Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications

Zhan Liu
Faculty of Business and Economics (HEC)
University of Lausanne, Switzerland
zhan.liu@unil.ch

Jialu Shan
Green Business Model Innovation Association
Switzerland
jialu.shan@gmail.com

Riccardo Bonazzi
Institute of Entrepreneurship Management (IEM)
University of Applied Sciences and Arts Western Switzerland
riccardo.bonazzi@hevs.ch

Yves Pigneur
Faculty of Business and Economics (HEC)
University of Lausanne, Switzerland
yves.pigneur@unil.ch

Abstract

Evidences collected from smartphones users show a growing desire of personalization offered by services for mobile devices. However, the need to accurately identify users' contexts has important implications for user's privacy and it increases the amount of trust, which users are requested to have in the service providers. In this paper, we introduce a model that describes the role of personalization and control in users' assessment of cost and benefits associated to the disclosure of private information. We present an instantiation of such model, a context-aware application for smartphones based on the Android operating system, in which users' private information are protected. Focus group interviews were conducted to examine users' privacy concerns before and after having used our application. Obtained results confirm the utility of our artifact and provide support to our theoretical model, which extends previous literature on privacy calculus and user's acceptance of context-aware technology.

1. Introduction

Personalization through contextual data is one of the salient characteristics of today's technology-based world. Personalization is generally defined as "*the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information*" [6]. The market of location-based services (LBS), which offer service personalization according to user's position, is enjoying strong growth along with the wider coverage of smartphone and the higher speeds of data transfer rate across mobile networks. According to Pyramid Research, LBS market revenue is expected to reach $10.3 billion in 2015, up from $2.8 billion in 2010. In addition to bringing positive returns to companies, which adopt the practice of personalization, LBS allows the creation of tremendous benefits for consumers such as the increase of convenience, task efficiency, individualization, and galvanizing intended purchases - it seems that a win-win situation is married.

Nonetheless, personalization also triggers consumers' privacy concerns [8]. In the competitive global marketplace, privacy has emerged as an important issue, due to the fundamental tension between company and consumer interests, since personalization is partly dependent on consumers' willingness to share their personal information (e.g., [1]). On one hand, companies need to collect users' personal information to provide more customized products to consumers. On the other hand, consumers of personalized products or services consider personal data collection as an invasion of their privacy and they often give as little information as possible to the service provider [35].

Accordingly, a significant body of research in privacy and information system has suggested that information privacy and consumer concern thereof is one of the most important issues in today's information-intensive environment [38,40]. Service user and service provider's conflicting goals create a "personalization-privacy paradox", where consumers share their private information with subjective expectation of personalized services, while assuming that the service provider will not indiscriminately use their personal information to increase its revenues [1,42]. Consumers' controls on who can access their information and on how their information is exploited become a crucial element, which alleviates their privacy concerns.

Consequently, consumers are expected to make decisions based on "privacy calculus" [8,14] , a cost-benefit analysis in assessing the outcomes of private information disclosure. The calculus perspective suggests that consumers tend to trade privacy when they can maximize the expected benefit that they can gain from disclosing personal information, while minimizing the expected harm that may come from disclosing it.

This study is addressed to researchers and practitioners concerned with design of context-aware applications, and it aims at providing a set of guidelines to improve location-based service design, based on a better understanding of privacy issues in the mobile business sector. Existing studies overlook the consumer's privacy calculus by assuming that consumer personal information is exogenously given to companies by incurring some costs (e.g., loss of privacy) simultaneously. This is not always the case in reality. In addition, while scholars have studied the interaction between personalization and privacy concern, or privacy concerns and control, little attention has been paid to the influence of personalization and control at the same time, especially in the context of mobile applications. Therefore our question is: **what role does personalization and control play in the design of a context-aware mobile application to protect users' personal information?** In this article we followed the seven guidelines for design research [16] and, according to guideline 1, this paper introduced a new artifact in the form of software application, called "Privacy Manager". In a previous study, we have tested the performance of the algorithm of "Privacy Manager" using longitudinal data from 200 users across one year. Nonetheless, in such study we did not perform any usability test. Therefore, by following guideline 2, we stated that Privacy Manager would protect users' mobile phones and their private information by limiting the access to their mobile phones by using their as locations and time to authenticate them. Section 2 illustrated how this application addresses a gap in the literature.

