Factors influencing privacy concern for explanations of group recommendation

Najafian, Shabnam; Delic, Amra; Tkalcic, Marko; Tintarev, Nava

DOI
10.1145/3450613.3456845

Publication date
2021

Document Version
Final published version

Published in
UMAP 2021 - Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization

Factors Influencing Privacy Concern for Explanations of Group Recommendation

Shabnam Najafian
Delft University of Technology
Delft, the Netherlands
s.najafian@tudelft.nl

Amra Delic
Vienna University of Technology
Vienna, Austria
amra.delic@tuwien.ac.at

Marko Tkalcic
University of Primorska
Koper, Slovenia
marko.tkalcic@gmail.com

Nava Tintarev
University of Maastricht
Maastricht, the Netherlands
n.tintarev@maastrichtuniversity.nl

ABSTRACT

Explanations can help users to better understand why items have been recommended. Additionally, explanations for group recommender systems need to consider further goals than single-user recommender systems. For example, we need to balance group members' need for *privacy* with their need for transparency, since a transparent explanation might pose a privacy hazard. In an online experiment with real groups (n=114 participants: 38 groups of size 3), we seek to understand which factors influence people's privacy concerns when a single explanation is presented to a group in the tourism domain. In particular, we study the direct effects of three factors on privacy concern: **a)** group members' personality (using the 'Big Five' personality traits), **b)** specific preference scenarios (i.e., having minority or majority preferences compared to two other group members), **c)** the type of relationship they have in the group (i.e., loosely coupled heterogeneous, versus tightly coupled homogeneous). We find that for *personality* two traits, Extroversion, and Agreeableness, each significantly affects the privacy concern. Moreover, having the *minority* or majority preferences in the group, as well as the *type of relationship* people have in the group, have a strong and significant influence on participants' privacy concern. These results suggest that explanations presented to groups need to be adapted to all three factors (personality, type of relationship, and preference scenario) when considering the privacy concern of users.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; **User studies**; • **Information systems** → *Recommender systems.*

KEYWORDS

explanation, privacy concern, information privacy, group recommendation

UMAP '21, June 21–25, 2021, Utrecht, Netherlands

ACM ISBN 978-1-4503-8366-0/21/06.
https://doi.org/10.1145/3450613.3456845

ACM Reference Format:
Shabnam Najafian, Amra Delic, Marko Tkalcic, and Nava Tintarev. 2021. Factors Influencing Privacy Concern for Explanations of Group Recommendation. In *Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization (UMAP '21), June 21–25, 2021, Utrecht, Netherlands.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3450613.3456845

1 INTRODUCTION

Explanations can be regarded as additional information that accompanies the recommendations and serves various goals, such as to explain the way the recommendation engine works (transparency), help users make good decisions (effectiveness), and increase users' confidence in the system (trust) [40]. Many studies have demonstrated the benefits of adding explanations to automated recommendations. For instance, Herlocker et al. [14] found that adding explanations to recommendations can significantly improve the acceptance rate of the recommendation and the satisfaction of the users thereof. Sinha and Swearingen [36] found that transparent recommendations can also increase the user's trust in the system. These results were replicated in various domains and using different explanation methods. The majority of research focused on single-user scenarios. However, when explaining recommendations to a group of users, an additional aspect, *privacy*, becomes relevant as well. This aspect requires a trade-off between a) generating effective explanations to group members and b) keeping each group member comfortable by not disclosing private preferences to other group members. For example, a person who is in a staff group, which includes the manager, might not feel comfortable that an explanation discloses that the Bulldog coffee-shop (a cannabis store) has been recommended to the group since (s)he likes it.

Early works [17, 31] about explanations of recommendations tailored for groups limited their focus on justifying the selected aggregation technique.[1] Quijano-Sanchez et al. [35] investigated how group dynamics (e.g., user's personality, tie strength between users, etc.) affects the perception of explanations. They speculated that group members might feel an intrusion to their privacy if their personal preferences are disclosed to other group members in the explanations. Besides, findings from previous works suggest that

[1] Group recommendations are, in most cases, generated by aggregating group members' individual preferences (or recommendations) with methods called aggregation techniques.

there may be some individual differences in the levels of participants' privacy concern about disclosing their information [21, 33]. To this end, in this paper, we study privacy concerns in explanations of group recommendations.

We investigate the relationship between factors identified in the literature and individual privacy concerns. The first factor we investigate is users' *personality*, modeled using the Five Factor Model (FFM, often referred to as the Big5). Furthermore, related work [1, 16, 30] indicates that there are two more factors that have an influence on participants' privacy concerns: *relationship type* (both relationship strength and equality of positions) and *preference scenario* (whether the active user's preference is in the minority or majority compared to others' preferences within the group).

Specifically, we investigate the following research question:

> *How do people's personality, their relationship type in the group, and preference scenario affect their privacy concern regarding group recommendation explanation?*

Our results indicate that the following variables have a significant impact on the participants' privacy concerns: two facets of personality (Extraversion and Agreeableness), preference scenario, and relationship type. These findings will inform the design of group explanation approaches in order to minimize privacy issues.

The next section presents related work in explanations for group recommendations with the focus on the work that discusses privacy aspects in group explanations. In Section 3, we develop a conceptual model of the relationships between the three aforementioned factors and privacy concern. In Section 4 we present two pre-studies that were needed in order to validate two factors for the main study: 1) sensitive information types and 2) questionnaire items measuring the construct of privacy concern. In Section 5 we describe the main user study performed to evaluate the developed model. Then, we describe the results and discuss implications for adapting the level of privacy to these three factors in Section 6. We summarize our results and their implications in Section 7, and conclude with plans for future work in Section 8.

2 RELATED WORK

We provide an overview of existing research related to explanations in group recommender systems. We also discuss privacy aspects in explanations for groups, which arise in these scenarios.

2.1 Explanations for group recommendations

Although there are many studies on group recommendations, only a few of them focus on *generating explanations*. The generation of explanations for group recommendations depends on how the group recommendations were generated in the first place. One approach to generate group recommendations, called aggregated models, aggregates individual preferences (e.g., existing ratings) into a group model. Group recommendations are then generated based on the group model. Another approach to generate group recommendations is called aggregated predictions. It aggregates individual item-ratings predictions and recommends to the group items with the highest aggregated scores [11]. Explanations based on these approaches reveal the underlying mechanisms of the employed social choice-based preference aggregation strategies [20, 34, 43].

