WILL YOU ACCEPT AN APP?  
EMPIRICAL INVESTIGATION OF THE DECISIONAL CALCULUS BEHIND THE ADOPTION OF APPLICATIONS ON FACEBOOK

Completed Research Paper

Nicole Eling  
Technische Universität Darmstadt  
Chair of Software Business & Information Management  
Hochschulstraße 1, 64289 Darmstadt, Germany  
eling@is.tu-darmstadt.de

Hanna Krasnova  
Universität Bern  
Institute of Information Systems  
Chair for Information Management  
Engelhardstrasse 8, 3012 Bern Switzerland  
hanna.krasnova@iwi.unibe.ch

Thomas Widjaja  
Technische Universität Darmstadt  
Chair of Software Business & Information Management  
Hochschulstraße 1, 64289 Darmstadt, Germany  
widjaja@is.tu-darmstadt.de

Peter Buxmann  
Technische Universität Darmstadt  
Chair of Software Business & Information Management  
Hochschulstraße 1, 64289 Darmstadt, Germany  
buxmann@is.tu-darmstadt.de

Abstract

Despite a rapidly increasing number of third-party applications on Facebook and, as a consequence, exploding concerns regarding their data handling practices, little is understood about the rationale behind app installation decisions. Following a Grounded Theory approach and drawing on the results of 20 interviews and textual responses of 392 subjects, we propose a unified model of users’ decision-making process when installing a Facebook app. We conceptualize the decisional calculus behind the adoption of applications and locate it in the proposed process model. To complement our findings, we analyze results of the experiment, finding that trust in the app provider and intrusiveness of the information request have a significant impact on willingness to accept an app for experienced users. The effect of trust, however, disappears once friend recommendation is involved. Nonusers are found to be insensitive to these secondary factors, rather aligning their behavior with the perceived value of the app.

Keywords: Facebook applications, Privacy, Social networks, Trust
Introduction

The decision of Facebook (FB) to open its platform for third-party applications (apps) in 2007 was the beginning of a breathtaking success story: Since then the amount of social apps has mushroomed reaching a whopping 10 million applications and websites, which are integrated with the FB platform generating a yearly revenue of $1.96 bn. (Facebook 2013a). At first sight, all participants in this social media ecosystem appear to benefit from this unprecedented development: The platform owner FB participates in the revenues generated by app developers; companies praise apps for revolutionizing their approach to engage, reward and get to know (potential) customers (Kalra and Shi 2010); and users are offered a wide spectrum of innovative, functional, and entertaining software products magnifying their social user experience (Claussen et al. 2011; Russell-Bennett and Neale 2009).

However, with FB users installing approximately 20 million apps daily (Pring 2012), more and more concerns regarding their extensive usage are raised (e.g., Perez 2009; Steel and Fowler 2010). In contrast to other contexts, third-party apps on FB enjoy a unique privilege to collect and process a wide array of private information pieces provided by users and their friends. Indeed, while users can rely on FB privacy settings, when they share information with their selected audiences, this protective barrier is of little value when it comes to interacting with Facebook applications. In fact, third party applications can potentially access a wide array of information pieces including name, picture, birthday, gender, check-ins, relationship status, and even private messages (Wang 2012), provided a user consents to a “permission” request. Considering the scale and sensitivity of information items FB apps can access, participating stakeholders and scholars increasingly question the rationale behind users’ behavior in this context. Their concerns are aggravated by the fact that already in 2008 Felt and Evans (2008) showed that 90 % of the 150 most popular FB apps requested more personal data than they actually needed to perform the promised functionality. Moreover, an investigation of the Wall Street Journal revealed that all of the 10 most popular FB apps transfer users’ information (and three of them even friends’ information) to outside companies – despite the fact that such practices are not allowed by FB (Steel and Fowler 2010).

As of now, little is known about the cognitive dynamics behind users’ decisions to install applications on Facebook. Indeed, does intrusiveness of an information request deter users from accepting a “permission” of an app? What other mechanisms underlie decisional calculus of users in this privacy-sensitive context? To address these issues, we employ a multi-method approach to develop and validate a process model of applications’ adoption on FB. By conceptualizing the decisional calculus behind the adoption of applications on FB and locating it in the proposed process model, we uncover the intricate web of cognitive processes governing user behavior in this unique context.

Related Work

Building on baseline models and theories, like the Technology Acceptance Model (Davis 1989), Diffusion of Innovation Theory (Rogers 2010), and Theory of Planned Behavior (Ajzen 1991), adoption decisions have been analyzed in a wide array of settings (e.g., the meta-study of Williams et al. 2009). However, to the best of our knowledge, only few research insights exist uncovering the unique properties of the adoption process in the context of FB apps (e.g., Besmer and Lipford 2010; Russell-Bennett and Neale 2009). This is rather surprising, considering their high economic and practical relevance; as well as their unique characteristics that question applicability of existing findings on adoption from other IT-related domains. One of these unique characteristics is that as part of the adoption process applications typically ask to access private information items of potential users that initially were provided to be shared with friends only. Here, FB differentiates between various categories of permission requests: For example, the permission Basic Information (BI), which is requested by default by all FB apps, allows to access a limited set of user’s data (e.g., Facebook ID, name), while the Extended Profile Properties (EPP) permission category, allows the application to get hold of various pieces of detailed information (e.g., photos). In sum, access to over 40 information pieces can be gained in this process (Facebook 2013b; Wang 2012). Considering this vast potential for privacy intrusion that is being explicitly signaled to the user in his or her first interaction with an application, it is plausible to expect that the decisional calculus behind the adoption decision will exhibit diverging patterns from those described in previous research. Another distinguishing characteristic of the app adoption process is reflected in its social nature, which is
particularly visible at the "point of contact". For example, Nazir et al. (2008) identify users’ walls as a primary advertising mechanism for FB apps, suggesting that the diffusion process is strongly influenced by network effects.

These distinctive characteristics of the adoption process are also discussed in the literature studying FB apps from other angles. This stream of research can be divided into studies on adoption and usage of FB apps on a market scale (e.g., Claussen et al. 2013; Gjoka et al. 2008; Nazir et al. 2008) and app usage on the individual level (e.g., King et al. 2011). Former category of studies reveals that the popularity distribution of apps is highly skewed with 10% of the top ranked applications accounting for approximately 98% of total installations (Gjoka et al. 2008). Therefore, it is increasingly hard for new and unknown apps to capture top ranks. Moreover, in a recent study, Claussen et al. (2013) find that policy changes in the FB ecosystem further promote this "super star effect" (Rosen 1981).

