Dangers of 'Facebook Login' for Mobile Apps: Is There a Price Tag for Social Information?

Completed Research Paper

Hanna Krasnova
Universität Bern
Institute of Information Systems
Engehaldenstraße 8, 3012 Bern, Switzerland
hanna.krasnova@iwi.unibe.ch

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

Olga Abramova
Humboldt-Universität zu Berlin
Berlin, Germany
olga110290@mail.ru

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

Abstract

Social networks offer horizontal integration for any mobile platform providing app users with a convenient single sign-on point. Nonetheless, there are growing privacy concerns regarding its use. These vulnerabilities trigger alarm among app developers who fight for their user base: While they are happy to act on users' information collected via social networks, they are not always willing to sacrifice their adoption rate for this goal. So far, understanding of this trade-off has remained ambiguous. To fill this gap, we employ a discrete choice experiment to explore the role of Facebook Login and investigate the impact of accompanying requests for different information items / actions in the mobile app adoption process. We quantify users' concerns regarding these items in monetary terms. Beyond hands-on insights for providers, our study contributes to the theoretical discourse on the value of privacy in the growing world of Social Media and mobile web.

Keywords: Social media, Privacy, Information privacy, User behavior, Facebook Login

Introduction

In a rapidly changing field of Social Media and mobile, Facebook (FB) strives to assert itself as a social layer for many forms of apps, platforms, and web-connected devices, all of which may profit from being connected around the social graphs of participating members (Darwell 2012). As of now, FB offers horizontal integration for any mobile platform, including iOS and Android, providing app users with a convenient single sign-on point in the form of FB Login (also formerly known as FB Connect) (White 2013). Emphasizing its advantages, FB boasts a high conversion rate for prominent apps, with 80 % of potential users accepting permissions requested via FB Login. Beyond offering a more streamlined login experience for users, use of FB Login also promises significant gains for app providers, including increased retention, engagement, higher in-app purchasing, and greater virality. For example, Shazam has witnessed a rush growth of 47 % for FB-connected users since launching with Open Graph (Osofsky 2012). Importantly, the option of FB Login offers third-party apps a unique opportunity to seamlessly collect data on their adopters, which ensures better targeting and more marketing insight. While Facebook Login represents one of the most prominent examples of this type of single sign-on mechanism, other social networks as Google+ offer the same type of functionality, illustrating its growing relevance.

While single sign-on via Facebook or other social networks may indeed offer multiple advantages for users and app providers, there are growing concerns about the effect of these efforts on user privacy concerns and, as a consequence, app adoption. Indeed, while users gain the benefits of convenience when engaging with mobile apps via FB Login, they have to - at minimum - sacrifice their basic information on FB, which includes their name, profile picture, gender, networks, user ID and a list of friends. Additionally, apps with FB Login can request other details, including users' "likes", political and religious preferences, relationship status, location, photos, and even personal messages, just to name a few. In a similar venue, apps using Google+ Sign-in can access information of users' public profiles as well as their friend lists in order to optimize their service. All in all, when it comes to information that can be accessed by third party apps – there is no such thing as a "secret" as long as a user consents to it.

These vulnerabilities inevitably trigger concerns among users and, in turn, providers who fight for their user base in an oversaturated market. Indeed, while providers would be happy to access and act on users' information, they are not necessarily willing to sacrifice their adoption rate for this goal – a critical trade-off. For example, only 2.27 % of apps request access to "likes", and 0.72 % to "interests" (Wang 2012) – a surprisingly low number considering the high value of this information for marketers. Indeed, "likes" and "interests" can be effectively used to tailor product offerings and homepage content, magnifying the effectiveness of marketing actions. Moreover, just 14.5 % of European and 6 % of U.S. top online retail platforms have adopted FB Login by 2013 (Cohen 2013b). This timidity might be attributed to the lack of knowledge on how users will react to FB Login itself and a request for information items involved in it.

So far, existence and gravity of this trade-off has remained ambiguous. While some studies suggest that users do not even notice the magnitude of information requested in a consent dialog (Egelman 2013), Eling et al. (2013) show that the amount of information a sweepstake app requests has a significant negative influence on users' willingness to install the app. FB comments on this issue in the following way: "*There is a strong inverse correlation between the number of permissions your app requests and the number of users that will allow those permissions. […] so we recommend that you only request the permissions you absolutely need for your app*" (Facebook Developers 2012). While this statement offers developers a rough guideline, it leaves many blind-spots for providers who may face "intrusiveness – adoption" trade-off in their operations. Indeed, which information items are perceived as more sensitive than others? How does intrusiveness of certain information items benchmark against other characteristics of the app, such as usefulness or number of reviews? Are users ready to pay more for the app so that it does not collect additional information items, and if so how much? Indeed, while viability and financial success of many apps is dependent on the amount and quality of the collected data, "charging for privacy" may be a viable business model (Krasnova et al. 2009). All in all, while these questions are critically important for the rapidly growing industry of mobile apps, little research evidence is available. To fill this gap, we employ a discrete choice experiment to verify the role of the single sign-on feature in the overall mobile app adoption process. We explore the impact of requests for different information items on user decisions, as well as quantify them in monetary terms. By doing so, our study provides hands-on insights for app developers as well as contributes to the growing theoretical discourse regarding the value users attach to their privacy in the novel context of Social Media and mobile web.

Theoretical Background

Several streams of research can inform our work, including studies on mobile / LBS services and apps, FB applications and a more general research on the role and value of privacy from a user perspective.

Adoption of Mobile Apps

A variety of determinants can be responsible for the adoption and continued use of mobile services (Nikou and Mezei 2013). Summarized in Table 1, our review of relevant research suggests that four groups of factors play a particularly important role in individual adoption decisions: perceived benefits, monetary costs, perceived risks to privacy and security as well as social influence. On the benefits side, constructs such as perceived usefulness (e.g., Lu et al. 2005; Malhotra and Malhotra 2009) and perceived enjoyment (e.g., Kim et al. 2008; Nysveen et al. 2005) are often considered. For example, Nikou and Mezei (2013) use Analytic Hierarchy Process to analyze substantial factors behind the adoption of mobile services and show that perceived usefulness (in terms of functionality and added value) represents the most important factor influencing individual adoption decision. While benefits attract users to adopt a mobile service, monetary cost is an impediment to adoption (e.g., Wu and Wang 2005). For instance, Wang et al. (2013a) find a detrimental effect of perceived fee on purchase intention of mobile newspapers after a free trial.

Table 1. Studies on the Determinants of the Adoption of Mobile Applications

Study	**Perceived benefit**				**Social influence**	**Monetary cost**	**Privacy / security**	Method	TAM as a theory	Dependent variable	Context
	Perceived usefulness*	Perceived ease of use	Perceived enjoyment**	Other Benefits***							
Fang et al. (2005)	✓	✓	✓				✓	SU	✓	Intent to use a handheld device	Mobile commerce
Keith et al. (2010)	✓	✓			✓		✓	EX		WTP	LBS
Kim et al. (2008)	✓	✓	✓	✓	✓	✓		SU	✓	Continued intent to use	SMS
Kim et al. (2011)		✓		✓	✓			SU	✓	Behavioral intent, usage behavior	MMS
Lu et al. (2005)	✓	✓			✓			SU	✓	Intent to adopt WIMT	Mobile services
Malhotra and Malhotra (2009)	✓	✓				✓		IN SU	✓	Adoption propensity of wireless web services	Mobile services
Nikou and Mezei (2013)	✓					✓		SU	✓	-	Mobile services
Nysveen et al. (2005)	✓	✓	✓	✓	✓			SU	✓	Intention to use	Mobile services
Pagani (2004)	✓	✓	✓			✓		FG SU	✓	Attitude toward using, behavioral intent to use	Multimedia Messaging Services
Petrova and Wang (2011)	✓			✓		✓	✓	CS		-	LBS
Racherla et al. (2011)				✓	✓	✓	✓	EX		WTPP	Mobile apps

Taylor et al. (2011)					✓			SU		Disposition to use mobile apps	Mobile apps
Wang et al. (2013b)	✓	✓	✓			✓		SU		Purchase continuance intent	Mobile services
Wu and Wang (2005)	✓	✓		✓		✓	✓	SU	✓	Behavioral intent to use	Mobile commerce
Xu et al. (2005)							✓	EX		Behavioral intent	LBS
Xu et al. (2009)						✓	✓	EX		Intent to disclose personal information in LBS	LBS

*Abbreviations: SU – survey; EX – experiment; CS – case study; FG – Focus Groups; IN – Interviews; LBS – location-based services; WTPP – Willingness to Pay and Purchase. *Functionality was also included under this category. **Factors such as perceived enjoyment and perceived playfulness are summarized under this category. ***Includes factors as personalization, quality and compatibility.*

Social influence is another critical driver. Taylor et al. (2011) find that the likelihood of the adoption and usage of an app increases if a user's strongest relationship partner is using this type of applications. In a study of four iPhone apps, Racherla et al. (2011) demonstrate that social information from others increases users willingness to purchase the app and also their willingness to pay for it, with information on reference price from students of the same university having a greater influence than information from all consumers who purchased the app. Interestingly, however, social information did not intervene with the impact of privacy assurance on users' perceptions, suggesting that "*people don't necessarily trust the decisions of those closer to them when it comes to mobile app privacy*" (Racherla et al. 2011, p. 8). Indeed, privacy and security issues represent a major impediment behind the adoption of mobile services (Racherla et al. 2011; Xu et al. 2005; Xu et al. 2009), with consumers ready to pay more for applications providing extra assurance of their privacy via privacy policy or privacy seal (Racherla et al. 2011). All in all, existing studies provide a number of insights into the key factors involved in the adoption of mobile services. However, with some exceptions (e.g., Racherla et al. 2011), many of these studies explore the landscape of mobile services before the arrival of smartphones and an accompanying explosion of the market for mobile apps.