Similarly, Quijano-Sanchez et al. [35], extended work on generating and personalizing explanations by including the social factors of personality and tie strength between group members involved in the recommendations decision-making processes. They showed that adding the social component to explanations increases users' likelihood to accept the recommendations. However, it is important to note that personalization may cause privacy concerns, especially when including social aspects. For example, this kind of explanation might damage friendships, by telling users that someone in the group does not trust them or offend users, by telling them that their preferences are taken into account less, due to their personality [35].

The existing works on generating explanations for group recommendations primarily consider the need for transparency, e.g., to clarify the reasoning and data behind a recommendation to help users better understand how the recommender system works and why a specific item has been recommended [42]. However, when generating explanations for *groups*, privacy becomes of great relevance as well. The work of Herzog and Wörndl [16] highlights the need for privacy in a group context, as it found that there was a greater amount of interaction with distributed displays when people were interacting on their individual devices rather than on a shared public display. For example, when using a shared public display to enter sensitive data, privacy was a concern for many participants.

2.2 Factors influencing privacy concern in groups

Social science and psychology scholars have noted that privacy might be more situation-specific than dispositional. They argued that privacy concern in a specific situation is more understandable than it is in the abstract [3, 8, 28, 37, 38].

Xu et al. [45] defined privacy concern as consumers' concerns about a possible loss of privacy as a result of information disclosure to a specific external agent (e.g., a specific website). We adapt the definition for groups as:"(each) group member's concerns about a possible loss of privacy as a result of the group recommender system presenting an explanation to the whole group".

We reviewed the literature to identify which factors may influence privacy concern in group recommendations. Privacy concern has to the best of our knowledge not been investigated for group recommendations. Therefore, we reviewed the extensive literature on privacy concern for users interacting online or with service providers, to identify which personal and situational factors could affect a user's privacy concern (e.g., [2, 9, 19, 22]).

We identified three factors relevant to explaining group recommendations, namely: *personality*, *relationship type*, and *preference scenario*.

2.2.1 Personality. Personality theories (or trait theories) suggest that personality traits, referring to an individual's stable, long-term psychological attributes, would have a potential impact on people's privacy perception. The association between personality and behavior is widely discussed in behavioral research. In terms of online information privacy, a large number of personality models

have been studied, including the Big Five personality model (encompassing five dimensions/traits: Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness) [2, 19, 24, 26]. Table 1 summarizes the correlations between each of these traits and concern for privacy in different domains. We see that two traits, Agreeableness and Neuroticism, are significantly related to privacy concern. While we see a significant effect for Extroversion in the E-commerce domain, the results across domains are inconsistent and all the correlations are weak.

2.2.2 Relationship type. Results of a previous study in group recommender systems suggest that people's privacy concerns would also be affected by the types of relationships within the group. Herzog and Wörndl [16] investigated different user interfaces for tourism group recommendations among two group types; *primary groups* (i.e., groups in which members shared a close relationship, such as family), and *secondary groups* (i.e., groups which are often created in goal-focused situations, such as colleagues). They found that primary groups felt more comfortable when sharing a display and revealing their preferences to other group members. In contrast, secondary groups preferred to use separate devices in order to specify their preferences individually.

2.2.3 Preference scenario. When having a minority preference or opinion, there is a chance that people may want to conform to the norm. Conformity is defined as *a change in opinion, judgment, or action to match the opinions, judgments, or actions of other group members* [12]. For instance, a person could express an opinion to match the opinions of others in the group, even though they might believe differently [1, 30]. Consequently, if they think differently from the rest of the group, they may not want their preferences disclosed by the recommender system either.

Similarly, Najafian et al. [33] investigated which information people would like to disclose in explanations for group recommendations in the music domain. Their results suggested that when a person differs in their preferences, they were sensitive to the system disclosing their personal information. These findings suggest that people's privacy concerns could be influenced by whether a person's preferences are in the minority compared to those of other group members (or not).

3 RESEARCH MODEL

In the previous section, we identified three factors that could affect privacy concern in the group, namely: *personality*, *relationship type*, and *preference scenario*. In this section, we are developing a conceptual model to understand the relationship between those factors.

Figure 1 depicts the conceptual model, which includes a well-established connection (personality -> privacy concern) and two new connections that may also apply in the context of groups (relationship -> privacy concern and preference scenario -> privacy concern). We examine this conceptualization through the proposed theoretical lens of *privacy in groups*.

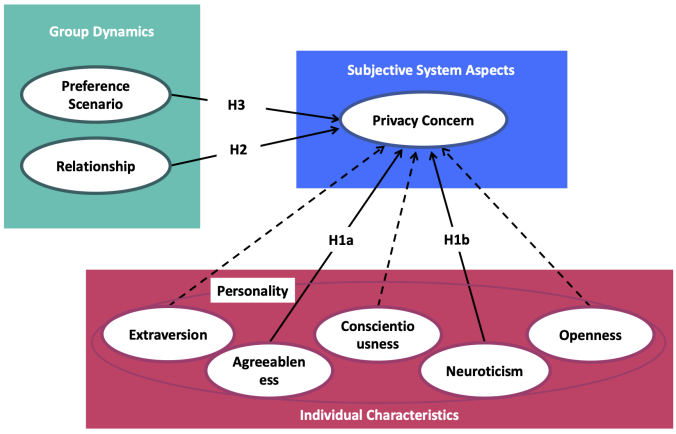

Figure 1: The conceptual model of disutility enhancers and reducers for disclosing personal information in group explanation.

3.1 Personality

Related work shows that two personality traits, Agreeableness and Neuroticism, are related to privacy concern.