While only few studies have taken an individual perspective on applications’ adoption and use, their insights nevertheless provide a valuable foundation for our study. For example, Russell-Bennett and Neale (2009) find that social or emotional value combined with functional value of an app trigger users to recommend this app to friends. Corroborating this finding, Besmer and Lipford (2010) identify social interaction as the major factor in app usage. They argue that social interaction is “coloring” users' perceptions of information disclosure. This effect becomes especially important, against the backdrop of the “Privacy Calculus” theory (Dinev and Hart 2006), according to which individual self-disclosure is a result of conflicting beliefs regarding expected benefits and privacy risks (Krasnova et al. 2010c). Following this argumentation, Kessler (2012) speculates that users may trade their personal data for the utility they receive from such an exchange. Nonetheless, King et al. (2011) find that many users do not understand how apps work and which kind of information apps have access to. This is in line with Wang et al. (2011), who argue that it is hard for users to understand the permissions largely due to their chaotic display and the fact that permission dialogs fail to sufficiently inform users about the actual scope of information access and use. These findings, in turn, have triggered an interesting discussion to help users during the respective privacy-related decision – for example Besmer et al. (2010) propose an approach based on “social navigation”. Further, Wang et al. (2011) argue for increasing transparency of acceptance dialogs and enabling users with more control regarding the data a specific app collects. In addition, the authors suggest to alert users if an already accepted app violates global privacy settings. Those results are complemented by traditional research on consent dialogs, which identifies an array of factors that influence users’ reaction to privacy warnings and end-user license agreements, including presentation of the dialog, users' willingness to trust the platform, habituation effects, limited knowledge and desire to complete the primary task (Böhme and Köpsell 2010; Egelman et al. 2008).

Taken together, even though traditional IT adoption models, complemented by well-established theories such as Privacy Calculus and the results of research on consent dialogs and privacy warnings provide a useful starting point for our research, very little is known about the cognitive dynamics that drives users’ decisions to install FB apps. Furthermore, the research on IT adoption has traditionally been dominated by empirical studies employing survey methods, which lead to recent calls for more methodological diversity when investigating user acceptance decisions (e.g., Williams et al. 2009). Considering the explorative nature of our research, we respond to this call by combining a qualitative study with a quantitative experimental design to examine decisional calculus behind FB app adoption – our focal research question.

**Qualitative Study**

**Data Collection and Sampling**

While many research methods focus on verifying existing theory, Grounded Theory (GT) as developed by Glaser and Strauss (1967) aims at theory construction. This method is especially suitable for our research question, as the adoption and usage of FB apps has hardly been studied so far. According to GT approach, theory is generated systematically from the data. This way the developed theory has fit and is relevant (Glaser 1978). In this study, we use GT as an analytical tool to gather first insights into the dynamics of an individual’s decision process when installing FB apps. By conducting a qualitative study we are able to gain an in-depths understanding of the cognitive processes involved and to obtain a comprehensive
overview of the factors affecting a user’s decision to install a FB app. As discussed by Glaser (1978), data collection and data analysis should be conducted in parallel. Hence, we collected three types of data: (1) initial interviews, (2) follow-up interviews involving elements of participatory observations and (3) textual data obtained in response to an open question in a survey with 392 subjects. Specifically, in the first stage (1), we conducted eight semi-structured interviews with university students. Respondents were asked various open-ended questions regarding their behavior when handling app requests. In order to get as close to the real situation as possible, respondents logged in to their FB account and talked about the apps already installed. Then, four different FB apps were shown to them in order to obtain a better understanding of users’ decision process when installing apps on FB. On average, interviews lasted 30 minutes.

Insights from these initial interviews served as basis for the execution of the twelve follow-up interviews – stage two (2) of our study. After initial questions regarding respondents’ usage of FB apps (e.g., “How many FB apps do you have?” or “How often do you use FB apps?”), five FB apps were presented to the respondents. These apps varied with respect to several factors (e.g., degree of trustworthiness of the app provider) in order to elicit respondents’ preferences and views when facing a variety of application scenarios. Specifically, this way we could test whether users processed different apps differently or whether there were general processing patterns. The scenario design was based on the findings from our initial interviews. For example, since perceived value emerged as a minimum requirement for accepting an app in the initial interviews, respondents were presented with FB apps having the functionality of five widely used FB applications. This way, their existing popularity was used as an indicator of their utilitarian or hedonic value (Davis et al., 1992; van der Heijden, 2004). Furthermore, since in the initial interviews trust in the app provider and the number of users arose as important factors influencing users’ decision to accept an app, we additionally manipulated these two variables. In order to vary provider’s trustworthiness we used well-known, reputable providers and widely known app names for the “high trust” scenarios and unknown providers and unknown app names for the “low trust” scenarios respectively. To manipulate the number of users we displayed 10 000 users for “popular” and 75 for “unpopular” user scenarios. For all five apps, we kept the level of intrusiveness of requested permissions constantly high. All apps asked for Basic Information, E-Mail Permissions, information items from Public Profile/ Friend List and Extended Profile Properties of permission categories as well as for the Extended Permission “publish action” (Facebook, 2013b). For each scenario, we asked respondents about their willingness to install the presented FB app and about the reasons leading to their decision. In case of respondents mentioning high risks associated with the information request, we additionally asked, whether it would influence their decision if only Basic Information and E-Mail permission were requested.

In addition, respondents were asked if their decision would change if they received a personal (e.g., when personally meeting a friend) or standardized friend’s request (e.g., standardized friend recommendation appearing as a notification in user’s Facebook account). Concluding the interviews, respondents were asked to state the three most important factors when deciding about the installation of an app.

In order to complement our findings, in the third step (3), 308 open-ended responses from a survey with a student sample (n=392) were coded and analyzed. Respondents were asked to “... describe how you generally decide whether to install a FB app” resulting in a data corpus of 89,444 words. Note, that this question was part of the quantitative study described in detail in the following section (“Experimental Study”).

**Data Analysis**

We follow the Glaserian approach to GT with open, selective as well as theoretical coding (Glaser, 1978). In contrast to the Straussian approach, in the Glaserian approach, categories are not fitted to the data but rather emerge from it. Another important difference is the availability of numerous coding families in contrast to the use of one paradigm model (Matavire and Brown, 2008; Urquhart et al, 2010). In the stage of open coding, the data is coded line by line to generate an emergent set of fitting and relevant categories and their properties (Glaser, 1978). The following quotation illustrates open coding procedure as applied in our study: “*Functionality (category: usefulness) is for me the most important, followed by friends using it (category: usage within a reference group) and number of users (category: number of users)*” (quotation Q). For open coding, the software atlas.ti.7.0.89 was used. In the next step – selective coding –
coding is limited to the variables related to the core category. The core category is determined by assessing several criteria such as centrality, frequent reoccurrence, and number of relationships to other categories. In our study, decisional calculus emerged as core category. In the final coding stage theoretical codes are applied. Glaser (1978) describes 18 coding families which are not mutually exclusive but overlap considerably, thereby allowing for a high degree of flexibility.

**Results of the Qualitative Study**

Based on our analysis of the two sets of interviews, we developed a process model reflecting users' decisional calculus when accepting a FB app. In order to facilitate reading, we first give an overview of the model illustrated in Figure 1, providing a detailed description of the major constructs in the following subsections.

---

1. In Figure 1, the numbers in brackets indicate the number of interviews in which the category was mentioned, the total number of quotes within the interviews and the number of survey responses.
2. As the scope of the open-ended question was very narrow, not all categories were mentioned.
Summarized in Figure 1, the model describes the cognitive process a user undertakes when deciding about the acceptance of a FB app. Indeed, according to our analysis, decisional calculus emerged as a core category in our data and is central to our model. Situated around this core category, the model encompasses four additional major categories, namely primary assessment, intervening conditions, the decision’s context as well as resulting actions and outcomes. The decision process is embedded in a context, which influences all of the other categories. When a user encounters an app, first, a primary assessment takes place. Depending on the point of contact, the user’s general attitude towards FB apps and a user’s value estimation of the respective app, a first assessment of the app is formed. If the result of this primary assessment is negative the user exits the process by ignoring the app. In case there is a positive assessment, the user clicks on the link to the FB app and thus, proceeds to the permission dialog. In this permission dialog (permission request) actual decisional calculus takes place. The user is presented with information about the functionality of the app as well as the requested permissions and has to decide whether to accept or reject the app. When deciding, users mainly focus on three core aspects: (1) perceived value, (2) risks/costs associated with the intrusiveness of the information request and (3) trust in the app (provider). These three factors are weighted against and influenced by each other during decisional calculus. Decisional calculus, in turn, is influenced by several intervening conditions including substitutability of the app or availability of requested data. As a consequence of a user’s intention formed during decisional calculus a respective action / outcome takes place.