As mobile and desktop uses get increasingly intertwined, users expose significant vulnerabilities in terms of their privacy, giving rise to significant concerns. The option of single sign-on via social networks is particularly controversial: On the one hand, a user is offered a convenient single sign-on point, eradicating the need to remember logins and passwords to multiple accounts. On the other hand, this type of single sign-on mechanism directly connects app users to their social network accounts, at minimum exposing their basic information to a third-party provider. While research on the effects of FB login option is very limited (e.g., Egelman 2013), a number of studies investigate user perceptions and behavior with regard to FB apps, informing our research in this problem area.

Privacy and Facebook Permission Requests

Possibilities for information requests in the context of "pure" FB apps are *identical* to those used in the context of other non-FB mobile or desktop applications. Figure 1 summarizes the three-step process of application installation for Android apps. First, a user has to decide if she/he wants to install a given app. In case the decision is positive, she/he is asked to consent to a set of Android permissions[1]. Once those are granted, the app is downloaded and a user can access it. If FB Login is used, a user is presented with an option to login via FB in step 3. Subsequently, a user is asked for permission to access different information items, which is part of FB Login procedure. Given subjects' consent, apps can thus collect multiple details on users, including those otherwise protected by privacy settings. Several categories of permission requests are distinguished by FB: Request for *(1) basic information* takes place every time a user chooses a FB Login option or installs a FB app. It involves a list of users' friends and a number of basic data items, which are typically publicly available (e.g., user's name, gender). *(2) Email permission* requests access to user's primary email address. An app can also ask for access to *(3) extended profile properties*, which involve 44 information items shared by a user and his or her friends (22 each).

[1] For iPhone, the second step is missing as iPhone Apps do not ask for permissions in this form during installation.

Examples include user / friends' activities, groups, location, relationship details, photos, or "likes". Using (currently) optional *(4) extended permissions* an app can additionally ask to publish stories to a user's profile – an opportunity frequently used to increase virality of an app. *(5) Open graph permissions* and *(6) page permissions* can also be implemented, but are used rarely (Wang 2012).

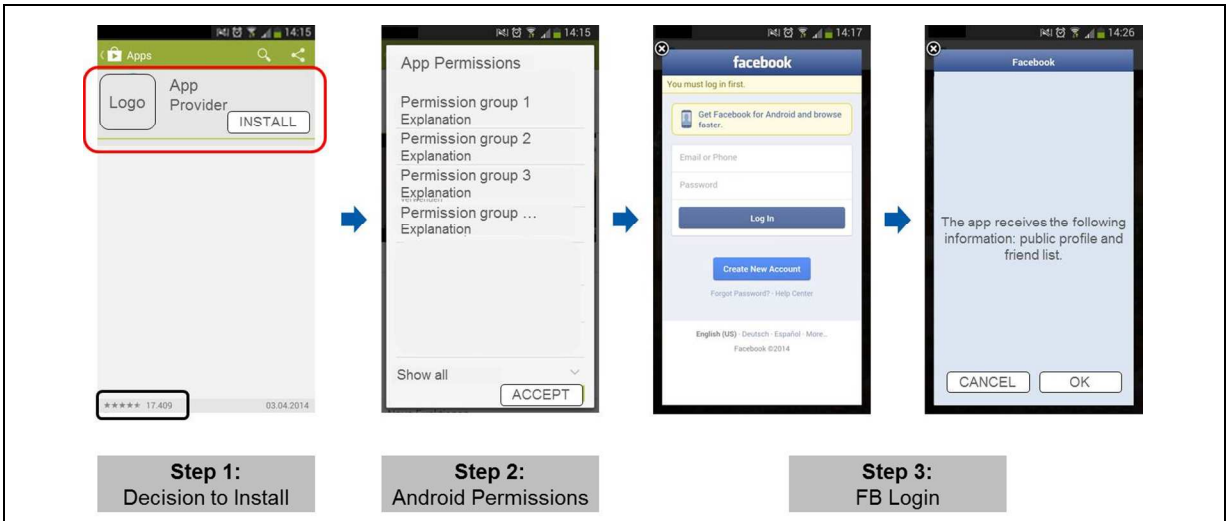

Figure 1. Example of the Android Installation Process

Even though access to user data is contingent on explicit user consent, several studies have questioned the effectiveness of such consent dialogs. Indeed, 20 million apps are installed daily on FB (Pring 2012), suggesting that users may not fully understand the scale of information access requested by FB apps (King et al. 2011). In addition, there is initial evidence that users do not always read complete consent dialogs, possibly as a result of growing habituation (Egelman 2013). A complimentary explanation traces these inconsistencies to privacy calculus of users: While the number of information items requested by an app has a negative effect on the decision to install it, privacy concerns may be dominated by other expected benefits (Eling et al. 2013), with users differentiating between functional and either social or emotional value of applications on FB (Russell-Bennett and Neale 2009).

In an attempt to gain a differential view on the value users attach to privacy in Social Media context, Krasnova et al. (2013) surveyed users regarding their level of concern for numerous information items. Their results suggest that users implicitly distinguish between five information types: *friends' information*, a user's *social information* (e.g., user likes, groups, activities), *basic curriculum vitae information* (email, basic info, hometown and birthday), *extended curriculum vitae* information (e.g., religious and political views, former employer, education), and *visual information* (photos and videos), with concern over the latter being the highest. While these findings provide initial insights into the value of various types of personal data in the context of Social Media, this research is descriptive in nature, and may suffer from "talk is cheap" problem common for privacy surveys (Harper and Singleton 2001, p. 6). To tackle these limitations, a number of approaches have been suggested that allow for a more realistic view on the value users attach to their information and ways to express this value, as discussed below.

Value of Privacy

Presented in Table 2, studies investigating the value users attach to their information privacy and personal data can be classified according to their focus: value of privacy in general vs. value of specific data items; and according to the methods employed in these studies: survey-based direct measures, laboratory / field experiments, and conjoint analysis or discrete choice experiments (DCE).

Table 2. Studies on the Value of Individual Privacy and Personal Data			
Focus / Method	Direct measurement	Laboratory / Field experiments	Conjoint analysis / DCE
Privacy in general	Bauer et al. (2012); Krasnova and Kift (2012); Racherla et al. (2011); Spiekermann et al. (2012);	Beresford et al. (2012); Jentzsch et al. (2012)	Hann et al. (2002); Hann et al. (2007); Krasnova et al. (2009)
Specific types of personal data		Cvrcek et al. (2006); Danezis et al. (2005); Grossklags and Acquisti (2007); Huberman et al. (2005)	Potoglou et al. (2013)

In an attempt to operationalize the value users attach to privacy, some studies directly elicit users' willingness to pay (WTP) for it in various contexts, arriving at different conclusions. For example, in a survey of German students Krasnova and Kift (2012, p. 10) find that when asked to consider that "*information [users] share on FB is not adequately protected and can be used for other purposes (e.g. personalized advertisement)",* users were willing to pay just € 0.29 per month (mean) to FB to avoid secondary use. This is in line with experimental research from other contexts that shows that even small price differences – of one dollar - can lead consumers to select a more privacy-invasive service provider (Beresford et al. 2012; Jentzsch et al. 2012).

In contrast, Spiekermann et al. (2012) arrive at somewhat higher valuations when exploring the impact of users' awareness of existing data markets: Using Becker et al. (1964)'s mechanism (BDM) to elicit users' WTP to keep their FB data (as opposed to it being completely erased) (Bauer et al. 2012), the authors find that the WTP of those users who were notified about the possibility of the secondary use of their data reached € 36 - € 72 (mean; median = € 5); while those in a "control" condition were willing to pay less for their data: € 16 - € 17 (mean; median = € 0). Providing additional evidence for the importance of privacy in the context of mobile applications, Racherla et al. (2011) show that the degree of privacy assurance has a significant effect on individual WTP for four different apps, suggesting that consumers may be willing to pay some premium to achieve greater privacy.