Agreeableness. Agreeableness is a trait related to the likeability and social conformity of individuals. Highly agreeable individuals have been found to trust others and to be less suspicious of their environment or other individuals [7]. Although warm and trusting in their social interactions, agreeable individuals are apprehensive of deviant behaviors [5]. Because privacy invasion is deviant social behavior, some argue that individuals with this trait are more concerned about their privacy than are others (e.g., [2, 19]). On the other hand, some other studies argue, agreeable individuals are less likely to appraise others' actions as potentially harmful when faced with privacy threats (e.g., [24]). Hence, their tendency to trust others and to be less suspicious of their environment should reduce their level of privacy concern [19]. The results from Table 1 indicate that there is an ambiguous effect of agreeableness in the literature. Even though all the mentioned studies found a significant effect of this trait on privacy concern, the direction was not consistent. This leads us to the following hypothesis,

H1a: Agreeableness will influence individuals' privacy concern regarding the presented explanation to the group.

Neuroticism. Neuroticism reflects how individuals react to stressful conditions. It is sometimes referred to as emotional instability, or if reversed as emotional stability (e.g., [2]). In the remainder of the paper, we will use the term "neuroticism" as it is the most widely used one. Individuals with this trait are described by terms such as anxious, depressed, stressed, suggestible, volatile, and fearful [13]. We conjecture that a person with a higher level of anxiety and fearfulness should be more nervous about disclosing their personal information and have a greater privacy concern. As can be seen in Table 1, a significant and positive effect of neuroticism on privacy concern was found in multiple domains. This leads us to the following hypothesis,

Table 1: Personality and online information privacy

Independent variables	Dependent variables	Online [24]	Finance [2]	Ecommerce [2]	Health [2]	Location [19]
Extroversion	Concern for privacy	0.04	ns	-0.11*	ns	-0.03
Agreeableness		0.17*	0.14**	0.14**	0.12*	-0.22**
Conscientiousness		0.13	ns	ns	ns	0.12*
Neuroticism		-	0.12*	0.11*	0.22***	0.05 (Stability)
Openness		-	ns	ns	ns	0.11*

Notes: * $p < .05$, ** $p < .01$, *** p < .001, 'ns' $p > .05$.

H1b: Neuroticism will influence individuals' privacy concern regarding the presented explanation to the group.

We will investigate the influence of these traits on privacy concern in the context of the tourism group recommendation (we included all the personality traits in our model).

3.2 Relationship type

The second factor that has been shown to be related to privacy concern is the relationship people have within the group. Wang et al. [44] distinguish between *positionally homogeneous* and *positionally heterogeneous* groups. In positionally homogeneous groups, such as friends or a group of strangers (e.g., a tourist group), the position of members is equal. In heterogeneous groups, such as family groups, the position of members is unequal. They also distinguish between *tightly-coupled* (strong relationship: members are close and intercommunication is important) and *loosely-coupled* (weak relationship: members are relatively estranged, and intercommunication is less frequent and less important) groups. Based on these two dimensions, Wang et al. [44] define four different group types: tightly-coupled homogeneous (e.g. a friends' group), loosely coupled homogeneous (e.g. a group of strangers like a tourist group), tightly-coupled heterogeneous (e.g. a family group), and loosely coupled heterogeneous (e.g. a staff group including managers). In this study, we only opted for two group types in order to reduce the number of independent variables. We chose to *study* the two extreme cases: "tightly coupled homogeneous" and "loosely coupled heterogeneous", in order to investigate whether there is any merit in modelling relationship type in relation to privacy concerns. In the first one, people have a strong relationship and the position of members is equal, in the second one people have a weak relationship, and the position of members is unequal. Hence, we conjecture,

H2: The relationship type people have in the group will influence their privacy concern regarding the presented explanation to the group.

3.3 Preference scenario

The third factor that has been shown to be related to privacy concern is when a person's preference is in the minority or majority compared to others' preferences within the group. As previously mentioned, people often conform to the group to avoid being disliked and express an opinion that matches the one of the rest of the group even though they might think differently [1, 30]. Hence, we conjecture,

H3: Preference scenario (having minority or majority preferences in the group) will influence individuals' privacy concern regarding the presented explanation to the group.

4 PRE-STUDIES

Before starting the main study we needed to (1) verify that the exposure of personal information in the explanations actually does raise privacy concerns in participants (pre-study 1) and (2) validate the instrument for measuring the privacy concern, which we adapted from related work (pre-study 2).

4.1 Pre-study 1: Group Explanation

Private information can fall under one or more of the following nine categories: location, medical, drug/alcohol, emotion, personal attacks, stereotyping, family or other associations, personal details, and personally identifiable information [4]. We selected the following subset which is relevant to the domain of tourism: location, drug/alcohol, emotion, personal details, and personally identifiable information. Some of this information is used in current tourism recommender systems, for example Mohamed et al. [32] use users' current location and emotion/mood, or Cheng et al. [6] consider user personally identifiable information (e.g., gender, age, race) to recommend personalized travel places to visit. In order to verify that the exposure of personal information in the explanations actually does raise privacy concerns in participants, we ran a study. We asked ten colleagues from a computer science faculty to indicate how privacy sensitive each type of information, specifically in the context of an explanation given to the whole group, would be on a 5-point Likert scale ranging from 1 (non sensitive at all) to 5 (very sensitive). In addition, we provided an example from the explanation for each type of information. For instance, for the Drug/alcohol category (e.g., *you will love the Bulldog coffee-shop, a cannabis store*), for the Emotion category (e.g., *you are sad*), for the Personal details category (e.g., *your sexual orientation, LGBTQ+*), for the Personally Identifiable Information category (e.g., *your birth-date*), and for the Location category (e.g., *your current location*). The mean score was above 3 (out of 5) for all the types. This result suggests that the information used in the explanations is likely to provoke privacy concerns.