**Primary Assessment:** Before the permission request is displayed to the user, s/he first has to click on a link directing to the app. The decision to undertake a “click” is based on a primary assessment by the user. The three relevant factors for this assessment are point of contact, general attitude towards FB apps and value estimation. If the result of primary assessment is negative, the user skips decisional calculus and does not further consider the app. Otherwise, the user proceeds to decisional calculus, on which primary assessment has an important impact.

Evidently, getting in contact with a FB app works as a trigger for an individual’s decision process. Three possible points of contact were discussed by our respondents: (1) the app is recommended by a friend, (2) the user encounters the app occasionally and (3) the user actively searches for it. The type and context of the encounter can greatly influence primary assessment as well as the results of decisional calculus. This can be especially significant, when a user is not actively searching for an app. While standardized friend requests are typically ignored — e.g., “If I just get a message like ‘Your friend sent you an app’ I wouldn’t click on it” (Q) — a personal message by a friend can change the final outcome. For instance, when asked for his willingness to install, one of the respondents stated: “Probably no; unless a friend would recommend it to me” (Q)³. Thus, a personal recommendation has the power to change a respondent’s decision. Inevitably, this effect is a function of the relation to the friend. Thus, ten respondents noted that the influence of a friend’s recommendation greatly depends on the closeness of their relationship: “First, I check the friend that sends it. If he knows what I am interested about, if it’s a good friend or relative.” (Q) The same holds for situations in which a user encounters the app occasionally. If good friends with similar interest were using the app, respondents were more inclined to accept the app “If I see many friends of mine using the app, I would accept it.” (Q)

In addition to the actual point of contact, an individual’s general opinion about FB apps plays a major role in the primary assessment. Specifically, if the general opinion about FB apps is very negative, users may not even access the permission dialog, but ignore the app request completely. For instance, one of the respondents stated “I do not think about it, I reject right away.” (Q) This is confirmed by the survey in which 145 respondents stated a general aversion towards FB apps, which in 87 cases led to not even considering the installation (see step (3) of data collection and analysis described in the “Data Collection and Sampling” section). At the same time, as the analysis of our interviews reveals, respondents with a high degree of aversion towards FB apps were willing to take a closer look at the app if friend’s recommendation was involved. Finally, preliminary estimation of the app value — based on the scarce information signals such as the logo of the app provider or the app category — is an important component of the primary assessment. If the app does not provide sufficient value, the user most likely ignores it.⁴

³ Some quotes are edited for style and translated to English.
⁴ Since in our interviews final permission dialog served as a basis for discussion (no app invitation was shown), the category “value estimation” was not directly discussed by respondents. However, since indirect evidence hints at the relevance of this factor, this category was included into our model (Figure 1) and is depicted in brackets.
Core Category – Decisional Calculus: With more than 150 mentions for each of the three sub-categories – perceived value, risks/costs, and trust – decisional calculus arose as a core category in our analysis. When engaging in the decisional calculus respondents reported to weight perceived value against predicted costs, while simultaneously accounting for the signals of trustworthiness of the app (provider), which is in line with the Privacy Calculus Theory discussed by Dinev and Hart (2006) in other settings. In the context of FB apps, perceived value comprises usefulness, fun and interest. As FB apps are offered free of any monetary costs, the price, respondents face are the permissions requested by the FB app. Thus, users need to weigh their gain by using the app against the privacy intrusion caused by granting the permissions. For instance one of the respondents commented “I weigh the benefits and the information for which the app receives access against each other.” (Q). Similarly, another respondent stated “Up to now, I have not encountered an app, where I assessed the sale of my data in relation to the provided benefit and the fun factor as justified.” (Q) This calculus is further influenced by trust, which can greatly reduce perceived risks “Considering that it is from a trusted institution, I would not have such big issues disclosing my data.” (Q) as well as enhance perceptions of perceived value “Such an app is always interesting to me, as in my opinion all internet users have something to do with the provider.” (Q).

Perceived Value: According to our data, perceived value is one of the most important factors influencing the acceptance of an app. Indeed, in 52% of the cases the first thing mentioned by the respondents, when asked about their assessment of the app, was its perceived value. If an app was neither considered as interesting, useful nor fun, respondents were not willing to install the considered app, independent of all the other factors: “I would definitely not do it. [...] I would not even know what value the app has for me.” (Q) In contrast, if perceived value was very high, it could overrule everything else “If it is really an offering that interests me, then I think for myself that the company will be ok and I don’t care about the actual permissions.” (Q).

In our setting, perceived value was evaluated across an array of axes, including perceived usefulness, interest, and fun. Importance attached to perceived usefulness is in line with the findings from prior IT adoption literature. Following the Technology Acceptance Model (Davis 1989), perceived usefulness as well as the later added construct perceived enjoyment both represent important factors influencing an individual’s adoption decision (Davis et al. 1992). Depending on the type of system, utilitarian or hedonic, either perceived usefulness or perceived enjoyment plays a greater role regarding an individual’s decision to adopt a new technology (van der Heijden 2004). Extending the definition by Davis (1989) in which perceived usefulness is defined as “the degree to which a person believes that using a particular system would enhance his or her job performance”, in our context, perceived usefulness is not restricted to job performance but performance in general. It serves as an umbrella term encompassing various aspects such as functionality (e.g., “I would take a look at the app [...] because it is ride sharing” (Q)), need of the app (e.g., “But I still allowed it, because I needed it.” (Q)), and personal gain (e.g., “For this app I do not know what my advantage would be.” (Q)). The categories fun and interest describe users’ considerations about how much fun they might have when using the app in the future and if using the app would be interesting for them. Thus, these two categories are very similar to perceived enjoyment as defined by Davis et al. (1992). For instance, one respondent noted “I think I would take a closer look at this one because it looks interesting.” (Q). Perceived ease of use – the third integral part of the Technology Acceptance Model (Davis et al. 1992) – was hardly mentioned by the respondents and thus, was not included in the model.

Risks/Costs associated with the Intrusiveness of the Permission Request: Following our data, risks/costs can be subdivided into five facets. The risk, mentioned most often throughout the 20 interviews we conducted (166 quotes) revolved around the apps accessing personal user information – data access. In addition, risks of data usage, as well as the risks associated with the app posting in user’s name – loss of control over posting – arose as important categories. Risks related to fraud and data linkage across networks were also discussed, but were mentioned less often. In the following, we discuss the three most important risks respondents were concerned about.