Studies employing 'second price auctions' shed some light on these conflicting findings as they show that the monetary value of individual information items can be dependent on the desirability of the trait (e.g., information on weight in the study by Huberman et al. (2005)), usage purpose (i.e. commercial usage or usage for research purposes) (Cvrcek et al. 2006), and the specific situation (selling information or paying to protect the information) (Grossklags and Acquisti 2007). Moreover, validity of findings obtained especially in the direct approach can be questioned. In these studies, users are placed in an artificial setting and are asked to provide a specific monetary value. While failing to report a truthful number has little consequences, responses can suffer from social desirability bias or/and "talk is cheap" problem (Harper and Singleton 2001). Conjoint analysis and discrete choice experiments can be seen as promising solutions to these problem areas, as they elicit users' preferences by assessing their choices across an array of trade-offs. This way, an experimental situation has a maximum approximation to the real-life settings (Bakken and Frazier 2006; Lambin 2007).

For example, applying conjoint analysis to the case of information disclosure to a web-site, Hann et al. (2002, p. 1) explore trade-offs between three forms of privacy concerns – errors, improper access and secondary use, and two types of benefits – monetary rewards and time savings. The resulting privacy value emerges as quite high: For example, "*disallowance of secondary use of personal information provided on a web-site is worth between $ 39.83 and $ 49.78"* Singapore dollars[2]. Conversely, users will be ready to accept secondary use of their data if offered a monetary reward in this price range. Krasnova et al. (2009) undertake a similar study in the context of Social Networking Sites, and show that users are willing to pay between € 1.18 and € 1.44 per month to insure that an SNS provider does not use their demographic data. Reaching between € 14.16 and € 17.24 when calculated on an annual basis, these numbers are still

[2] Considering exchange rate for January 1st, 2002, this amounts to $ 21.52 and $ 26.89 U.S. dollars respectively.

substantial (even though lower than those of Hann et al. (2002)). Noteworthy, this amount was higher than the amount users were willing to pay to gain extended functionality, suggesting that users have a preference towards privacy when facing 'usefulness-privacy' trade-off. Using DCE approach, Potoglou et al. (2013) study the value users attach to specific information items (e.g., purchase history and email) in the e-business and search engine context. The authors find that 'sharing of personal information with third parties' was negatively perceived, resulting in the highest valuation of £ 5.65 for product purchase and £ 7.28 for service purchase. Moreover, respondents in the e-business scenarios exhibited significant reluctance to choose providers that saved and linked their data to their personal accounts.

Taken together, while existing studies provide a number of relevant insights, there is little research investigating the specifics of social information shared in the Social Media context. In this context, the case of FB Login is highly attractive since it naturally involves "social information" items shared in these settings. Moreover, FB permission requests ask to access social information provided for a different purpose, namely the share and exchange with others on a Social Networking Site. In addition, in contrast to many other complex, abstract, or sometimes unnoticeable warming dialogs and end-user license agreements, permission requests directly confront a user with the data items the application wants to access, which provides a higher degree of priming on these issues. In order to explore the value users attach to their personal data in this novel setting, in this study, we adopt a DCE approach (similar to Potoglou et al. (2013)) to the context of mobile applications with a FB Login option.

Methodology

The Discrete Choice Experiment Approach

In order to determine the value users attribute to different types of information a discrete choice experiment was conducted. This approach allows eliciting consumer preferences in hypothetical settings and helps to identify the independent influence of attributes in the choices made by respondents and their valuation of these attributes. In contrast to conjoint analysis methods that are purely mathematical and are criticized for being inconsistent with economic demand theory, DCEs are based on a long-standing and well-tested concept of choice behavior, referred to as random utility theory (RUT) (Louviere et al. 2010). According to RUT, a rational decision-maker maximizes utility relative to his or her choices. Specifically, an individual i assigns to each alternative j in the choice set I^i a perceived utility or "attractiveness" U_j^i (Cascetta 2009). Under RUT "utility" is a latent construct in the mind of a person, which cannot be totally observed by the researchers (Louviere et al. 2010, p. 62). Formally, it splits up U_j^i into two parts: systematic utility and a random residual.

$$U_j^i = V_j^i\left(X_{kj}^i\right) + \varepsilon_j^i = \sum_k \beta_k X_{kj}^i + \varepsilon_j^i \qquad \forall j \in I^i \tag{1}$$

Systematic utility V_j^i is a mean utility of all individuals having the same choice set as an individual i and is a function of measurable characteristics, or *attributes* X_{kj}^i, related to the alternative itself (e.g., time, costs, service frequency) and to the decision-maker (e.g., income, age) (Cascetta 2009, p. 93). For analytical and statistical convenience V_j^i has a linear form with coefficients β_k estimating each attribute's influence on the choice of an alternative j. *Random residual* ε_j^i represents the deviation of the utility perceived by decision-maker i from the mean value. Because of the random component, utilities are inherently stochastic, allowing to predict not the exact choice of a person, but only the probability with which individual i will choose alternative j conditional on the choice set I^i (Louviere et al. 2010, p. 63). This is the probability that the perceived utility of alternative j is greater than that of all other available alternatives:

$$p^i(j/\, I^i) = Pr\left[U_j^i > U_k^i \;\forall k \neq j, k \in I^i\right] = Pr\left[V_j^i - V_k^i > \varepsilon_k^i - \varepsilon_j^i \quad \forall k \neq j, k \in I^i\right] \tag{2}$$

If ε_j^i are independently identically distributed extreme value type 1 random variables, then the resulting model is the multinomial logit model (MNL). This assumption is "*equivalent to assuming that the unobserved attributes have the same variance for all options in each choice set and that these attributes are uncorrelated over all the options in each choice set*" (Street and Burgess 2007, p. 59). In MNL models the probability of choosing alternative j takes the form of the conditional logit model and expression 2 can be rewritten as:

$$p^i(j/\ I^i) = \frac{\exp(\theta V_j^i)}{\sum_{k\in I^i}(\exp \theta V_k^i)} \quad (3),$$

where θ is a scale parameter and is equal to 1 if an experiment is conducted once, i.e. without repetition (McFadden 1974).

Hence, collecting the choices of survey respondents across different sets of alternatives makes it possible to estimate the parameters of the model and the probability that a certain alternative will be chosen. Moreover, if a vector of denoting attributes comprises a special attribute of cost (price), the estimates can be used to derive consumers' willingness to pay (or willingness to accept) to obtain some benefit (or avoid some cost or situation) from a specific action (Accent and RAND Europe 2010).

Study Design and Choice of the Attributes

The preparation of our DCE included three main steps: (1) model specification, (2) experimental design and (3) questionnaire creation (Rose and Bliemer 2008). To fulfill our purposes, we employed a hypothetical scenario of a mobile app installation procedure, with an option of FB Login. While "pure" FB apps are distributed for free, there is often a price tag for mobile apps that allows us to naturally include the "monetary cost" factor into our experimental set-up.

Since users only see a FB Login and an accompanying permission request if they show active interest in an app (by clicking on it in an app store, see Figure 1), an app has to promise some value proposition in terms of usefulness or other benefits (Eling et al. 2013). To meet this criterion but to avoid reputation effects likely for well-established apps, we selected a relatively new and unknown app DropSpot for our scenarios[3]. This location-based application informs users about their surroundings, e.g., major crime scenes, or well-known film spots. Users can subscribe to the topics of interest to them and will be sent a notification every time they are nearby something that applies to the topic of their choice. For example, by subscribing to the "famous crimes" theme, users will be notified each time they pass a place where a specific crime has happened.

In the model specification step, attributes and their levels had to be specified. According to DCE, selected attributes and levels have to be important for the choice situation considered in the experiment (Rose and Bliemer 2008). Following findings on critical determinants behind an app adoption reported in Table 1, we varied four different attributes, namely (1) monetary cost, (2) perceived benefit (in terms of functionality), (3) social influence and (4) privacy intrusiveness of an app.

Monetary cost: Monetary cost or price is an important impediment of the adoption of mobile services (Wang et al. 2013a). Additionally, this attribute had to be included and varied to allow for calculating monetary values for different levels of other attributes. Moreover, it is interesting to explore the importance of this attribute since the question of whether app providers should charge a fixed price or use other revenue models (e.g., those that rely on user data or advertising) is one of the main practical issues providers face when launching a new app. Since a huge portion of all app downloads are free – 89.6 % in 2012 – (Gartner 2013), this level was included and later used as a reference level in the analysis. The selection of the other price levels was based on the assessment of 500 top paid travel apps in the Google play store (information retrieved on February 3rd, 2014). Following analysis of common price levels, we used the mode value of € 0.99 and median value of € 1.99 as further levels in our model. In addition, we added € 2.99 as a maximum price level because this was one of the prices charged most often for higher priced apps. Moreover, average willingness to pay varies around € 1.99 for iPhone users and Android users accept prices up to € 2.72 on average (Lardinois 2010), which is very close to our maximum price level.