4.2 Pre-study 2: Establishing Construct Validity

Before we could measure the user's privacy concern regarding the presented group explanation, we needed to establish the validity of the instrument's items. We used confirmatory factor analysis (CFA), which can establish both the convergent (the question items

are actually measuring a single construct) and discriminant validity (the question items are actually measuring different constructs). A rule of thumb for CFA is to have at least five participants per questionnaire item [23]. For 8 items, the minimum number of required sample size for our study is therefore estimated to be 40. The participants for this purpose were recruited using Prolific.[2] We used results from 40 participants, after removing 5 participants who failed an attention check. The question items for measuring privacy concern were adapted for the purpose of our main study from previous instruments developed for measuring consumer information privacy in online contexts [21, 27]. We adopted a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The values for both the CFI [3] and TLI [4] were above 0.95. The value of the Standardized Root Mean Square Residual (SRMR) was below 0.5. These values indicate a very good fit [23]. The question items with low squared loading values were removed from the final instrument (3 out of 8 items were removed).[5] The remaining items were:

- **P1)** The system disclosed, in this group explanation, information about me that I consider private.
- **P2)** All things considered, this group explanation would cause serious privacy problems.
- **P3)** To me, it is the most important thing to keep my privacy intact from the group members of the group I am in.
- **P4)** The system shows, in this group explanation, more information about me than I am comfortable with.
- **P5)** This group explanation is revealing too much personal information about me to the other group members.

5 EXPERIMENT

In this section, we describe an online between-subjects study that investigates which factors influence the group members' privacy concern regarding the information disclosed in the presented group recommendation explanation.

We had two experimental manipulations (relationship type and preference scenario), an observed variable (personality), and a dependent variable (privacy concern). The *relationship type* variable takes the value of 1 for participants who are in a "loosely coupled heterogeneous group" (e.g., staff group including a manager), and 0 when they are in a "tightly coupled homogeneous" group (e.g., friend group). We controlled the *preference scenario* variable by setting its value to 1 for the member with minority preference (i.e., Carol in the scenario description in Section 5.1) and to 0 for the members that are in majority in terms of preferences (Bob and John from the scenario description).

We used the Big Five Inventory (BFI) to assess the *personality* on the five factors of Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism [18]. It is composed of 44 items with a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

[2] www.prolific.co [July 2020].
[3] The Comparative Fit Index evaluates the model fit by analysing the discrepancy between the conjectured and the null model.
[4] The Tucker–Lewis index is preferable for smaller data samples and it indicates how much the conjectured model improves the fit relative to the null model.
[5] This decision is made on the basis of squared loading, using the recommended threshold of 0.50 [23]).

For the qualitative analysis, we distinguish between high and low for each trait. First, we aggregate all question items for each trait. Then after normalizing, we split the scores into two bins around the normative mean value for that trait as obtained in a large data-set of adult American Internet users [39]. With several question items, validated in the pre-study 2 (see Section 4.2), we measured the group members' *privacy concern* about a possible loss of privacy as a result of the group recommender system presenting an explanation to the group.

5.1 Procedure

In the previous section, we validated both the example explanation that we use in our user study and the question items for the main variable that we are measuring, privacy concern, in this user study. Here we introduce the online study we designed to evaluate people's privacy concern regarding a presented group explanation in the real groups.

We designed an online between-subjects experiment in which participants were randomly assigned to form either a) a tightly coupled homogeneous group or b) a loosely coupled heterogeneous group. The group size was set to three, similar to previous studies of group recommendation [15, 29]. This was executed in two phases: 1) setting up groups, and 2) evaluating privacy concern.

Setting up groups. In this phase participants who see the advertisement and would like to participate in our study click on the provided link and are redirected to our ''sign up'' page. For each group, the experiment is initiated by one person, which we will refer to as an *inviter* as they are requested to invite the other two members.

Step 1: While inviters sign up, they need to invite two other group members based on the group type we assign to them. For example for the "loosely coupled heterogeneous" type, they are requested to form a group where the position of members is unequal, the members are relatively estranged, and intercommunication is less frequent and less important (e.g., a staff group including a manager). By entering the potential group members' names and emails, an invitation email is sent to the invitees.

Step 2: When the two *invitees* get the invitation email they have a week to accept the invitation. Once both invitees accept the invitation, all group members get an email containing a link. This link which contains group members' information redirects them to the second phase (evaluating privacy concern), corresponding to that group.

Evaluating Privacy Concern. When all the group members are redirected to the second phase, they go through the following steps:

Step 0: Participants are shown a description of the scenario and the explanation for the recommended point of interest (POI) as can be seen in the following example.

The defined scenario:
Imagine that you and your group members have a plan to visit a place in Amsterdam together. A tourism app makes recommendations for your group based on all group members' individual preferences.
Carol has different tastes (preferences), compared to the other two group members. The recommended place is Carol's favorite. The app has recommended the Bulldog coffee-shop to visit for your group which will explain why it made this recommendation for all of you as follows.

Names and ages will be adapted in the following explanations based on users' inputs. Apart from that, it is the same for all the participants.

The presented explanation:
"The "Bulldog coffeeshop" (cannabis store) has been recommended to your group since Carol will love it! The coffee-shop isn't the primary preference of Bob and John, but they are okay with it. Their preferences will be taken into account in the next recommendations. Besides, Carol is feeling quite sad today, and we know that she really wants to visit the coffee-shop and won't be talked out of it easily.
It's a good recommendation geographically – it is close to all three of you. Carol is at Vondelpark, only a minute's walk from the coffee-shop. Bob and John are at SoHo (LGBTQ+) bar, five minutes from the coffee-shop. You can all meet there in 10 minutes.
Since you're all above 18 years in age, you can buy cannabis at the coffee-shop (Carol is 29, Bob is 28, and John is 35)."

Step 1: Participants are asked to fill in some demographic-related questions as well as a set of questions to assess their personality traits.

Step 2: Participants are asked to answer a set of survey questions related to their privacy concern regarding a shared explanation within the group in the defined scenario (the same questions validated in Section 4.2). We also include three attention check questions. At the end of the survey, participants are given the opportunity to freely express their opinions regarding the key factors that can influence their privacy preferences for a shared explanation in an open-ended question and the information they considered private.

6 RESULTS

To investigate the effects of different factors on the dependant variable, privacy concern, we built a structural equation model (SEM) upon the data collected with our questionnaire by using the R library Lavaan [6]. All questionnaire items are modeled as ordinal variables. SEM is able to analyze the effects in an integrative structure where we can associate all the desirable effects.