When considering the intrusiveness of the requested permissions in terms of data access respondents typically first noted the length of the permission list – amount of requested information – and then mentioned one or two items especially sensitive for them to underline their objections: “That is just too much for me. Especially that they can access photos and posts and that in addition, they can also post in my name is quite a lot for me.” (Q) Thus, they considered both, the amount of permissions as well as the
sensitivity of the requested items. Particularly photos appear to be seen as highly sensitive as this permission was especially emphasized by respondents in nine of twelve follow-up interviews. Another aspect considered when pondering about the associated costs of data access included the necessity of the requested items for the performance of the app’s functionality. In cases there was an evident mismatch between permissions requested by an app and those actually needed to provide a promised functionality, respondents were considerably more inclined to reject the permissions: “I just ask myself why they need my photos. I don’t understand it at all. I think that’s awful. That’s why I would not do it.” (Q)

With respect to risks related to data usage, 14 respondents stated to be concerned about data transfer to third parties and the usage of their data in order to send advertising and spam messages. Others were insecure about how their data might be used and therefore, tended to refrain from using the apps.

In contrast to the other permissions, which mainly request data access rights, the permission “publish actions” allows the app to post to a user’s and his friends’ streams (Facebook 2013b). According to our data, this permission magnifies perceived risk as users do not only have to give up information to an app, but also partially lose control over their communication and self-representation on FB. In addition, to a general dislike regarding this kind of privacy intrusion – “Nobody can post on my wall and I don’t want it to post on the walls of my friends.” (Q) – interviewees were concerned about molesting their friends. For instance one of the respondents of the survey considered if “the app unasked annoyed [his] friends with invitations and status updates” (Q).

Trust in the App (Provider): In addition to perceived value and risk, trust in the app (provider) – mentioned 181 times throughout the interviews – arose as the third major factor involved in decisional calculus. Interestingly, one of the first comments made by respondents, when considering an app, was whether they were familiar with the app or provider – “Yes, I think I would click on App 1. I sometimes shop there.” (Q) – or not – “App 2 does not tell me anything. […] I do not know it.” (Q). Depending on their degree of familiarity respondents either relied on their experience with the app and its reputation or, if they did not know the offering, they relied on hints as number of users or app rating. Aspects, further promoting the feelings of trust included perceived intention of provider, integrity of offering as well as the first impression of the app. Once trust was established, the willingness to install an app increased greatly. For instance one of the respondents stated “I make the decision [as follows]: If I need it and I trust it, I install it. If I don’t trust it, I reject and if I need it, but I don’t trust it, I reject.” (Q).

Intervening Conditions: Following our data, decisional calculus as described above, is contingent on several intervening conditions. For instance, perceived substitutability of the FB app by other offerings may play an important role. Specifically, once respondents were interested in the functionality of an app, they compared the app’s peculiarities regarding factors such as privacy intrusiveness and trustworthiness of the provider with the peculiarities of similar FB apps or alternative offerings like web pages or mobile apps. Consecutively, they selected the offering that best met their requirements. For example, for one app, eight of the twelve respondents in the follow-up interviews stated that they would rather use the alternative known app instead of the presented app they had never heard of.

The effect of substitutability can be mitigated by other intervening conditions such as usage within a reference group, number of users and rating. When these factors were high, this was interpreted as a sign of quality, reliability and relevance, serving as foundation of users’ trust towards the app. Especially usage by a reference group such as friends can have a considerable effect: “If friends of mine would be using it, this would be a sign of quality, that this is something good.” (Q). In contrast, if the rating of the app did not reach a certain threshold, respondents were less inclined to install the app “For instance this app has only three stars. I would look, why it has only three stars.” (Q). Finally, according to our data, the number of users can have a positive effect on users’ trust towards the app “I would check how many people use the app, I look at the information, but if it’s what I need and it’s used by millions of people I would accept it.” (Q).

Further, availability and sensitivity of the requested data can influence the salience of perceived risks in users’ decisional calculus. Specifically, respondents whose profile did not contain a lot of data or who used fake accounts were oftentimes more willing to accept FB apps than other respondents “Maybe if I would have posted many photos and personal information about my preferences, I would be more concerned about that, but I haven’t posted about my favorite movies and stuff.” (Q).
**Context:** Various aspects such as, among others, relation to FB, user’s previous experience, knowledge, habit, and personality constitute the context around user’s decision to install a FB app. These aspects can be structured into two groups: (1) user characteristics and (2) FB-related user factors. As part of the sub-group (1) user characteristics, a user’s personality and mood builds the background for his or her decision process. While there are users who are very rational and weigh all factors against each other (e.g., “I am quite rational.” (Q)), others solely decide according to their current mood “It depends on my mood. Sometimes I am in a mood where I say: ‘It doesn’t matter, I will disclose all my information.’ And other times I think: ‘Why should I disclose all my information?’” (Q). Another particularly important category is user’s general privacy concern, with many respondents having stated to be worried about data access and the usage of personal data for spam in general.

Amidst FB related user factors, a user’s relation to FB emerged as very important factor. In cases when respondents did not like FB or used it predominantly as communication tool, they tended to have fewer apps than very active users and they did not use them as intensively: “I use Facebook more for talking and communication with friends rather than app.” (Q) Thus, this relation to FB was closely connected with FB app installation. Further, depending on previous experiences, respondents form attitudes towards FB apps in general: “Depends on the app but the majority of apps are games and then I think it’s just tiring.” (Q). Many of the respondents in our sample had only restricted prior knowledge about apps and permissions and therefore, had difficulties evaluating the permission requests “You get some kind of description; I have no idea what it is. I just clicked because I wanted to read it [an article shared by friends].” (Q). Since information request is always structured the same way, respondents who are accustomed to using FB apps, develop a habit in processing these requests which eventually influences decisional calculus “All of these agreements ask for the same things. I have read this a thousand times.” (Q). “This is in line with past research on end-user license agreements, which also suggests “habit” as a critical component of users’ decisional outcomes (Böhme and Köpsell 2010).”

**Actions and Outcomes:** Decisional calculus only takes place when the primary assessment of the app is positive and the link to the app is clicked. Otherwise the user ignores the app and does not further consider it. Once the request is clicked, the permissions as well as the description of the app are displayed. This, in turn, triggers decisional calculus which then leads to the respective action. Specifically, when the outcome of the decisional calculus was positive, respondents tended to install it without further hesitation “I would definitely click on it. I like it.” (Q) In contrast, if the assessment throughout decisional calculus was very negative, respondents clearly rejected the app: “No, I would not install this because they want to access my private data and I don’t want that. That’s why I don’t do it.” (Q). In cases where the willingness to install was weak, respondents tended to postpone their decision or to reject the app. “I don’t think so. Sounds quite nice, but it’s not really something I definitely need.” (Q) In some cases, when respondents were very concerned about permissions or the lawfulness of an offering they decided to investigate further before making a decision. Specifically, in this case, they searched for more information on the internet or asked friends about their experiences. When it comes to being more proactive, only five of all respondents were willing to recommend apps to a friend themselves – “When I really think the app is very interesting for that person or can be very useful, then yes.” (Q) This is due to the fact that recommending an app to someone involves stronger dedication and effort than just accepting the app, as the user does not only consider his own interest but also the interest of his friends “Yeah, I would recommend an app, but only to friends that might be interested.” (Q). This finding may also provide additional explanation to the fact why people attach such strong value to friend recommendation throughout the phase of primary assessment.