Perceived benefit was modeled by extending the geographical area in which the app could be used. Obviously, this app might prove useful during travel, as users in these situations are less familiar with the surroundings, and an app may help them not to miss out on relevant spots. For this reason, the app only working within the boundaries of a home city will probably be less useful than an implementation with a worldwide coverage. Four levels of this attribute were modeled: (1) place of living (max. one city), (2) Germany (the country of respondents), (3) Europe, and (4) worldwide coverage.

[3] Disclosure Notice: While at the time of the submission the first author was connected to a DropSpot team member, the choice of this particular application idea was dictated by the suitability of the app context for the purposes of the experiment.

Table 3. Attributes Used in the Discrete Choice Experiment in Our Study		
Attribute:	**Description text used in the experiment**	**Levels**
Monetary cost	**Price:** While many apps are offered for free, some apps with extended functionality and more features charge a fee. In our scenarios prices can have one of the following levels:	1) Free 2) €0.99 3) €1.99 4) €2.99
Perceived benefit	**Working range:** Functionality can be limited to one region or the app can have a worldwide reach. If the area is restricted to your place of living, only notifications about interesting places in your home town can be received. An app with a worldwide reach works everywhere. For this attribute the following levels are possible:	1) Place of living (max. one city) 2) Germany 3) Europe 4) Worldwide
Social influence	**Quantity of user reviews:** When downloading an app, the customer is shown a star rating as well as the number of customers who have rated the app. An app can have a maximum of five stars. In our scenarios the following levels are possible:	1) 4 stars, 3 reviews 2) 4 stars, 10 reviews 3) 4 stars, 50 reviews 4) 4 stars, 150 reviews
Privacy intrusiveness	**Type of user login:** After installation some apps display a login dialog. For some apps a user can directly access the app without any login; for others, a user has to login with his/her FB account. When using FB Login, an app automatically receives access to user's basic information from FB profile (in particular, name, profile picture, gender, user ID, friends' list, and all other public information); In addition, the app can ask for additional permissions (e.g., email, likes, or photos). If FB Login is requested, the app can only be used if a user grants corresponding permissions. In our scenarios the following options are possible:	1) No FB Login: the user can directly access the app (no FB information is collected) 2) FB Login: BI 3) FB Login: BI and email (provided on FB) 4) FB Login: BI and likes (referring to your likes of FB pages) 5) FB Login: BI and photos (shared by you on FB) An app can ask a user to be allowed to post in the user's name on FB. These posts are visible for the friends of the user. 6) FB Login: BI and permission to post on your behalf

Social influence: When it comes to app adoption, social influence can take different forms, with app ratings and number of people who provided reviews emerging as key variables in this process (e.g., Keith et al. 2010). Our analysis of star ratings for top apps in Google play store has rendered an average of 4.37 stars for 500 top paid apps and 4.17 stars for 500 top free apps as of April 30th, 2014. All in all, 4 star rating is likely to send a strong signal of app quality (Fu et al. 2013; Vasa et al. 2012). Hence, in our model we decided not to vary the star rating, but kept it fixed to 4 stars to reduce cognitive load for participants. Instead, the number of reviews the star rating was based on was varied. Indeed, Keith et al. (2010) show that network size – as determined by the number of reviews – can significantly reduce location privacy risk, increase perceived usefulness and perceived ease of use. Especially for start-ups, the number of reviews may have an important impact: Even though ratings are designed to serve as a sign of quality, these may be perceived as unreliable if based on only a small number of reviewers (Keith et al. 2010). Considering that the selected app was intended to be largely unknown, relatively low levels have been chosen – 3, 10, 50, and 150 reviews respectively. This way, our study promises relevant insights for new apps who struggle to accumulate the "right" number of reviews to get traction.

Privacy intrusiveness: This study centers on the value users attach to avoiding privacy intrusion, with a specific focus on information items typically shared on Social Media. To model different levels of intrusiveness the following levels have been included: At a baseline, no FB Login was requested and, therefore, no personal data was accessed. In the following levels, users were only offered an option of FB Login with additional requests for information. In its simplest form, FB Login option was only associated

with the access to "basic information" (BI)[4]. For four consecutive levels, we combined this default request for BI with a request for another information item/action. All in all, a resulting number of levels was fixed to six in order to avoid a high number of choice sets and to reduce cognitive load of respondents.

Levels including information items beyond BI were selected based on their practical relevance. Specifically, user "likes" were included because of their relevance for marketers, as they allow them to determine users' preferences, thereby facilitating personalized advertising (Kosinski et al. 2013). For another level, email permission was requested. Email is especially useful for marketers, as it allows them to directly address their customers. Further, in order to test the influence of asking for a very sensitive item, the permission to access photos was included (Krasnova et al. 2013). Finally, previous studies found that users were highly concerned about an app posting in their name (Eling et al. 2013). Since this opportunity is very attractive for app providers as a means of viral marketing, this permission was also included (Cohen 2013a).

All in all, with the distinction between "No FB Login" vs. "FB Login: BI (+ different information items)", an important trade-off for many app developers is addressed. Indeed, providers have to weigh the advantage of being able to identify and learn more about their users with the downside of losing potential adopters to objections against login mechanisms and privacy risks. Table 3 summarizes attributes, their respective levels, and instructions used in the study.

Experimental Design and Questionnaire Creation

Following model specification, in the next step, experimental design and questionnaire were developed (Rose and Bliemer 2008).

While a full factorial design (i.e. 4x4x4x6 = 384 profiles in our study) is desirable in theory, in practice, it can hardly be realized as there would be too many questions. In order to maximize the information obtained from respondents given the limited number of choice tasks, D-efficient design has been used. D-efficient design contains a low D-error (equation *4*), i.e. a low scaled measure of the determinant of an asymptotic variance-covariance matrix (AVC) for the parameter estimates (Rose and Bliemer 2013, p.1026). It is determined as follows:

$$D - error = \left(det(\Omega_N)\right)^{1/K} \quad (4),$$

where Ω_N is the AVC for N respondents, and K is the number of attributes (Rose and Bliemer 2013). We decided to use D-efficient designs as they can provide better parameter estimates than orthogonal designs (e.g., Bliemer and Rose 2010; McFadden 1974; Sándor and Wedel 2001; Yu et al. 2009).

D-optimal matrices were created using SAS software (SAS 2014) revealing that efficient designs could be found with either 48 or 96 different profiles. Fractional factorial design was employed, and taking into account 3 possible app profiles for each choice situation, 16 choice sets were generated.

When accessing the survey respondents were first provided with a detailed description of the application, its functionality and its value proposition. Their perceptions of the usefulness of this app were then elicited. For example, respondents were asked to indicate their agreement with the following statement: "*This app appears useful*" on a five-point Likert scale, with 1="absolutely disagree"; 2="disagree", 3="neutral", 4="agree" and 5="absolutely agree". Next, attributes and their levels were presented and explained, as shown in Table 3. In the next step, respondents were offered 16 choice sets (the sequence of presentation was randomized), with three application alternatives per choice. In each choice set, the same application was presented, but levels of attributes varied (see Figure 2). Respondents were asked to choose one application alternative that they would install for each choice set. To make the choice set complete, a "no choice" option was included to cover cases when none of presented applications was acceptable for a respondent. Application presentation was approximated to the reality as close as possible. However, in an attempt to reduce cognitive load for the participants, we decided to avoid presenting two distinct screens – general information screen and FB Login-screen (see Figure 1). Hence, we deviated to some extent from a current design and merged both screens into one as shown in Figure 12. Additionally, several questions about user demographics and prior experience were asked at the end of the survey.

[4] All applications and websites using FB Login ask for basic information per default. Therefore, if FB Login was requested, basic information was always included as well.