[6]http://lavaan.ugent.be/, October 2020

The resulting SEM model (Figure 2) shows how type of *relationship*, *preference scenario* and *personality* influences privacy concern. Based on the final results we removed two question items (P1 and P2; which were validated in Section 4.2) with low squared loading values and three question items (P3, P4, and P5; see Section 4.2) remained valid to measure group privacy concern. The model has a good model fit: chi-square(205) = 340.423, $p = .000$; root mean squared error of approximation (RMSEA) = .047; 90% CI : [0.026, 0.059], Comparative Fit Index (CFI) = .880, Turker-Lewis Index (TLI) = .808.

6.1 Participants

To determine the required sample size, we performed a power analysis [10] of a medium-sized effect (0.5 SD) with a power of 85% in a between-subjects experiment. It showed that a minimum of 100 participants are needed in total. This was inline with the suggested minimum sample size for SEM in Knijnenburg and Willemsen [23].

The participants for this paper were a convenience sample recruited through university networks. 114 participants (38 groups of 3 people) voluntarily joined our study (Age: Mean = 31.8, SD = 7.7; Gender: Female = 47%, Male = 53%). Half of the participants were assigned to form a loosely coupled heterogeneous group (19 groups) and the other half a tightly coupled homogeneous group (19 groups). By design,[7] among those one-third of participants (38 participants) were assigned to have minority preferences in the group and two third majority preferences (76 participants). All responses were included in the data analysis due to successful attention checks.

6.2 H1. Effects of Personality

Here we discuss the effects of the two personality traits we hypothesised would have an effect on privacy concern:

H1a. Agreeableness. We found that the Agreeableness trait in our participants has significant effect on their privacy concern ($p < .01$). The positive sign (coefficient=0.47) indicates that people who scored high on Agreeableness perceived higher privacy concern rather than people who scored low on this trait. Thus, we can accept hypothesis H1a: Agreeableness will influence individuals' privacy concern regarding the presented explanation to the group.

H1b. Neuroticism. We found no significant effect of participants' score on the Neuroticism trait on the participants' privacy concern. We argue that one possible reason that we did not find an effect could be the distribution of scores on this trait in our sample. Only 19 participants scored high on this trait in comparison to 95 participants with a low score on this trait.

6.3 H2. Effects of Relationship

We found that people's relationship type within the group has a significant effect on their privacy concern ($p < .001$). Specifically, the negative sign (coefficient=−0.90) indicates that participants in a tightly coupled homogeneous group (e.g., friend group) perceived a lower privacy concern, compared to participants in a loosely coupled heterogeneous group (e.g., staff group). Thus, we can accept hypothesis H2: The relationship type people have in the group will

[7]Recall that in each group, one participant preferred the POI and this was in contrast with the preferences of the other two group members who constituted the majority.

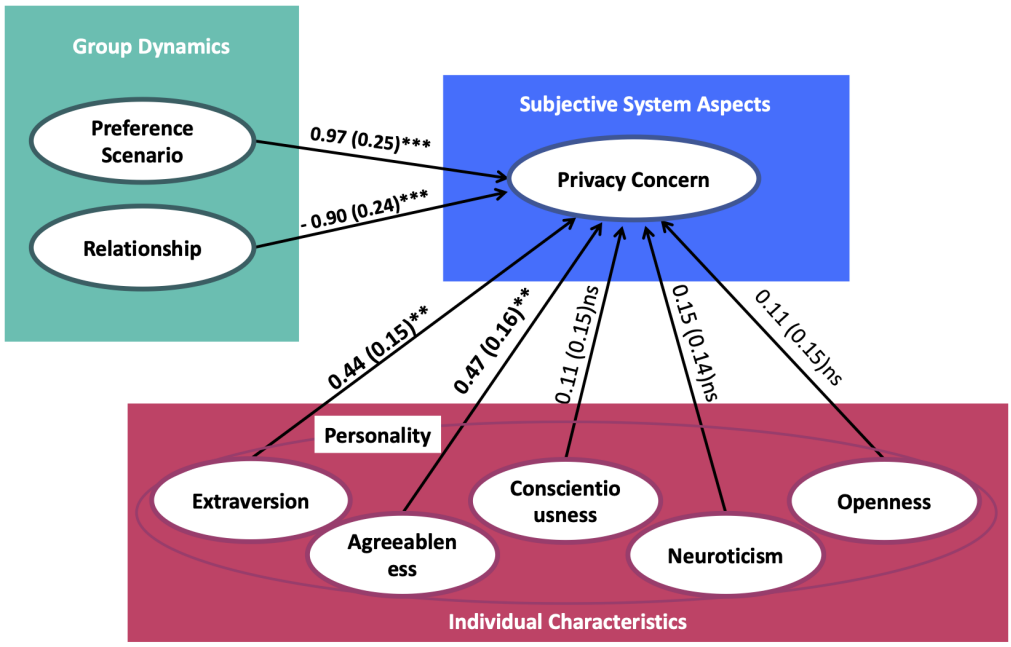

Figure 2: The structured equation modeling (SEM) results. Numbers on the arrows represents estimated coefficients (and standard error) of the effect. Significance levels: *** $p < .001$, ** $p < .01$, **'ns'** $p > .05$.

influence their privacy concern regarding the presented explanation to the group.

6.4 H3. Effects of Preference Scenario

We found that having the *minority* or *majority* preferences in the group has a significant effect on people's privacy concern ($p < .001$). Specifically, the results are consistent with conformity: the positive sign (coefficient=0.97) indicates that people having minority preferences perceived higher privacy concern rather than people having majority preferences. Thus, we can accept hypothesis H3: Preference scenario (having minority or majority preferences in the group) will influence individuals' privacy concern regarding the presented explanation to the group.

6.5 Post-hoc Analysis

The results from related work for the trait of Extraversion were weak and inconsistent. Given that we included all the personality traits in our model, we are able to report the results for Extraversion here for further comparison. Extraversion reflects people orientation and pleasure in social interactions. Descriptions of this trait include being talkative, bold, assertive, sociable, and demonstrative [13]. We found that the Extraversion trait in our participants has a significant effect on their privacy concern ($p < .01$). The positive sign (coefficient=0.44) indicates that people who scored high on Extraversion perceived higher privacy concern rather than people who scored low on this trait. We argue that a possible reason that we found a significant and strong effect could be the distribution of scores on this trait in our sample. We had a similar number of participants who scored high and low on this trait.