**Experimental Study**

**Motivation**

Our analysis of qualitative data reveals that point of contact and general attitude towards FB apps represent two important heuristics first processed in users’ decision-making process. Have these criteria been processed and met, factors such as perceived value, risks/cost associated with the intrusiveness of the information request, but also perceptions related to trust in the app provider may flow into users’ assessment. However, while providers can typically do little to change users’ general attitudes towards FB
Security and Privacy of Information and IS

apps, users’ perceptions of value and point of contact at a given point in time, intrusiveness of the permission request and trust beliefs can be managed (Krasnova et al. 2010a) and, hence, their role in the decisional calculus is of high interest to app providers. Nonetheless, the impact of these determinants appears to be characterized by high complexity and is contingent on a variety of contextual conditions. For example, while some interviewees lamented intrusiveness of the information request, they associated little risk with accepting it in the view of their low activity on FB: “Probably I would [accept it], because I don’t have the information in my profile. But it would bother me” (Q). Moreover, respondents appeared to evaluate intrusiveness of information requests differently when a known vs. unknown provider was involved, suggesting a possible interaction between risk and trust perceptions: “I automatically trust big names, because if there is a big scandal they get harmed, and I think that’s why they try to keep the data safe” (Q). Considering that only users who have a positive attitude towards FB apps in general and see some value in a considered app represent a real target audience for an app provider, investigating the role of intrusiveness of the information request and trust in the app provider in the decision-making process emerges as particularly critical. To deepen our understanding of this cognitive dynamics, an experimental study was conducted investigating this main decisional calculus. This is in line with Glaser (1992) who argues that even though GT is typically used in conjunction with qualitative data (e.g., Koroleva et al. 2011a; Schalow et al. 2013), quantitative evidence can also be drawn into the analysis to enrich emerging propositions (Pace 2004); and to verify the presence of the identified effects with a bigger sample (Krasnova et al. 2010b). Overall, experimental designs get increasingly common in privacy-focused studies, since they allow gaining an unbiased view on the causality and factor interactions behind complex decision-making processes in this area (Xu et al. 2012).

**Experimental Design**

To achieve the goals of our study, a 2-by-2 experiment was conducted, in which a permission dialog for a sweepstake app was presented to respondents (see Figure 2).

Our choice of the sweepstake was dictated by the relevance of this app category for page providers and marketers. Indeed, numerous industry reports provide evidence for the power of sweepstakes in increasing user engagement and stimulating conversion rates (Delo 2011). For example, a recent case study has shown that a FB contest app with daily prizes resulted in a considerable lift in daily “likes” of page content (Kirkpatrick 2012). However, our interviewees had a mixed reaction towards this category of FB apps: “I would think that this is just another sweepstake where they want to collect my data and where I […] do not have any benefits” (Q). In the light of these controversies, there appears to be a pressing need to better understand user behavior in this important but underexplored context. In the experiment, permission dialog presented to respondents described the sweepstake as a “Giveaway App: Win One of Several iPads”. iPads were chosen as a reward since they can help to improve the learning engagement and provide a valuable prize that users would be likely to share with their Facebook friends.
experience for students (a primary target group in our sampling procedure); can be used in both hedonic and utilitarian ways; and also enjoy a strong brand image of Apple products (Badenhausen 2012). Hence, using iPads as a reward was likely to set significant incentives to install the app (Muntinga et al. 2011), ensuring that the criteria of perceived value was fulfilled.

Following the logic above, two factors were manipulated in our experiment and their influence on users’ willingness to accept an app (in terms of likelihood) was explored: trust towards app provider (high vs. low) and intrusiveness of an information request (high vs. low). While this set of factors was found to play a role across a variety of applications discussed in our interviews, these determinants gain additional meaning in the sweepstake context. Specifically, since FB allows page providers only a limited insight into their fan base, sweepstakes are commonly used to elicit more information about page fans (Gingerich 2013). Hence, issues concerning a possibly deterrent impact of the information request in this process inevitably emerge as pertinent. At the same time, only scarce research findings consult application developers in this regard (e.g., Krasnova et al. 2013). Furthermore, since winning a reward is the primary goal of participation in sweepstakes, trustworthiness of the provider of the sweepstake may be of particular importance, since it may substantiate the reward promise and signal that the sweepstake is not a fake: “If it was a different provider, I would have rejected it right away” (Q). However, despite the importance of the sweepstake instrument for both “no name” and well-known companies with trust-evoking brands, little is known about whether the success of sweepstake apps is directly associated with the trustworthiness of the provider behind it. Summarizing, exploring the role of trust in the app provider and intrusiveness of the information request as independent predictors of users’ willingness to install a sweepstake represent research tasks of significant theoretical and practical relevance.

Specific manipulation conditions have been implemented as follows. The logo of our well-known reputable university was used for “high” trust manipulations. This is in line with past research, which provides substantial evidence that reputation (Jarvenpaa et al. 1999) and familiarity (McKnight et al. 2002) represent significant premises for trusting beliefs to develop. Since the university in question belongs to the top 100 among universities worldwide (Times Higher Education 2012-2013), our choice was justified. For “low” trust scenarios, a logo of a fictitious provider “ZO GmbH” (no registered trademark) was self-developed (see Figure 2).

To develop a manipulation with “low” intrusiveness of the information request, the permission structure of a set of application types comparable to sweepstakes – quizzes, promotions and giveaways – was studied based on Socialbakers (2012) (see Table 1). Besides basic information, the three most common information items: email, user likes, and user birthday, were included to represent scenarios with “low” intrusiveness. Following FB approach to structuring information within permission dialogs, our information items resulted in 3 bullet points, which is reflective for the app types presented in Table 1 with a mean number of bullet points of 2.71, 2.07 and 1.78 (own analysis). For scenarios with “high” intrusiveness, besides basic information, 14 user-information items have been requested: email, birthday, likes, about me, activities, education, groups, interests, location, religious and political views, former employer, events, status updates and photos; and 6 friend-related items have been incorporated: birthday, education, location, former employer, events, and status updates. Further, two permissions from the “extended permissions” category were included: “publish_stream” and “read_stream” - enabling an app to post and access user’s News Feed respectively. In sum, our permission requests included ten bullet points (see Figure 2).

<table>
<thead>
<tr>
<th>Table 1: Top Permission Requests in Categories Promotions, Giveaways and Quizzes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Promotions, top 20</strong></td>
</tr>
<tr>
<td>basic_info 85.0% u_about_me 20.0%</td>
</tr>
<tr>
<td>email 55.0% u_birthday 15.0%</td>
</tr>
<tr>
<td>u_likes 45.0%</td>
</tr>
<tr>
<td><strong>Giveaways, random 20</strong></td>
</tr>
<tr>
<td>basic_info 75.0%</td>
</tr>
<tr>
<td>email 40.0%</td>
</tr>
<tr>
<td>u_likes 25.0%</td>
</tr>
<tr>
<td><strong>Quizzes, top 30</strong></td>
</tr>
<tr>
<td>basic_info 90.0%</td>
</tr>
<tr>
<td>email 40.0%</td>
</tr>
<tr>
<td>u_birthday 13.3%</td>
</tr>
</tbody>
</table>

5 Only permission requests with a frequency of more than 10% are listed. Full list is available from the second author.
6 Only giveaway applications with monthly active users (MAU) >= 1000 users were considered.
The online link to the survey was advertised using a mailing list of one German university, whose logo was also used in “high trust” scenarios. A raffle of thirty EUR10 Amazon.de gift cards was used as an incentive to take part. Upon accessing the survey respondents were randomly assigned to one of the four scenarios. After studying the presented permission request, respondents were asked to answer a set of closed and open questions (see Table 2 for more information). All survey items were initially developed in English and then carefully translated into German.

