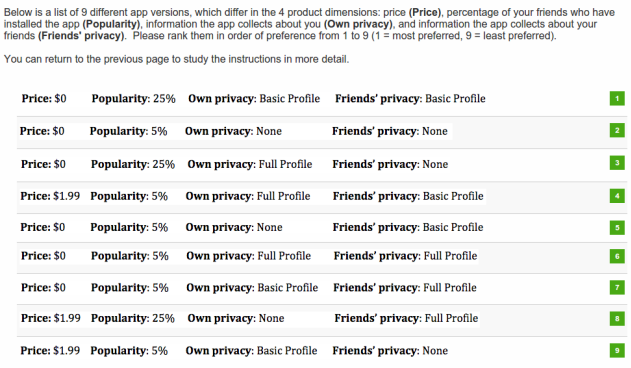

Figure 6: A typical task in full-profile conjoint analysis study

B. AN EXAMPLE OF CALCULATING MONETARY VALUE OF PRIVACY

Following the practice in Krasnova et al. [62], we calculate privacy valuations based on utility associated with each attribute level. For example, consider Table 4 which lists the utilities a person has for each attribute level. We can then calculate the monetary value that person assigns to friends' basic information by taking the following four steps:

1. Calculating utility change of price level change from "$1.99" to "$0.00", which is: $1.63-(-1.63)=3.26$.

Attributes	Attribute Levels	Part-worth Utilities
Price	$0.00	1.63
	$1.99	-1.63
Network Popularity	5%	-0.73
	25%	0.73
Own Privacy	None	0.93
	Basic profile	0.43
	Full profile	-1.36
Friends' Privacy	None	0.60
	Basic profile	0.40
	Full profile	-1.00

Table 4: An example of part-worth utilities

2. Calculating amount of utility change per dollar change, which is $3.26/1.99=1.64$.
3. Calculating utility change of friends' privacy level change from "Basic profile" to "None", which is $0.6-0.4=0.2$.
4. Calculating dollar equivalent for friends' privacy level change from "Basic profile" to "None", i.e., dollar value of friends' basic information, which is $0.2/1.64=0.12$.

C. SURVEY INSTRUMENTS

Table 5, on the following page, includes the survey instruments that we utilized in our study.

Construct	Question wording
TrustInApp	Third-party app developers tell the truth about the collection and use of personal information.
	Third-party app developers can be relied on to keep their promises.
	I trust that third-party app developers will not use users' information for any irrelevant purposes.
	I can count on third-party app developers to take security measures to protect customers' personal information from unauthorized disclosure or misuse.
Privacy Knowledge	Companies today have the ability to place online advertisements that target you based on information collected about your web browsing behavior.
	When you go to a website, it can collect information about you even if you do not register.
	Popular search engine sites, such as Google, track the sites you come from and go to.
	Many of the most popular third-party apps reveal users' information to other parties, such as advertising and Internet tracking companies.
PastPrivacy Invasion	How often have you personally been victim online of what you felt was an invasion of privacy?
	How often have you personally been victim online of what you felt was an invasion of privacy?
	How often have you noticed others being victims online of what you felt was an invasion of privacy?
	How often have you noticed others being victims offline of what you felt was an invasion of privacy?
DispositionTo ValuePrivacy	Compared to others, I am more sensitive about the way personal information is handled.
	Keeping information private is the most important thing to me.
	Compared to others, I tend to be more concerned about threats to information privacy.
OtherRegarding Preference	I have recently helped a person with a problem.
	I should go out of my way to help people more often.
	If a member of my "social group" comes to me with a personal problem, I'm willing to listen without being judgmental.
	If a member of my "social group" needs help on a task, I am willing to help even if it causes me some inconvenience.
	I am willing to help a "social group" member I don't know.
Perceived Control	I believe I have control over who can get access to my personal information collected by third-party app developers.
	I think I have control over what my personal information is released by third-party app developers.
	I believe I have control over how my personal information is used by third-party app developers.
	I believe I can control my personal information provided to third-party app developers.
OwnPrivacy Concern	It usually bothers me when third-party app developers ask me for personal information.
	When third-party app developers ask me for personal information, I sometimes think twice before providing it.
	It bothers me to give my personal information to so many third-party app developers.
	I'm concerned that third-party app developers are collecting too much personal information about me.
FriendPrivacy Concern	It usually bothers me when third-party app developers ask me for my friends' personal information.
	When third-party app developers ask me for my friends' personal information, I sometimes think twice before providing it.
	It bothers me to give my friends' personal information to so many third-party app developers.
	I'm concerned that third-party app developers are collecting too much personal information about my friends.

Table 5: Survey instruments