6.6 Qualitative feedback

We asked the participants to motivate their responses. In this section, we analyse their comments to better understand whether the three factors (personality, relationship type, and preference scenario) influenced privacy concerns differently for the five information types (Location, Drugs, Emotion, Personally identifiable Information, and Personal Details). The users' feedback was analysed using closed/fix coding [25]. They were coded based on one or more information categories (among the five information categories) users mentioned in their comments. For example, we coded the comment: *"The description indicates both that I would love a* ***cannabis cafe****, and that I am* ***very sad****. I consider both statements to be way too personal and private!"* for the category of *Drugs* and the category of *Emotion*. Then we divided these categories based on our three main factors: their relationship type, preference scenario, and their personality. All participants' comments were considered in this analysis. Following we describe the results in detail.

Location. *Personality.* 31% (17 out of 54) who scored high on Extraversion, and 31% (6 out of 19) who scored high on Neuroticism expressed privacy concern in their comments regarding disclosing their current location. Also, 25% (18 out of 72), who scored high on Agreeableness showed privacy concern about revealing their current location. Conversely, only a few participants, about 5% of participants who scored low on these three traits, showed privacy concern regarding this type of information.

Relationship type. 21% (12 out of 57) of participants who were in a loosely coupled group expressed privacy concern about revealing their current location. From the participants in a tightly coupled homogeneous group, only half of this number of participants (10%,

6 out of 57) expressed privacy concern for disclosing their current location to the group.

Preference scenario. 21% (8 out of 38) of participants who had minority preference within the group expressed privacy concern in their comments regarding disclosing their current location. Fewer participants (16%, 12 out of 76), who had majority preferences, expressed privacy concern for this type of information.

Drug/alcohol. Overall, participants expressed less concern about disclosing this type of information.

Personality. The highest number belongs to participants who scored high on Extraversion: 15% (8 out of 54). A comparable number of participants who scored high on Agreeableness and Neuroticism expressed concern about disclosing this type of information, both 10%.

Relationship type. 17% (10 out of 57) of participants who were in a loosely coupled group expressed privacy concern about revealing drug/alcohol information. From the participants in a tightly coupled homogeneous group, only 2% (1 out of 57) expressed privacy concern for disclosing this type of information to the group.

Preference scenario. 18% (7 out of 38) of participants who had minority preference within the group showed privacy concern in their comments about disclosing drug/alcohol information. A small proportion of participants about 8% (6 out of 76) of participants, who had majority preferences, showed privacy concern for this type of information.

Emotion. *Personality.* Participants showed more concern about disclosing their emotional state in the group. The highest number belongs to participants who scored high on Neuroticism: 47% (9 participants out of 19). Besides, 37% (20 out of 54) of participants who scored high on Extraversion showed concern for this type of information in their comments. Fewer participants about 18% (13 participants out of 72), who scored high on Agreeableness, expressed this concern.

Relationship type. 28% (16 out of 57) of participants who were in a loosely coupled group expressed privacy concern about revealing their emotion. From the participants in a tightly coupled homogeneous group, about 17% (10 out of 57) of the participants expressed privacy concern for disclosing this type of information to the group.

Preference scenario. 34% (13 out of 38) of participants who had minority preference within the group expressed privacy concern in their comments regarding disclosing their emotional state. Fewer participants about 10% (8 out of 76), who had majority preference within the group expressed privacy concern for this type of information.

Personally identifiable information (age). *Personality.* 30% (16 out of 54) of participants who scored high on Extraversion showed concern about disclosing their age within the group. Besides, 25% (18 out of 72) of participants who scored high on Agreeableness showed concern for this type of information in their comments. From participants who scored high on Neuroticism, 19% (4 out of 19) stated this concern.

Relationship type. 26% (15 out of 57) of participants who were in a loosely coupled group showed privacy concern about revealing their age. From the participants in a tightly coupled homogeneous group, about 10% (6 out of 57) showed privacy concern for disclosing this type of information to the group.

Preference scenario. 24% (9 out of 38) of participants who had minority preference within the group expressed privacy concern in their comments regarding disclosing this type of information. Fewer participants, about 14% (11 out of 76), who had majority preferences, expressed privacy concern for this type of information.

Personal details (LGBTQ+). *Personality.* The highest number of participants who showed concern about disclosing this type of information to the group were the ones who scored high on Agreeableness: 26% (19 out of 72). For participants who scored high on the two other traits, Extraversion and Neuroticism, fewer participants showed concern for this type of information in their comments (10%).

Relationship type. 28% (16 out of 57) of participants who were in a loosely coupled group showed privacy concern about revealing their sexual orientation. From the participants in a tightly coupled homogeneous group, fewer participants, about 5% (3 out of 57), showed privacy concern for disclosing this type of information to the group.

Preference scenario. 31% (12 out of 38) of participants who had minority preference within the group showed privacy concern in their comments regarding disclosing this type of information. Fewer participants, about 10% (8 out of 76), who had majority preferences, showed privacy concern for this type of information.

6.7 Discussion

Personality. We found that participants who scored high on Agreeableness or Extraversion were more concerned with information privacy. This was further supported by the qualitative comments from participants. The comments indicate that participants who scored high on Agreeableness were concerned more about their location, age, and sexual orientation information than about other types of information (about 19% of these participants). In contrast, the highest concern for participants who scored high on Extraversion was about their emotional information (about 37% of these participants). This was similar for participants who scored high on Neuroticism (about 47% of these participants), who showed more concern about their emotional information. As a guideline for designing explanations, we should adapt which information is disclosed depending on the personalities in the group. Different personality traits varied in terms of which information they found sensitive.

Relationship Type. The highest number of participants, who showed concern about sexual orientation and emotional information were in a loosely coupled heterogeneous group (about 28% of these participants). The highest number of participants, who were in a tightly coupled homogeneous group showed concern about only emotional information (about 17% of these participants). We should adapt to the loosely coupled heterogeneous group for all five information types.