<p>| Table 2: Operationalization, Means and Cronbach’s Alpha of the Variables Used in the Survey |</p>
<table>
<thead>
<tr>
<th>Construct / Scale Items</th>
<th>Mean (SD)</th>
<th>CA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Willingness to Accept an App</strong> (DV</td>
<td>Scale: 1=absolutely not; 2=rather not; 3=rather yes; 4=definitely yes</td>
<td>self-developed)</td>
</tr>
<tr>
<td>InstallAsIs. How likely are you to accept this application?</td>
<td>1.35 (.58)</td>
<td>n.a.</td>
</tr>
<tr>
<td>InstallFRRe. How likely are you to accept this application if it was recommended?</td>
<td>1.60 (.71)</td>
<td></td>
</tr>
<tr>
<td><strong>Intrusiveness of the Information Request</strong> (MC</td>
<td>Scale: 1=very little; 2=little; 3=some; 4=many; 5=very many</td>
<td>self-developed)</td>
</tr>
<tr>
<td>IIR1. In order to use this app, I would have to give it access to the following amount of my personal information items:</td>
<td>2.63 (1.04)</td>
<td>n.a.</td>
</tr>
<tr>
<td><strong>Trust in the App Provider</strong> (MC</td>
<td>5-point Likert Scale</td>
<td>based on McKnight 2002)</td>
</tr>
<tr>
<td>TR1. ...competent in protecting my personal data.</td>
<td>2.04 (1.00)</td>
<td>.85</td>
</tr>
<tr>
<td>TR2. ...has my interests in mind when it comes to my personal data.</td>
<td>1.93 (1.00)</td>
<td></td>
</tr>
<tr>
<td>TR3. ...trustworthy when dealing with the data I provide.</td>
<td>2.06 (1.00)</td>
<td></td>
</tr>
<tr>
<td>TR4. ...honest when it comes to using my personal data.</td>
<td>2.41 (1.11)</td>
<td></td>
</tr>
<tr>
<td>TR5. ...to have more to lose than to gain by misusing the data its users provide.</td>
<td>2.45 (1.22)</td>
<td></td>
</tr>
<tr>
<td><strong>Perceived Value</strong> (Covariate</td>
<td>5-point Likert Scale</td>
<td>partly based on Davis (1989), Davis et al. (1992)</td>
</tr>
<tr>
<td>USF1. This app appears useful to me.</td>
<td>1.89 (.99)</td>
<td>.86</td>
</tr>
<tr>
<td>USF2. This app appears interesting for me.</td>
<td>2.10 (1.16)</td>
<td></td>
</tr>
<tr>
<td>USF3. It will be fun to use this app.</td>
<td>1.78 (.94)</td>
<td></td>
</tr>
<tr>
<td><strong>Subjective Amount of Self-Disclosure</strong> (Ad Hoc Covariate</td>
<td>Scale: 1=never; 7=several times a day</td>
<td>(Koroleva et al. 2011b)</td>
</tr>
<tr>
<td>How often do you:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDA1. ...comment.</td>
<td>3.48 (1.47)</td>
<td>.77</td>
</tr>
<tr>
<td>SDA2. ...post photos.</td>
<td>2.11 (.75)</td>
<td></td>
</tr>
<tr>
<td>SDA3. ...update status on FB.</td>
<td>2.49 (1.21)</td>
<td></td>
</tr>
<tr>
<td><strong>Subjective Sensitivity of Self-Disclosure</strong> (Ad Hoc Covariate</td>
<td>5-point Likert Scale</td>
<td>self-developed)</td>
</tr>
<tr>
<td>SDS1. Information which I provide on FB is of very personal nature.</td>
<td>2.55 (1.08)</td>
<td>.67</td>
</tr>
<tr>
<td>SDS2. I share some private details when I communicate on FB.</td>
<td>3.14 (1.12)</td>
<td></td>
</tr>
</tbody>
</table>

Specifically, respondents had to state their willingness to accept the suggested app: “How likely are you to accept this application (“as is”)? (InstallAsIs); and “if it was recommended by a friend” (InstallFRRe) – our dependent variables. The following parts included additional questions and manipulation checks (MCs). Respondents had to indicate how many apps they have already installed – recoded into dichotomous values: “none” and “at least one” – responses to this question (AttGen) were used as a proxy to discern respondents with positive and negative attitude towards apps in general – a primary heuristics identified in our qualitative analysis. MC for the intrusiveness of the information request was
implemented using a single-item measure as shown in Table 2; MC for trust in the app provider was implemented using a 5-item scale based on McKnight (2002). To control for the influence of value perceptions – a critical component of the decisional calculus (see Figure 1) – perceived value was captured using a 3-item scale, which reflected the basic value proposition of the apps as uncovered in the analysis of the qualitative data.

Further, since availability of (requested) data emerged as an important intervening condition in our qualitative analysis, we additionally measured the extent of information sharing on FB using three different approaches. First, to elicit an objective value for the amount of data accessible via FB profile, subjects were asked to indicate whether they provided each of the 17 items, which can also be requested within a permission request (e.g., birthday, likes, status updates, photos). The self-disclosure score (SDSc) was derived by summing up items with affirmative responses (min=0; max=17). Second, we have captured the subjective amount of self-disclosure, revealed on one’s profile and in communication with others, by asking respondents about the frequency with which they commented, posted photos and updated their status on FB. Third, the subjective sensitivity of self-disclosure was captured using a self-developed 2-item scale to provide insight into the self-assessed personal nature of data respondents provided on their FB profiles – information applications can potentially gain access to.7

Sampling

A net of 392 respondents took part in the survey (100/93/98/101 per manipulation). 62.3%/37.7% were female/male. Majority of respondents were students – 93.2%. The median age was 24 years old. 93.3% spent most of their life in Germany. In terms of FB use, 48.2% stated to use FB up to 30 minutes a day. 6% used FB for more than 3 hours each day. The median number of FB friends reached 180. 64.2% admitted to have never installed any app. In terms of information disclosure, out of 17 items were asked for, the largest share of respondents – 89% – have liked at least one page; 87% provided photos; 81% shared status updates. Using a one-way ANOVA we did not discover any significant differences in terms of gender, number of FB friends, time on FB, number of apps installed and self-disclosure score across different treatment groups, which provides evidence that randomization worked well.

Data Analysis

First, performance of our experimental manipulations was assessed: The mean difference for “low” vs. “high” level of intrusiveness of the information request for a IIR1 item was statistically significant (p=0.004); the difference was also significant for “high” vs. “low” level of trust in the app provider, across all respective items TR1-TR5 (p-value<=0.001) (Cronbach’s Alpha (CA)=0.85). Taken together, experimental conditions were successfully manipulated. Next, a two-by-two analysis of covariance (ANCOVA) was conducted to understand the dynamics behind users’ willingness to install an app “as is” (InstallAsIs) and “if it was recommended by a friend” (InstallFRRe), which were entered into the analysis separately as dependent variables. This approach has allowed us to discover differences in the decision-making process for these two different possibilities for the point of contact (specifically, occasional encounter vs. friend recommendation), as suggested by our qualitative analysis.