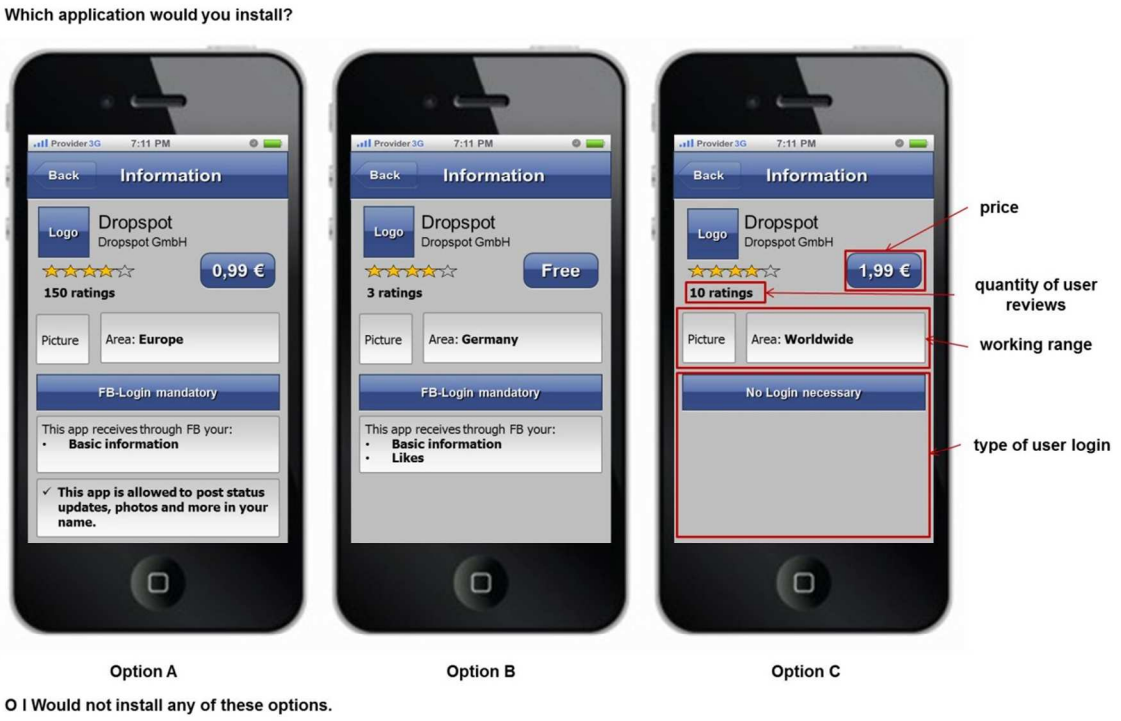

Figure 2. Exemplary Scenario Used in Our Discrete Choice Experiment[5]

Sample

Survey participants were recruited through the mailing list of a large German university in February 2014. As an incentive, 50 Amazon.de gift cards (€ 5 value) were raffled among respondents. A total of 398 respondents, who spend on average 12.65 minutes to complete the survey, participated in our study. Of these, 22 had no Facebook account, had no smartphone and no tablet or always selected the "no choice" option. Hence, their responses were excluded from further analysis. A resulting dataset of 376 responses by far exceeds the threshold of necessary answers 500*6/(3*16) = 62.5 for such a type of studies (Orme 1998). This threshold level can be calculated by the following formula:

$$N \geq 500 \cdot \frac{L^{max}}{J \cdot S}, \qquad (5),$$

where N is the suggested sample size, L^{max} is the largest number of levels for any of the attributes, J is the number of alternatives and S is the number of choice situations in the design.

The sample substantially consists of students (92.2 %). There is a slight predominance of female respondents (59.6 %). Only 6.0 % of respondents are over 31 years old, with the majority (56.0 %) being between 18 and 24 years of age – an important segment of FB users (39.3 % were 25-30 years old). Approximately half of respondents (47.5 %) are obtaining undergraduate degree and one-third (33.2 %) has already completed their bachelor studies. 19.6 % pursued Languages and Culture studies, and 14.5 % studied Economics. Generally, no major was particularly dominant in our dataset. Finally, around 88 % of respondents have spent most of their life in Germany.

Of particular interest is the subsample of 175 users who found the app useful ("likers"), as they "agreed" or "strongly agreed" to the statement "*This app appears useful*". In contrast to "non-likers" (those who were "neutral", "disagreed", or "strongly disagreed" to the statement above), these users are likely to proceed to

[5] Actual pictures were used in the "logo" and "picture" areas.

the permission screen relevant for our experiment, and hence are the main group in the focus of our analysis.

Empirical Results

DCE data was analyzed using mixed logit model (error-component-multinomial-logit) which is appropriate when approximating any random utility model. Being tolerant to the three limitations of standard logit model, mixed logit allows "for random taste variation, unrestricted substitution patterns, and correlation in unobserved factors over time" (Train 2009), thus accounting for the correlation between 16 observations obtained from one respondent. The specification of the utility function of a participant i choosing an app alternative j in a choice set t is as follows:

$$U_{jit} = c_j + \beta_1 Price + \beta_2 Work\ range + \beta_3 Reviews + \beta_4 Type\ of authorisation\ + \mu_i + \varepsilon_{jit} \quad (6),$$

where μ is the error component with the normal distribution with mean zero and standard deviation σ_μ which varied across app alternatives j and users i and accounted for the correlations between observations obtained from the same user. The error component ε followed the Gumbell distribution with mean zero and accounted for differences between users i, alternatives j and choice exercises t. The parameters of the model β1-β4 and the constant c were estimated using SAS software (SAS 2014). Normal mixing distribution for price was assumed. All attributes except price were dummy-coded.

The estimation results are presented in Table 5 for both the overall sample and more importantly for the sample of app "likers". In addition, Goodness-of-Fit Statistics are presented in Table 4. For instance, according to Estrella's measure, which takes values between 0 and 1 and which is often used for discrete choice modeling, the empirical fit of our model is 0.62.

Table 4. Goodness-of-Fit Measures	
Adjusted Estrella	0.6194
AIC	11796
Aldrich-Nelson	0.4506
Cragg-Uhler 1	0.5596
Cragg-Uhler 2	0.5969
Estrella	0.6218
McFadden's LRI	0.2958
Schwarz Criterion	11964
Veall-Zimmermann	0.6131

We observe that the majority of coefficients are significant at 0.01 level for both the overall sample and the sub-sample of "likers". In terms of *perceived benefits*, respondents reacted positively to the widening of the working range of a mobile application, thus exhibiting preference for more functional benefits. With place of living (city) set as a reference level, the opportunity to be serviced in Europe was valued twice as much compared to Germany only. However, the difference was not as large when expanding from a European to a worldwide service. In terms of *number of reviews* – our *proxy for social influence* – we find that the choice of "likers" was only influenced if the number of reviewers was relatively high (150 reviewers). Apparently, lower quantity of reviews was not considered as reliable social information that could facilitate adoption for this group of users. As expected, price was a significant impediment of adoption for both "likers" and users in the overall sample. Finally, when it comes to the importance users attach to *privacy*, we observe that respondents were less likely to install the application using their FB account as compared to direct installation. Requests for BI and additional data, namely email, "likes" or photos, were almost two times less desired when compared to BI only. The request asking for the permission to post on user's behalf on FB was by far the least popular option.

Table 5. Estimation Results of the Experiment							
Attribute	Attribute levels	Users finding app useful: n=175[6]			Overall sample: n=376		
		Estimate	SE	WTP	Estimate	SE	WTP
Working range	Place of living (City)	Reference Level					
	Germany	0.95****	0.24	€ 0.68	0.76****	0.11	€ 0.62
	Europe	1.89****	0.34	€ 1.36	1.52****	0.15	€ 1.24
	Worldwide	2.40****	0.42	€ 1.72	2.01****	0.19	€ 1.64
Quantity of user reviews	4 stars, 3 reviews	Reference Level					
	4 stars, 10 reviews	-0.11	0.22	€ -0.08	0.07	0.12	€ 0.05
	4 stars, 50 reviews	0.25	0.19	€ 0.18	0.40***	0.11	€ 0.33
	4 stars, 150 reviews	0.70**	0.23	€ 0.50	0.84****	0.13	€ 0.68
Type of user login	No FB Login	Reference Level					
	FB Login: BI	-2.50****	0.43	€ -1.79	-2.14****	0.19	€ -1.75
	FB Login: BI and email	-4.77****	0.88	€ -3.42	-4.21****	0.46	€ -3.44
	FB Login: BI and likes	-4.78****	0.83	€ -3.42	-4.06****	0.40	€ -3.31
	FB Login: BI and photos	-5.55****	1.05	€ -3.97	-4.75****	0.51	€ -3.88
	FB Login: BI and "posting" on your behalf	-8.72****	1.63	€ -6.24	-8.42****	1.03	€ -6.88
Price of the App		-1.40****	0.24		-1.22****	0.10	

Note: Significant at **** <0.0001; *** <0.001; **<0.01; *<0.05 level. SE – standard error.