Preference scenario. The highest number of participants who showed concern about emotional information had minority preferences (about 35% of these participants). This was about location information for the participants who had majority preferences (about

16% of these participants). Minority preferences matter a little for all information types, but in particular for emotion. We should adapt to people with minority preferences in particular when disclosing emotion.

Information Type. Among the five types of information we included in the explanation, the highest number of participants showed concern for the emotional information. Information regarding participants' age came second with regards to the concern. Surprisingly, Drugs appear to be the least important to adapt to (18% max). This might be related to the cultural background of our participants. As our participants mainly live in the Netherlands, maybe in the Netherlands people are less sensitive in disclosing this type of information. In the future, it would be interesting to study the relationship between the nationality/where participants live and their concern for different types of information.

Setting up groups. Recruitment of groups participants is a challenge when aiming to control for the group type. The challenge increases when recruiting heterogeneous, loosely coupled groups, in particular with a leader. A recommendation for future studies is to first ask the participants from a "higher" position, rather than to recruit organically or to request participants in "lower" positions to recruit others. We received feedback from several participants that it is difficult for them to ask a person in a higher position (e.g., their boss) to form a group with them.

6.7.1 Limitations. In this section, we discuss the limitations of our study.

Firstly, we measured participants' privacy concerns for a hypothetical scenario rather than their actual preferences. This might cause people not to be able to imagine the situation very well. Although we used actual groups and participants' answer to the open-ended question shows their high engagement in the study, asking participants to imagine sharing their information still might lead to different results than actually sharing it.

Secondly, we defined the scenario in such a way that we expected to maximize the privacy concern. In future studies, we plan to study the effect on different information types in more detail. Besides, in our study we studied preference in relation to a single POI which was sensitive due to being a coffee shop. Different results might be found for other types of preference scenario.

In addition, participants were recruited from universities worldwide through our professional networks. This sample may not be representative of the general population. For example, an effect for the personality trait of Neuroticism might be found in a sample that controls for the balance of high and low scores on this trait. Or the sensitive information is probably less sensitive culturally for the majority of the members of this sample.

Our work could also benefit from the larger sample size. In this study, we considered a bare minimum for relatively simple SEM models (100 observations). Besides, we relied on the independence of the data points in our model.

Finally, this study was conducted in the context of recommendations for tourism. This domain was suitable for studying group recommendations, as it is relatable for many participants. However, the results may differ in domains where preferences are less subjective in nature or differ in terms of their level of investment or risk [41].

7 CONCLUSION

In this paper, we investigated and found an effect for three factors that influence participants' privacy concern regarding an explanation of a tourism group recommendation: relationship, preference scenario, and personality. *Relationship type* has a strong and significant effect on privacy concerns. The results showed when participants are in a tightly coupled homogeneous group perceived lower privacy concern compared to a loosely coupled heterogeneous group. Besides, the *preference scenario* also has a strong and significant effect on privacy concerns. Participants being in the minority preference-wise perceived higher privacy concern compared to group members who were in the majority preference-wise. For *personality* we found the expected effect of the personality trait of Agreeableness on privacy concern. However, we did not find the hypothesized effect of the trait of Neuroticism. Additionally, we found an effect on the trait of Extraversion. Both Agreeableness and Extraversion had a positive effect on privacy concern, meaning that an individual that shows high levels of Agreeableness or Extraversion would perceive higher privacy concern. Moreover, the participants' comments suggested that there are individual differences with regards to which information to disclose in relation to the three factors.

8 FUTURE DIRECTIONS

Our results suggest that there is merit in modeling factors that influence privacy concern for users of group recommender systems. In this section, we outline the implications of our findings and offer suggestions for future work.

Individual (privacy) user modeling. The qualitative comments from participants demonstrate that individuals perceive privacy concerns differently, e.g., depending on different personality traits participants varied in terms of which information they found sensitive. Further work is required to investigate the different information types, in a granular way – allowing us to study when people prefer to disclose or hide the different types of information.

Group (privacy) user modeling. In this study, we saw a tension between the preference of the person being in the minority preference-wise and the rest of the group who was in the majority. E.g., when one user wants to hide their location, but the other two users do not. Our next research steps will therefore build on the work of preference aggregation strategies (e.g., [11, 30]), and study how to reconcile these differences in privacy concern when generating explanations to the entire group.

These should lead us ultimately to design and automatically generate privacy-preserving explanations for group recommendations adapted to all three factors (personality, type of relationship, and preference scenario).

REFERENCES

[1] Solomon E Asch. 1956. Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological monographs: General and applied* 70, 9 (1956), 1.

[2] Gaurav Bansal, Fatemeh Mariam Zahedi, and David Gefen. 2016. Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management* 53, 1 (2016), 1–21.

[3] Colin J Bennett. 1992. *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

[4] Aylin Caliskan Islam, Jonathan Walsh, and Rachel Greenstadt. 2014. Privacy detective: Detecting private information and collective privacy behavior in a large social network. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. 35–46.

[5] Bruno Chauvin, Daniele Hermand, and Etienne Mullet. 2007. Risk perception and personality facets. *Risk Analysis: An International Journal* 27, 1 (2007), 171–185.

[6] An-Jung Cheng, Yan-Ying Chen, Yen-Ta Huang, Winston H Hsu, and Hong-Yuan Mark Liao. 2011. Personalized travel recommendation by mining people attributes from community-contributed photos. In *Proceedings of the 19th ACM international conference on Multimedia*. 83–92.

[7] Paul T Costa and Robert R McCrae. 1992. *Neo personality inventory-revised (NEO PI-R)*. Psychological Assessment Resources Odessa, FL.

[8] National Research Council et al. 2007. *Engaging privacy and information technology in a digital age*. National Academies Press.

[9] Ralf De Wolf, Koen Willaert, and Jo Pierson. 2014. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 35 (2014), 444–454.

[10] Franz Faul, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. 2007. G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods* 39, 2 (2007), 175–191.

[11] Alexander Felfernig, Ludovico Boratto, Martin Stettinger, and Marko Tkalčič. 2018. Explanations for Groups. In *Group Recommender Systems*. Springer, 105–126.

[12] Donelson R Forsyth. 2018. *Group dynamics*. Cengage Learning.