We iterated our analysis for three (sub-)samples – app users, non-users and the overall sample based on AttGen – so that in total six models were assessed (see Tables 3 and 4). The fixed independent factors were intrusiveness of the information request (Intr.) and trust in the app provider (Trust). Items measuring perceived value (PV) of the app have exhibited a high internal consistency of 0.86 measured by CA (Nunnally 1978) and were highly correlated: Spearman’s rho ranged from 0.692 to 0.737 (p<0.01). This outcome corroborates our qualitative findings, suggesting that when assessing the value of the app, respondents’ beliefs about the apps’ usefulness, interest and entertaining value flow into the overall individual perception of the app’s value. Hence, a factor score obtained as a result of principle component analysis on the responses to this 3-item scale was treated as a proxy of perceived value (PV) and was entered as a covariate into the analysis to control for the perceptions of perceived value in users’

7 For a full list of items please consult Table 3 / columns 1 and 5 in Krasnova et al. (2013).
8 Please note that a series of additional questions, not reported in this study, were also part of the questionnaire: this analysis is presented in Krasnova et al. (2013).
decisional calculus. Additional ad hoc tests were conducted by entering self-disclosure score (SDSc), and factor scores for subjective amount (SDA) and sensitivity of self-disclosure (SDS) as additional covariates into our model to control for the influence of these factors, following our qualitative findings.

From the start, the fulfillment of the ANCOVA assumptions has been examined. The minimum requirement of 5 cases per cell was met. Second, reliability of multi-item (main and ad hoc) covariates – PV, SDA, SDS – was verified using CA, which surpassed the required threshold of 0.7 (CA for SDS was only slightly below: 0.67) (Nunnally 1978). Next, assumption of the normal distribution of the dependent variable and covariate was verified. Even though this criterion was not met for the specific variables in our analysis (e.g., skewness statistic=1.425; 0.977; 0.569 / kurtosis statistic =1.047; 0.523; -0.764 for InstallAsIs, InstallFRRe and PV respectively), ANCOVA was found to be robust to this violation (Norman 2010; Schwab 2007). Further, a correlation analysis has shown a strong and significant (with one exception) relationship (p<0.05) between our dependent variables (InstallAsIs / InstallFRRe) and covariate(s) (rPV=0.49/0.44; rSDSc=0.22/0.22; rSDA=0.15/0.17; and rSDS=0.13/0.04 n.s.). Assumption of the homogeneity of regression slopes was assured by specifying a custom model for interaction terms between independent variable and covariate(s). Since p-value of interaction terms across all models (InstallAsIs / InstallFRRe | app users / non-users / overall sample) was above a cut-off level of 0.05, this assumption was met. Finally, Levene’s test of the equality of error variances was passed for all models we tested. The only exception was the model estimated for the overall sample with InstallAsIs as a dependent variable (see column 3 in Table 3). However, since the variance ratio was less than 3, we can consider our analysis to be robust to this violation (Schwab 2007). Taken together, our data is well-suited for the ANCOVA analysis summarized in Tables 3 and 4.

<table>
<thead>
<tr>
<th>Table 3: Results of the ANCOVA Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependent Variable</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>n of sample</td>
</tr>
<tr>
<td>Factors</td>
</tr>
<tr>
<td>Trust</td>
</tr>
<tr>
<td>Intr.</td>
</tr>
<tr>
<td>Intr. x Trust</td>
</tr>
<tr>
<td>Perc. Value</td>
</tr>
<tr>
<td>R²adjusted</td>
</tr>
</tbody>
</table>

Ad Hoc Analysis (for better readability, results are provided only in the case of p-value<0.1)

<table>
<thead>
<tr>
<th></th>
<th>SDSc</th>
<th>SDA</th>
<th>SDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.9*(.02)</td>
<td>n.s.</td>
<td>6.03**(.02)</td>
<td>n.s.</td>
</tr>
<tr>
<td>2.65* (.02)</td>
<td>n.s.</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
</tbody>
</table>

Significance values: **p-value<0.05; *p<0.1; *?p=0.106; n.s. - not significant.

Of most interest are the findings reported for those users who have already installed at least one app – “app users” – and, hence, represent a “target group” for app providers (columns 1 and 4 in Tables 3/4). We find that when no friend recommendation is involved both intrusiveness of the information request and trust in the app provider play a role in users’ decisional calculus (column 1 in Tables 3/4) for this sub-group. Specifically, when trust is high, users are more likely to accept an app (Madjusted high=1.776 vs. Madjusted low=1.472; p=0.002); the same is true when an app requests for less (as opposed to more) information items (Madjusted high=1.503 vs. Madjusted low=1.745; p=0.013).
Table 4: Estimated Marginal Means (Standard Errors) for Willingness to Accept an App

<table>
<thead>
<tr>
<th>Manipulation</th>
<th>Willingness to Accept “As Is”</th>
<th>Willingness to Accept “if Recommended”</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>column</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sample</td>
<td></td>
</tr>
<tr>
<td></td>
<td>app users</td>
<td>non-users</td>
</tr>
<tr>
<td><strong>Trust in the App Provider</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“low” - trust</td>
<td>1.472 (.07)*</td>
<td>1.222 (.04)</td>
</tr>
<tr>
<td>“high” - trust</td>
<td>1.776 (.07)</td>
<td>1.190 (.04)</td>
</tr>
<tr>
<td><strong>Intrusiveness of the Information Request</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“low” - intr.</td>
<td>1.745 (.07)</td>
<td>1.241 (.04)</td>
</tr>
<tr>
<td>“high” - intr.</td>
<td>1.503 (.07)</td>
<td>1.171 (.04)</td>
</tr>
</tbody>
</table>

*grey cells are used when significant effect has been found (see respective cells in Table 3).

Even though we do not find support for the presence of interaction effect between intrusiveness of the information request and trust in the app provider (p-value=0.166), examination of the plot presented in Figure 3 may still hint at a potential presence of this effect conditional on a larger sample size. To be interpreted with great caution, Figure 3 for “install “as is” (InstallAsIs)” case (on the left), suggests that when trust in the app provider is low, respondents make little differentiation between high and low level of intrusiveness of the information request – their willingness to accept an app remains low. However, for app providers who appear trustworthy, magnitude of information request is of greater importance, with less intrusive requests being more likely to be accepted. Nonetheless, considering the non-significance of the interaction effect reported in this study and a low level of explanatory value of this model component (PEtaS=0.02), these effects cannot be seen as verified based on our data. Even so, it would be advisable for future research to investigate the presence of these effects with a larger sample of respondents.

Interestingly, when an app is being recommended by a friend to an app user (column 4 in Table 3 and 4), likelihood of acceptance is contingent on the intrusiveness of the information request (Madjusted[^1] = 1.808 vs. Madjusted[^2] = 2.114; p=0.009), and does not depend on the trust in the app provider (p=0.228). Apparently, friend recommendation acts as a substitute for providers’ trustworthiness in this case.