Taking into consideration DCE consistency with utility maximization and demand theory, once parameter estimations are obtained, it is possible to derive willingness to pay (or willingness to accept) for changes in the level of a given attribute. In the case of mixed logit model used in this study, it can be calculated as follows (Potoglou et al. 2013):

$$WTP = -\beta_{price}^{-1} ln\left\{\frac{\sum_j \exp(V_j^1)}{\sum_j \exp(V_j^0)}\right\} \quad (7),$$

where V_j^0 represents the marginal utility of the base level (e.g., No FB Login) and V_j^1 represents the marginal utility of another level of the same attribute (e.g., FB Login: BI). β_{price}^{-1} is the coefficient of the cost of the application and gives the marginal utility of price. In a simple linear relationship, each attribute in the utility expression and price are associated with one coefficient each. In that case, equation (3) can be simplified for any individual to the ratio of two utility parameters and can provide an estimate of WTP (Potoglou et al. 2013):

$$WTP = -1\left(\frac{\beta_{attribute}}{\beta_{price}}\right) \quad (8)$$

The results of the above calculations are presented in Table 5 (columns "WTP" for the sample of "likers" and the overall sample respectively). We find that "likers" valued BI linked to their FB account on average at € 1.79. Avoiding FB Login that asks for BI and email was worth € 3.42; BI and "likes" had the same value of € 3.42; while BI and photos were estimated at € 3.97. The most undesirable option during registration was request for BI in combination with a permission to post on user's behalf: "Likers" were ready to pay around € 6.24 to opt out of this option when given a choice.

Market Simulations

Based on the estimates for the different attribute levels, market shares for a pre-defined set of alternatives can be calculated. Hence, we conducted three series of market simulations in order to gain a deeper

[6] Referred in the paper as „likers".

understanding as to how much users value their private information and how market shares are distributed when privacy-relevant trade-offs are involved. In each simulation, we systematically varied some of the attributes in order to show how these differences affect market shares. In addition, we included a "no choice" option across simulations to account for the share of people who would not install any of the apps involved in the market simulation. Market shares were simulated using mixed logit model, which assumes that probability of choice is a logit function of utility (SAS Institute Inc. 1993). Parameter estimates originally obtained from mixed logit model (Table 5) were used as initial for simulation. Only data from "likers" was included into the analysis.

In a series of simulations 1, we aimed to investigate the effect of FB Login mechanism on market shares. As mentioned earlier, FB Login is a very easy way to obtain user information and, thus, very attractive for providers. However, our results in Table 5 show that compared to "No FB Login" option, users associate a negative utility with it. Therefore, a simple market with two apps – one app with "FB Login: BI" and one without FB Login ("No FB Login") – was simulated. Functionality and a number of reviews were fixed to "worldwide" and "150" respectively for both apps. The price of the "FB Login: BI" app was kept at zero (free) for all simulations. Figure 3 illustrates the market shares of the two apps as a function of price of the "No FB Login" app.

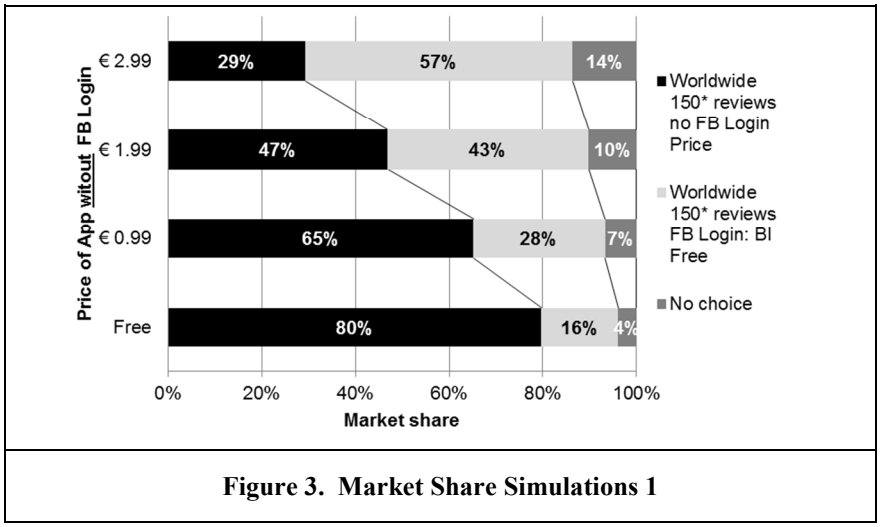

Figure 3. Market Share Simulations 1

Except for the one simulation where both apps were offered for free, our results shed light on user behavior when confronted with "privacy vs. price" trade-off. We observe that as the price for "No FB Login" app increases, its market share decreases. At the same time the share of a "free" privacy-intrusive "FB Login: BI" app rises. This is in line with the research finding that users trade off private information in exchange for money and that consumers decide upon data disclosure based on cost-benefit analysis (Hann et al. 2002; Hann et al. 2007; Hui et al. 2006). Moreover, when the price reaches € 2.99, a "No FB Login" app loses its market leadership. Therefore, if provider's gains from using BI obtained via FB Login are lower than € 1.99 per user, it seems reasonable to refrain from asking for FB Login and offer a paid app instead. Notably, the share of those opting out of the app selection ("no choice" in Figure 3) rises from 4% in the "free / free" scenario to 14 % in the scenario when € 2.99 is charged for "No FB Login" app, suggesting that a certain segment of users is unwilling to choose "FB Login: BI" option under any circumstances. Finally, it is noteworthy that when both apps are offered for free, the model predicts 80 % market share for "No FB Login" app.

In the second series of simulations 2 "functionality vs. privacy" trade-off was explored. As shown in Figure 4, users may be willing to exchange their privacy, by choosing "FB Login: BI" over "No FB Login" app, for other benefits. However, in comparison to the first series of simulations, they are more reluctant to give up private information for functional benefits. This may indicate that monetary cost is a more important reason to give up privacy, than added functional value.

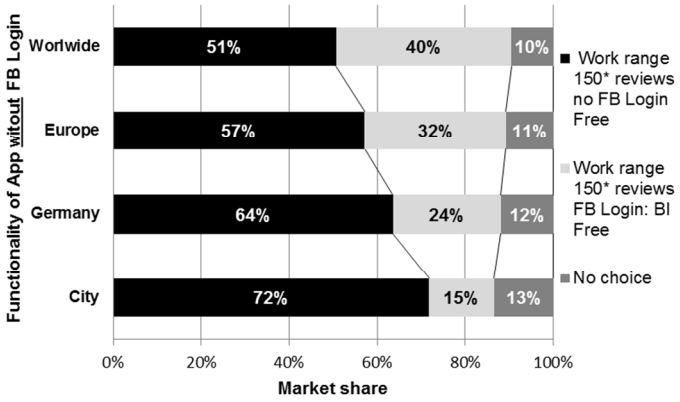

Figure 4. Market Share Simulations 2

In the third simulation 3, we extended the potential product assortment in the market to estimate the market shares of all investigated login types and corresponding information requests for the case when apps are offered for "free". As in the first series of simulations, both functionality and number of reviews were fixed to "worldwide" and "150" respectively and a "no choice" option was included. The resulting distribution of market shares is illustrated in Figure 5. Our analysis reveals the following hierarchy of market shares: "No FB Login" (65.1 %, the most preferable), "FB Login: BI" (13.4 %); "FB Login: BI and "likes" (6.2 %); "FB Login: BI and email" (5.7 %); "FB Login: BI and photos" (5.1 %); "FB Login: BI and "posting" on user's behalf" (1.4 %, least desired). We observe that if given a choice between these six alternatives, the absolute majority (65.1 %) will install an application without FB Login, showcasing a critical impact of the "FB Login" decision for providers.

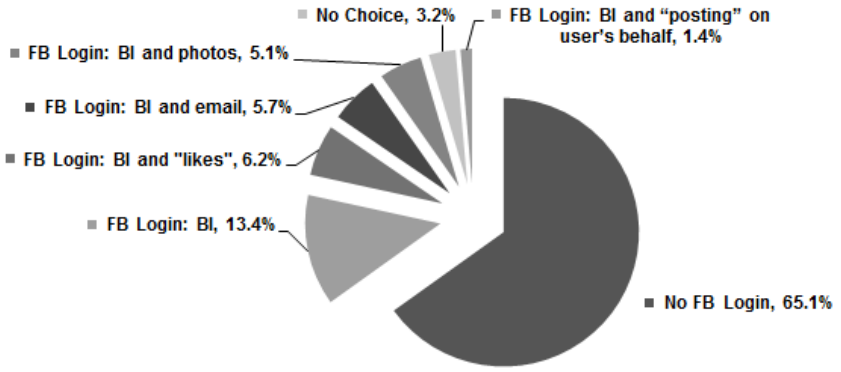

Figure 5. Market Share Simulations 3

Discussion, Implications and Concluding Remarks

On a global level, this study contributes to a better understanding of the value users attach to privacy in a novel context of Social Media. We show that users are willing to change to more privacy-invasive options in exchange for lesser price or extended functionality, with functionality being less valued than money (costs) in these trade-offs. Beyond insights on privacy, we find that a high number of reviews has a significant effect on adoption decisions, supporting the findings of Keith et al. (2010). Specifically, the threshold of 150 reviews seems to signal "review reliability" – an important insight for start-up apps struggling for their market share. Taking a narrower perspective, this study is the first attempt to investigate the role of FB Login and similar single sign-on mechanisms as part of an individual's decision to adopt a mobile app. By accounting for price, perceived benefit, number of reviews (as a proxy for social influence) as well as the presence and intrusiveness of FB Login we were able to model adoption decisions