[13] Lewis R Goldberg. 1992. The development of markers for the Big-Five factor structure. *Psychological assessment* 4, 1 (1992), 26.

[14] Jonathan L Herlocker, Joseph A Konstan, and John Riedl. 2000. Explaining collaborative filtering recommendations. In *Proceedings of the 2000 ACM conference on Computer supported cooperative work*. ACM, 241–250.

[15] Daniel Herzog and Wolfgang Wörndl. 2019. User-centered evaluation of strategies for recommending sequences of points of interest to groups. In *Proceedings of the 13th ACM Conference on Recommender Systems*. 96–100.

[16] Daniel Herzog and Wolfgang Wörndl. 2019. A User Study on Groups Interacting with Tourist Trip Recommender Systems in Public Spaces. In *Proceedings of the 27th ACM Conference on User Modeling, Adaptation and Personalization*. ACM, 130–138.

[17] Anthony Jameson. 2004. More than the sum of its members: challenges for group recommender systems. In *Proceedings of the working conference on Advanced visual interfaces*. 48–54.

[18] Oliver P John, Sanjay Srivastava, et al. 1999. The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research* 2, 1999 (1999), 102–138.

[19] Iris A Junglas, Norman A Johnson, and Christiane Spitzmüller. 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems* 17, 4 (2008), 387–402.

[20] Öykü Kapcak, Simone Spagnoli, Vincent Robbemond, Soumitri Vadali, Shabnam Najafian, and Nava Tintarev. 2018. Tourexplain: A crowdsourcing pipeline for generating explanations for groups of tourists. In *Workshop on Recommenders in Tourism co-located with the 12th ACM Conference on Recommender Systems (RecSys 2018)*, Vol. 2222. CEUR.

[21] Bart Piet Knijnenburg. 2015. *A user-tailored approach to privacy decision support*. Ph.D. Dissertation. UC Irvine.

[22] Bart P Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71, 12 (2013), 1144–1162.

[23] Bart P Knijnenburg and Martijn C Willemsen. 2015. Evaluating recommender systems with user experiments. In *Recommender Systems Handbook*. Springer, 309–352.

[24] Melinda L Korzaan and Katherine T Boswell. 2008. The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems* 48, 4 (2008), 15–24.

[25] Jonathan Lazar. 2010. Feng. JH; Hochheiser, H. Research Methods in Human-Computer Interaction.

[26] Yuan Li. 2012. Theories in online information privacy research: A critical review and an integrated framework. *Decision support systems* 54, 1 (2012), 471–481.

[27] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[28] Stephen T Margulis. 2003. On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues* 59, 2 (2003), 411–429.

[29] Judith Masthoff. 2004. Group modeling: Selecting a sequence of television items to suit a group of viewers. In *Personalized digital television*. Springer, 93–141.

[30] Judith Masthoff. 2011. Group recommender systems: Combining individual models. In *Recommender systems handbook*. Springer, 677–702.

[31] Kevin McCarthy, Maria Salamó, Lorcan Coyle, Lorraine McGinty, Barry Smyth, and Paddy Nixon. 2006. Group recommender systems: a critiquing based approach. In *Proceedings of the 11th international conference on Intelligent user interfaces*. 267–269.

[32] Soha A Mohamed, Taysir Hassan A Soliman, and Adel A Sewisy. 2016. A context-aware recommender system for personalized places in mobile applications. *Int. J. Adv. Comput. Sci. Appl* 7, 3 (2016), 442–448.

[33] Shabnam Najafian, Oana Inel, and Nava Tintarev. 2020. Someone really wanted that song but it was not me! Evaluating Which Information to Disclose in Explanations for Group Recommendations. In *Proceedings of the 25th International Conference on Intelligent User Interfaces Companion*. 85–86.

[34] Shabnam Najafian and Nava Tintarev. 2018. Generating Consensus Explanations for Group Recommendations: an exploratory study. In *Adjunct Publication of the 26th Conference on User Modeling, Adaptation and Personalization*. ACM, 245–250.

[35] Lara Quijano-Sanchez, Christian Sauer, Juan A Recio-Garcia, and Belen Diaz-Agudo. 2017. Make it personal: a social explanation system applied to group recommendations. *Expert Systems with Applications* 76 (2017), 36–48.

[36] Rashmi Sinha and Kirsten Swearingen. 2002. The role of transparency in recommender systems. In *CHI'02 extended abstracts on Human factors in computing systems*. 830–831.

[37] Daniel J Solove. 2005. A taxonomy of privacy. *U. Pa. L. Rev.* 154 (2005), 477.

[38] Daniel J Solove. 2008. Understanding privacy. (2008).

[39] Sanjay Srivastava, Oliver P John, Samuel D Gosling, and Jeff Potter. 2003. Development of personality in early and middle adulthood: Set like plaster or persistent change? *Journal of personality and social psychology* 84, 5 (2003), 1041.

[40] Nava Tintarev and Judith Masthoff. 2007. A survey of explanations in recommender systems. In *2007 IEEE 23rd international conference on data engineering workshop*. IEEE, 801–810.

[41] Nava Tintarev and Judith Masthoff. 2009. Evaluating recommender explanations: Problems experienced and lessons learned for evaluation of adaptive systems. In *In the workshop on User-Centred Design and Evaluation of Adaptive Systems in association with UMAP'09*. Citeseer.

[42] Nava Tintarev and Judith Masthoff. 2015. Explaining recommendations: Design and evaluation. In *Recommender systems handbook*. Springer, 353–382.

[43] Thi Ngoc Trang Tran, Müslüm Atas, Alexander Felfernig, Viet Man Le, Ralph Samer, and Martin Stettinger. 2019. Towards Social Choice-based Explanations in Group Recommender Systems. In *Proceedings of the 27th ACM Conference on User Modeling, Adaptation and Personalization*. ACM, 13–21.

[44] Zhu Wang, Xingshe Zhou, Zhiwen Yu, Haipeng Wang, and Hongbo Ni. 2010. Quantitative evaluation of group user experience in smart spaces. *Cybernetics and Systems: An International Journal* 41, 2 (2010), 105–122.

[45] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 12, 12 (2011), 1.