Finally, we find that for non-users, if friend recommendation is not given (column 2 in Table 3), no factor is important besides PV (column 2 in Table 3). This outcome clearly suggests that users, who are not
attracted to apps in general and do not have an additional stimulus to consider them (e.g., in the form of friend recommendation), do not take additional cognitive efforts to examine secondary privacy and trust-related factors. As expected, our covariate — perceived value — was significantly related to the willingness to accept an app in all models we tested. Taken together, our results are in line with qualitative analysis which shows that perceived value, general attitude and point of contact define the presence and importance of the subsequent cognitive processes involved in the evaluation of FB apps.

Finally, a series of ad hoc analyses have revealed a mixed picture regarding the link between amount and sensitivity of information disclosed in one's profile and users' willingness to accept an app. In cases when the relationship was significant (see rows SDSc, SDA, SDS in Table 3), respondents with little and less sensitive information where also more likely to reject an app, which is in contrast to the interviewees' self-reports. A possible explanation behind this incongruence can be traced to the low level of recall of respondents when commenting on their self-disclosure in a face-to-face interaction with an interviewer. Moreover, respondents who reveal less information on FB can be more concerned about their privacy to begin with and, hence, also reject FB apps for this reason. Overall, including SDSc, SDA, SDS separately as covariates did not have a noticeable effect across the models we tested.

**Discussion**

While there is a growing body of research regarding privacy, trust and IT adoption, studies investigating these topics in the context of FB apps are still very scarce. To close this gap, in this study we develop a model reflecting an individual’s decision process when installing FB apps. Based on the analysis of the qualitative data, “decisional calculus” arises as the core category in our model. In the process of decisional calculus three factors are weighted against each other — perceived value, risks/costs, and trust. Note that this is in line with Privacy Calculus Theory, which states that an individual’s decision about information disclosure is a result of weighing perceived benefits and associated risks against each other (Dinev and Hart 2006; Krasnova et al. 2010c).

Decisional calculus as the core category is embedded in four additional categories comprising the process model — primary assessment, intervening conditions, context and actions and outcomes. Primary assessment embraces three factors — point of contact, general attitude towards FB apps and value estimation. With respect to the point of contact especially social aspects play an important role. This is in line with Besmer and Lipford (2010) who show that friend recommendation can positively influence users’ perceptions of information disclosure. Indeed, our qualitative analysis reveals that friend recommendation increases users’ willingness to install a FB app. This finding suggests that future research regarding privacy calculus with respect to FB apps should consider these aspects. When it comes to intervening conditions, social aspects play an important role as well. Specifically, decisional calculus can be influenced by the number of users as well as the usage by a reference group. This complements the finding of Claussen et al. (2013) that the diffusion process of FB apps is strongly influenced by network effects. In addition, our qualitative findings indicate that the proposed decisional calculus is affected by the substitutability of the FB app in question as well as the information disclosed on FB. This, however, is in contrast to our quantitative results that show that the amount of disclosed information is positively correlated with the willingness to disclose. This might be explained by the fact, that people who in general are not concerned about privacy and disclose a lot are also less concerned about granting the permissions. Considering these controversies, we urge future research to further investigate this domain. The context of decisional calculus consists of various categories also discussed in literature on permission dialogs. For example, our qualitative study complements the findings by previous studies which state that many users have problems to understand how apps work (King et al. 2011) and that habituation effects can influence the processing of the permissions (Böhme and Köpsell 2010).

In addition to our theoretical contribution, our research provides various implications for practitioners. First, app providers who have low initial trust should engage in trust enhancing measures as trust has a positive effect on the acceptance of a FB app. Second, providers should carefully consider if a high number of permissions is worth the loss of potential users, deterred by the intrusiveness of the information request. Thus, especially in the case of sweepstakes, which in many cases, aim at generating “likes”, it seems advisable to avoid intrusive information requests. Third, considering the relevance of network effects in the FB app context, FB app providers should try to support the viral promotion of their apps, e.g.,
by allowing users to easily relate to the app on their newsfeeds. However, if the amount of app requests is too high and the message to impersonal, the positive effect of word of mouth might be reversed as users feel annoyed by spam “Some people send me requests for applications. That makes me really tired.” (Q).

Fourth, as users with a general aversion towards FB apps will hardly ever install any FB apps, in the short run, app providers should try to focus on the app affine group of FB users. However, in the long run it might be promising to invest in the overall promotion of FB apps in order to improve the users’ general attitude towards them.

The presented model of the FB app adoption process might also be transferred to user decisions in the context of the Facebook Connect network. This network offers a convenient way to login to websites, since the same consent dialogue as for FB apps is used. Egelman (2013) describes the user decision in this context as privacy / convenience tradeoff, since FB transfers various information pieces to the requesting web site after the user has granted the permissions. Beside this, various parts of the model could be generalized to the context of other social applications (e.g., other social networks that plan to offer apps).

All in all, our research integrates various research findings into one comprehensive process model of the FB app installation process. Our quantitative study complements this model providing interesting insights into the decisional calculus of users especially with respect to friend recommendation and the interplay between user perceptions of the intrusiveness of information request and trust in an app provider.

Limitations and Future Research

This study is subject to several limitations, which, however, can be seen as promising opportunities for future research. First, a major constraint of this study is our concentration on hypothetical behavior – especially against the backdrop of the special link between behavioral intentions and actual behavior in the privacy context (cf. Smith et al. 2011). Therefore, the next step in our research program will be to validate our findings in a real environment, exposing users to existing applications, instead of their proxies. Second, dependent variables in our study have been captured with single-item measures. While this approach was chosen to keep the survey as short as possible to increase response rate, future studies should address this limitation by capturing more markers of user behavioral intentions to reduce the sources of measurement error. Third, both dependent variables in our study were measured on a 4-point scale, with most respondents tending to “reject” an app. Hence, undesirable floor effects may potentially arise – a limitation of most IS studies using ordered dependent variables. Fourth, alternative methods of study design and analysis should be considered: For example, the value of structural equation modeling in experimental designs has recently been demonstrated by Xu et al. (2012). Finally, in our experimental study we have chosen to concentrate on sweepstakes scenarios. While sweepstakes provide great value for companies, helping them to attract new and engage existing fan base, other types of applications dominate Facebook landscape, including business-and entertainment-oriented apps and different forms of social utilities (Socialbakers 2012). Moreover, contrasting anecdotal evidence suggests that sweepstakes are likely to attract unengaged reward-seeking users, resulting in lower future engagement rate and, hence, causing a page more detriment than value in the long-run (Hochberg 2011). Hence, future research may concentrate on exploring decisional calculus for other categories of apps to ensure greater external validity of the findings.

Conclusion

Analyzing two sets of interviews with Grounded Theory methodology, we developed a process model of the decisional calculus a user undertakes when installing a FB app. In the second step, we complemented our qualitative insights by conducting a quantitative study with 392 respondents. Our results indicate that especially two categories of primary assessment, namely point of contact as well as general attitude towards FB apps can interfere with decisional calculus. Specifically, users’ trust in the app provider and his or her perceptions of the intrusiveness of the permission request exert a differential impact on users’ willingness to install an app when different points of contact / attitudes are at hand. All in all, our findings can serve as a basis for further research on the decisional calculus in the FB app context and can help researchers and practitioners investigating the underpinnings of user behavior in this emerging privacy-sensitive context.
References


Times Higher Education 2012-2013. "Times Higher Education World University Rankings " Retrieved 03.05.2013