as well as investigate the role of these key attributes in this process. This analysis has high practical relevance since just on April 30th, 2014 Marc Zuckerberg has voiced concerns over the future of Facebook Login at the F8 Facebook Developers Conference, advocating for a more privacy-friendly solution (Breithut 2014). We find that privacy plays an important role in the app adoption process, with 80 % of users choosing "No FB Login" app over app asking for "FB Login: BI", suggesting that most users are still reluctant to use FB Login. Our approach also enables us to assess users' WTP for different levels of privacy intrusion: We show that in the mobile app context there is indeed a WTP for privacy, which is in line with findings of Hann et al. (2007). For example, just to opt out of "FB Login: BI", users' WTP reaches on average € 1.79. If, in addition to BI, access to email or "likes" is requested, WTP nearly doubles, signaling users' high valuation of their information. Remarkably, WTP for the highest possible working range "worldwide" – our proxy for perceived benefit – is lower than WTP to avoid "FB Login: BI", hinting at the importance of the decision over the inclusion of this login mechanism. Our analysis reveals that while FB Login allows for the identification of customers and easier targeting, it may be more profitable for app developers to charge for an app instead. Indeed, running a market simulation, we could show that even when an app charged € 1.99 and did not use any login mechanism there would be more users installing this app than an app offered for free but requesting a "FB Login: BI".

Regarding the valuation of different information items/actions, results of our study generally correspond to the findings by Krasnova et al. (2013): Photos emerge as a highly sensitive item while "likes" and email are seen as less sensitive. Importantly, request to post in one's name emerges as by far the most sensitive permission. Users appear to be more disturbed by the loss of control over their identity construction, than by third parties accessing their private details, even such sensitive ones as photos (Krasnova et al. 2013). In fact, we find that users' WTP to opt out of this request amounts to a whopping € 6.24, supporting qualitative findings by Eling et al. (2013). Further, the effect of the intrusiveness of a permission request has been also demonstrated in a market simulation. We find that an app with "No FB Login" would clearly dominate the market, holding a market share of 65.1 %, while the shares of all the other apps would vary around 5 %, with an app asking to post on user's behalf merely taking up a market share of 1.4 %.

Despite the value of our findings, this study has several limitations, which, however, offer exciting venues for future research. First, our study has focused only on one mobile application, which imposes constraints on the transferability of our findings to other contexts. For other apps with different perceived benefits or prices in a different range, the results might vary. Therefore, in future research, other apps should be considered as well. We have also chosen not to vary star ratings to streamline model specification and experimental design. Next, a simplification of permission presentation has been done to fit all data into one dialog (see Figure 2). In this regard, users were also not given an option to opt out from a permission to post on user's behalf – a current practice adopted by FB (Cohen 2013a). Especially in the context of social media, social influence can play an important role. While we varied the number of reviews, there is a wide array of other forms of social influence, as the opinions of friends or users' willingness to interact with them through mobile apps as well, which should be considered in future studies. Furthermore, it would be interesting to additionally include convenience-privacy tradeoff in the here presented research design. Finally, our respondents were mainly German students. While reliance on student samples is acceptable considering "universalistic" nature of our research constructs (Kruglanski 1975), future research may investigate these issues with a more representative sample of users, including inter-cultural comparisons. In addition, as students usually represent a low-level income group, further research could be improved by controlling for income level, general privacy concern and other personal traits. All in all, our study offers exciting insights on the privacy behavior and preferences in the novel context of Social Media and mobile web.

References

Accent, and RAND Europe. 2010. "Review of Stated Preference and Willingness to Pay Methods," Retrieved 2014-05-02, from http://webarchive.nationalarchives.gov.uk/+/http://www.competition-commission.org.uk/our_role/analysis/summary_and_report_combined.pdf.

Bakken, D., and Frazier, C. L. 2006. "Conjoint Analysis: Understanding Consumer Decision Making," in *The Handbook of Marketing Research,* R. Grover and M. Vriens (eds.). Thousand Oaks, CA: Sage.

Bauer, C., Korunovska, J., and Spiekermann, S. 2012. "On the Value of Information - What Facebook Users Are Willing to Pay," in *Proceedings of the 20th European Conference on Information Systems*, Barcelona, Spain.

Becker, G. M., Degroot, M. H., and Marschak, J. 1964. "Measuring Utility by a Single-Response Sequential Method," *Behavioral Science* (9:3), pp. 226-232.

Beresford, A. R., Kübler, D., and Preibusch, S. 2012. "Unwillingness to Pay for Privacy: A Field Experiment," *Economics Letters* (117:1), pp. 25-27.

Bliemer, M. C. J., and Rose, J. M. 2010. "Construction of Experimental Designs for Mixed Logit Models Allowing for Correlation across Choice Observations," *Transportation Research* (44:6), pp. 720-734.

Breithut, J. 2014. "Anonyme Anmeldung Bei Apps: Zuckerberg Verspricht Facebook-Nutzern Mehr Kontrolle." Retrieved 2014-05-02, from http://www.spiegel.de/netzwelt/web/facebook-nutzer-sollen-mehr-kontrolle-bei-apps-erhalten-a-967093.html.

Cascetta, E. 2009. "Random Utility Theory," in *Transportation Systems Analysis - Models and Applications*. Springer, pp. 89-167.

Cohen, D. 2013a. "Login with Facebook Update: Apps Must Now Separately Request Permission to Post on Behalf of Users." Retrieved 2014-04-25, from http://www.insidefacebook.com/2013/08/22/login-with-facebook-update-apps-must-now-separately-request-permission-to-post-on-behalf-of-users/.

Cohen, D. 2013b. "Study: Login with Facebook Implementation Double for European Retailers Vs. U.S.", from http://allfacebook.com/betapond-europe-retailers-login-with-facebook_b116788.

Cvrcek, D., Kumpost, M., Matyas, V., and Danezis, G. 2006. "A Study on the Value of Location Privacy," in *Proceedings of the 5th ACM workshop on Privacy in electronic society*, Alexandria, VA, USA, pp. 109-118.

Danezis, G., Lewis, S., and Anderson, R. 2005. "How Much Is Location Privacy Worth?," in *Proceedings of the 4th Workshop on the Economics of Information Security*, Cambridge, MA, USA.

Darwell, B. 2012. "Facebook Mobile Plattform Gains Ground with 200k Apps Now Connected." Retrieved 2014-04-24, from http://www.insidefacebook.com/2012/12/05/facebook-mobile-platform-gains-ground-with-200k-apps-now-connected/.

Egelman, S. 2013. "My Profile Is My Password, Verify Me!: The Privacy/Convenience Tradeoff of Facebook Connect," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Paris, France: pp. 2369-2378.

Eling, N., Krasnova, H., Widjaja, T., and Buxmann, P. 2013. "Will You Accept an App? Empirical Investigation of the Decisional Calculus Behind the Adoption of Applications on Facebook," in *Proceedings of the 34th International Conference on Information Systems*, Milan, Italy.

Facebook Developers. 2012. "Authentication." Retrieved 2014-04-25, from http://www.facebook-developers.jp/core_concepts/authentication.html.

Fang, X., Chan, S., Brzezinski, J., and Xu, S. 2005. "Moderating Effects of Task Type on Wireless Technology Acceptance," *Journal of Management Information Systems* (22:3), pp. 123-157.

Fu, B., Lin, J., Li, L., Faloutsos, C., Hong, J., and Sadeh, N. 2013. "Why People Hate Your App: Making Sense of User Feedback in a Mobile App Store," in *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, Chicago, IL, USA, pp. 1276-1284.

Gartner. 2013. "Gartner Says Mobile App Stores Will See Annual Downloads Reach 102 Billion in 2013." Retrieved 2014-05-02, from http://www.gartner.com/newsroom/id/2592315.

Grossklags, J., and Acquisti, A. 2007. "When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information," in *Proceedings of the 6th Workshop on the Economics of Information Security*.

Hann, I.-H., Hui, K.-L., Lee, T., and Png, I. 2002. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off," in *Proceedings of the 23rd International Conference on Information Systems*, Barcelona, Spain, pp. 1-10.

Hann, I.-H., Hui, K.-L., Lee, T., and Png, I. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13-42.

Harper, J., and Singleton, S. 2001. "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," Retrieved 2014-04-30, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=299930.

Huberman, B. A., Adar, E., and Fine, L. R. 2005. "Valuating Privacy," *Security & Privacy, IEEE* (3:5), pp. 22-25.

Hui, K. L., Tan, B. C. Y., and Goh, C. Y. 2006. "Online Information Disclosure: Motivators and Measurements," *ACM Transactions on Internet Technology* (6:4), pp. 415-441.