Section 3 illustrated our chosen methodology and addresses guidelines 3, 4 and 5 of [16]. According to guideline 3, we have tested the usability of this application by performing focus group interviews among ten test users. We then stated that our main research contribution was the context-aware mobile application called "Privacy Manager" based on the notion that context awareness could help to achieve proper trade-offs between adaptive authentication and utility (guideline 4). Our study results has also confirmed and extended the three kernel theories that we have used, namely: (a) the four key factors of an individual's privacy concerns [36], (b) the notion of privacy calculus model [14] and (c) the users' technology acceptance model [11]. Later, we have applied rigorous methods to collect users' requirement, we have used existing frameworks to develop our software and we have applied data triangulation while performing analysis of data collected in the focus groups (guideline 5).

According to guideline 6, we stated that we have performed two main iterations, which were associated to two main clusters of users interviewed. The results of such iterations were presented in section 4.

Finally, we have followed guideline 7 and decided to present our results to an audience that was interested in technology details as well as management implications of our study, presented in section 5.

2. Theoretical background and related work

In this section we derive a set of gaps in the literature by: (1) introducing the notions of privacy concerns, personalization and controls, (2) assessing the existing literature on privacy management mobile applications (3) underlying the gap, which we aim to address.

2.1. Privacy concerns, personalization and control

Privacy concerns is receiving increased attention due to the huge amount of personal information being collected, stored, transmitted and published on the internet [17]. Smith et al. [36] identified four dimensions of an individual's concern about privacy, namely: (1) collection, (2) errors, (3) unauthorized secondary use and (4) improper access. The four factors provide a framework to explain the concerns for information privacy [38]. That is, the likelihood of privacy breaches is expected to occur, when any of the following cases happens: (1) large amounts of personally identifiable data are being collected, (2) data are inaccurate, (3) companies use personal information for undisclosed purposes, and (4) companies fail to protect consumers' personal information. Consumer privacy concerns vary dramatically by information type. For instance, Both Phelps et al. [30] and Ward et al. [41] found that consumers are more sensitive about their financial and personal identifier information than other demographic information. In other words, consumers are likely to avoid revealing personal information that may identify themselves to companies in exchanges for values or services that companies would provide. It is noteworthy that privacy concern may differ from

person to person. Junglas et al. [19] examined consumers' personality traits and concerns for privacy, showing that agreeableness has a negative effect on concerns for privacy, whereas conscientiousness and openness positively affect privacy concerns. Even in situations in which perceived usefulness is the same, people may exhibit different levels of privacy concern in different types of services. For instance, a study conducted by Barkhuus and Dey [2] found that location-tracking services generated more concerns for privacy than position-aware services, despite the fact that these two types of location-based services use similar technology.

Privacy concerns and personalization. According to some authors, privacy concerns are not absolute concepts [35]. Rather, they are users' subjective perceptions about their rights to control the collection and use of their personal information. Individuals make choices based on tradeoffs in which they give up a certain degree of privacy in exchange for benefits that are valuable for them. This is consistent with expectancy theory in marketing [29] where users will behave in ways that maximize positive outcomes and minimize negative outcomes [14]. Therefore, consumers may be willing to disclose and share their personal information for the benefit of personalization if the perceived overall value is balanced by, if not outweighed by, the loss of information privacy. On the one hand, Chellappa and Sin [6] confirmed this claim by finding that consumers are concerned about their personally identifiable information and about their anonymous and personally unidentifiable information. On the other hand, Culnan and Bies [9] argued that individuals are more likely to accept the loss of privacy as long as benefits exceed the perceived risks of information disclosure. A more recent study conduct by Liu et al. [24] found that personalized services played a significant moderating effect on the relationship between users' disclosed information and their perceived benefits. Moreover, privacy concerns may vary by the purpose or the context of use, and thus are situation dependent. For example, Sheng et al. [35] found that consumers are more concerned about the potential loss of privacy in utilizing personalized services in a non-emergency than in an emergency context. In addition, cultures may serve as a moderator in information privacy concerns. Dinev et al. [12] revealed a cross-cultural difference existed in the privacy calculus model in e-commerce between Italy and the United States, indicating that culture values played a significant moderating effect on consumers' privacy concerns. In addition, empirical results have provided evidence that consumers usually are willing to share their information with another party when they trust it. For example, Chellappa and Sin [6] found that consumer intention to use personalization services is positively influenced by consumer trust in the services provider.