Jentzsch, N., Preibusch, S., and Harasser, A. 2012. "Study on Monetising Privacy. An Economic Model for Pricing Personal Information," Retrieved 2014-05-02, from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy.

Keith, M. J., Babb, J. S., Furner, C. P., and Abdullat, A. 2010. "Privacy Assurance and Network Effects in the Adoption of Location-Based Services: An Iphone Experiment," in *Proceedings of the 31st International Conference on Information Systems*, Saint Louis, MO, USA.

Kim, G. S., Park, S.-B., and Oh, J. 2008. "An Examination of Factors Influencing Consumer Adoption of Short Message Service (Sms)," *Psychology & Marketing* (25:8), pp. 769-786.

Kim, K. K., Shin, H. K., and Kim, B. 2011. "The Role of Psychological Traits and Social Factors in Using New Mobile Communication Services," *Electronic Commerce Research & Applications* (10:4), pp. 408-417.

King, J., Lampinen, A., and Smolen, A. 2011. "Privacy: Is There an App for That?," in *Proceedings of the 7th Symposium On Usable Privacy and Security*, Pittsburgh, PA, USA.

Kosinski, M., Stillwell, D., and Graepel, T. 2013. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior " in *Proceedings of the National Academy of Sciences of the United States of America*.

Krasnova, H., Eling, N., Schneider, O., Wenninger, H., Widjaja, T., and Buxmann, P. 2013. "Does This App Ask for Too Much Data? The Role of Privacy Perceptions in User Behavior Towards Facebook Applications and Permission Dialogs.," in *Proceedings of the 21st European Conference on Information Systems*, Utrecht, Netherlands.

Krasnova, H., Hildebrand, T., and Guenther, O. 2009. "Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis," in *Proceedings of the 30th International Conference on Information Systems*, Phoenix, AZ, USA.

Krasnova, H., and Kift, P. 2012. "Online Privacy Concerns and Legal Assurance: A User Perspective," in *AIS SIGSEC WISP Workshop on Information Security and Privacy*, Orlando, FL, USA.

Kruglanski, A. W. 1975. "The Human Subject in the Psychology Experiment: Fact and Artifact," *Advances in Experimental Social Psychology* (8), pp. 101-147.

Lambin, J.-J. 2007. "Market-Driven Management: Supplementary Web Resource Material," Retrieved 2014-04-30, from http://www.palgrave.com/business/lambin/students/pdfs/Note%207.pdf.

Lardinois, F. 2010. "Iphone Users Are More Than Willing to Pay for Apps - but Don't Want to Pay a Lot." Retrieved 2014-04-25, from http://readwrite.com/2010/03/31/iphone_users_more_willing_to_pay_for_apps_-_but_do#awesm=~oCqOvdJazqYFUs.

Louviere, L., Flynn, T., and Carson, R. 2010. "Discrete Choice Experiments Are Not Conjoint Analysis," *Journal of Choice Modelling* (3:3), pp. 57-72.

Lu, J., Yao, J. E., and Yu, C.-S. 2005. "Personal Innovativeness, Social Influences and Adoption of Wireless Internet Services Via Mobile Technology," *Journal of Strategic Information Systems* (14:3), pp. 245-268.

Malhotra, A., and Malhotra, C. K. 2009. "A Relevancy-Based Services View for Driving Adoption of Wireless Web Services in the U.S," *Communications of the ACM* (52:7), pp. 130-134.

McFadden, D. 1974. "Conditional Logit Analysis of Qualitative Choice Behavior," in *Frontiers in Econometrics,* P. Zerembka (ed.). New York: Academic Press, pp. 105-142.

Nikou, S., and Mezei, J. 2013. "Evaluation of Mobile Services and Substantial Adoption Factors with Analytic Hierarchy Process (Ahp)," *Telecommunications Policy* (37:10), pp. 915-929.

Nysveen, H., Pedersen, P. E., and Thorbjørnsen, H. 2005. "Intentions to Use Mobile Services: Antecedents and Cross-Service Comparisons," *Journal of the Academy of Marketing Science* (33:3), pp. 330-346.

Orme, B. 1998. "Sample Size Issues for Conjoint Analysis Studies," in *Sawtooth Software Technical Paper*.

Osofsky, J. 2012. "Facebook at Leweb 2012." Retrieved 2014-04-30, from https://developers.facebook.com/blog/post/2012/12/05/facebook-at-leweb-2012/.

Pagani, M. 2004. "Determinants of Adoption of Third Generation Mobile Multimedia Services," *Journal of Interactive Marketing* (18:3), pp. 46-59.

Petrova, K., and Wang, B. 2011. "Location-Based Services Deployment and Demand: A Roadmap Model," *Electronic Commerce Research* (11:1), pp. 5-29.

Potoglou, D., Patil, S., Gijón, C., Palacios, J. F., and Feijóo, C. 2013. "The Value of Personal Information Online: Results from Three Stated Preference Discrete Choice Experiments in the Uk," in *Proceedings of the 21st European Conference on Information Systems*, Utrecht, Netherlands.

Pring, C. 2012. "100 Social Media Statistics for 2012." Retrieved 07.12.2012, from http://thesocialskinny.com/100-social-media-statistics-for-2012/

Racherla, P., Babb, J. S., and Keith, M. J. 2011. "Pay-What-You-Want Pricing for Mobile Applications: The Effect of Privacy Assurances and Social Information," in *Conference for Information Systems Applied Research Proceedings*, Wilmington, NC, USA, pp. 1-13.

Rose, J., and Bliemer, C. 2008. "Stated Preference Experimental Design Strategies," in *Handbook of Transport Modelling,* D.A. Hensher and K.J. Button (eds.). Oxford: Elsevier, pp. 151-180.

Rose, J., and Bliemer, C. 2013. "Sample Size Requirements for Stated Choice Experiments," *Transportation* (40), pp. 1021-1041.

Russell-Bennett, R., and Neale, L. 2009. "Social Networking: Investigating the Features of Facebook Application," in *Proceedings of the Academy of Marketing Annual Conference*, Leeds.

Sándor, Z., and Wedel, M. 2001. "Designing Conjoint Choice Experiments Using Managers' Prior Beliefs," *Journal of Marketing Research* (38), pp. 430-444.

SAS. 2014. "Sas on Demand for Academics." Retrieved 2014-04-29, from http://support.sas.com/ondemand/SAS93M2.html

SAS Institute Inc. 1993. "Sas Technical Report R-L 09, Conjoint Analysis Examples," SAS Institutie Inc., Cary, NC, USA, Retrieved 2014-05-02, from http://support.sas.com/documentation/onlinedoc/v82/techreport_r109.pdf.

Spiekermann, S., Korunovska, J., and Bauer, C. 2012. "Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy," in *Proceedings of the 33rd International Conference on Information Systems* Orlando, FL, USA.

Street, D., and Burgess, L. 2007. *The Construction of Optimal Stated Choice Experiments: Theory and Methods*. Hobogen, NJ: Wiley-Interscience.

Taylor, D. G., Voelker, T. A., and Pentina, I. 2011. "Mobile Application Adoption by Young Adults: A Social Network Perspective," *International Journal of Mobile Marketing* (6:2), pp. 60-70.

Train, K. E. 2009. "Mixed Logit," in *Discrete Choice Methods with Simulation*. New York: Cambridge University Press.

Vasa, R., Hoon, L., Mouzakis, K., and Noguchi, A. 2012. "A Preliminary Analysis of Mobile App User Reviews," in *Proceedings of the 24th Australian Computer-Human Interaction Conference*, Melbourne, Australia, pp. 241-244.

Wang, N. 2012. "'Third-Party Applications' Data Practices on Facebook," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA.

Wang, N., Shen, X.-L., and Sun, Y. 2013a. "Transition of Electronic Word-of-Mouth Services from Web to Mobile Context: A Trust Transfer Perspective," *Decision Support Systems* (54:3), pp. 1394-1403.

Wang, T., Oh, L.-B., Wang, K., and Yuan, Y. 2013b. "User Adoption and Purchasing Intention after Free Trial: An Empirical Study of Mobile Newspapers," *Information Systems and e-Business Management* (11:2), pp. 189-210.

White, V. 2013. "The Landscape of Social Login & Sharing: Consumers Want Choice." Retrieved 2014-04-24, from https://blog.gigya.com/the-landscape-of-social-login-sharing-consumers-want-choice/.

Wu, J.-H., and Wang, S.-C. 2005. "What Drives Mobile Commerce? An Empirical Evaluation of the Revised Technology Acceptance Model," *Information & Management* (42:5), pp. 719-729.

Xu, H., Teo, H.-H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk," in *Proceedings of the 26th International Conference on Information Systems*, Las Vegas, NY, USA.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-173.

Yu, J., Goos, P. P., and Vandebroek, M. 2009. "Efficient Conjoint Choice Designs in the Presence of Respondent Heterogeneity," *Marketing Science* (28), pp. 122-135.