Privacy concerns and control. Privacy concerns may come from lack of adequate control over the disclosure of personal information. Users take high risks when they submit their personal information to companies [26]. They feel more threatened if technology has the capability to access, collect and use their personal information without users' content. For this reason, their privacy concerns would arise from the feeling that their personal information is vulnerable and they are not able to control it [13]. Hence, loss of control over information is a kind of invasion of privacy. Many privacy surveys indicate that Internet users find it important to know how their personal information is being used and to have control over this usage [22]. A number of studies have examined the effect of such privacy controls. For example, Culnan and Armstrong [8] argued that consumers perceived information disclosure as less privacy-invasive when they believed that they were able to control future use of the information and that the information would be used to draw accurate inferences about them. Xu and Teo [43] proved that the assurance of consumers' perceived control over their personal information had a considerable influence on alleviating their privacy concerns. Based on two field surveys and data from 742 household respondents, Malhotra et al. [26] demonstrated that control over personal information served as one of the most important factors in Internet users' information privacy concerns. Hui et al. [18] found that the existence of a privacy statement, which makes a more accurate assessment of the risks of disclosing personal information to websites, induced more consumers to disclose their personal information. Benisch et al. [3] also found that diversified rules of controls over the conditions under which users' information is shared may increase the efficiency without violating users' personal privacy preferences.

2.2. Privacy Management Mobile Applications

A number of research efforts have been conducted in the area of privacy in context-awareness mobile systems. Most existing approaches for designing privacy related mobile systems mainly consist of: (1) the context (CA) perspective; (2) the user preference (UP) perspective and (3) the authorization and access control (AC) perspective. Table 1 illustrates examples for each perspective. The context approach promotes services adaptable to context changes [25]. The second approach proactively tailors products or services with users, and adapt according to the user's personal preferences [33]. The authorization and access control

approach promotes policies that constrain what a user can do directly and what programs executing on behalf of the users are allowed to do [34].

2.3. Gaps in the existing literature

Despite a considerable amount of studies exist on personalization and privacy, or control and privacy, little attention has been paid at the overlapping between personalization, control and privacy concerns. We try to fill this research gap.

Table 1. Mobile applications for privacy management

Privacy management mobile applications	CA	AC	UP
[27], [15]	X		
[28]		X	
[20]			X
[10]		X	X
[4], [39]	X	X	
[7], [32]	X		X
Our application Privacy Manager	X	X	X

3. Methodology

The empirical part of this study is qualitative. This section focuses on: (1) a quick glance at the design, realization and implementation of our application to address the gap in the literature; (2) how participants used our application, in order to allow us to assess their privacy concerns; (3) the description of the participants to the study; (4) the procedure used for data analysis.

3.1. The objectives of our application

The main objective of our application is to induce an user's movement pattern, in terms of time and location. Such user's movement pattern is to be used as an unique identifier for a single sign-on application, which should be easy to use and adaptive, since user's location and user's movement pattern change over time. Accordingly, time and location data should be safely stored within the application to protect user's privacy.

3.2. The development of our application

Before developing our application we conducted a set of individual interviews to help us develop the probe questions to conduct the focus group sessions. Each of the individual interviews lasted for approximately one hour. Building on the results obtained by our individual interviews, as well as cluster 1 (we will explain in section 3.3), we designed and developed a mobile application called "Privacy Manager". This application is based on Android 2.1 to 4.1 mobile phone platforms, and it is developed using the Android Software Development Kit (SDK), which is a comprehensive set of development tools and user interface frameworks. Our application implements two sensors that are commonly used for location-based services: location and time. There are four main functions in the application: (1) user's preferences configuration, (2) training, (3) tracking, and (4) import and export. The *user's preferences configuration* uses SQLite database to store user's preferences, and those preferences include notification modes (email, vibration, and alarm), frequencies of tracking data and analysis (between one minute and one hour) and precision of localization (between one hundred meters and ten kilometers). The *training function* uses SQLite database to store a set of clusters defined by the user (e.g. home and work place), and to assign them to user's positions in terms of location and time. The *tracking function* collects user's position at a certain time and assesses if there is any user's activated profile that includes (a) the current time and (b) the current location. At this stage, one or more profiles can be activated with user's circumstance in order to identify the mobile phone user. If there is no match, the tracking function would send a notification to the user. The *import and export function* is used to export (after having submitted the correct password) all the tables of SQLite database in an XML file, and it allows to import the XML file in another phone to copy user's preferences configuration, training, and tracking data.

3.3. Use case of our application

Study participants were asked to install the application, and to use it for at least one week. The use case can be split into three stages of different duration: (1) configuration (5 minutes); (2) training (1 day); (3) tracking (6 days).

During the configuration phase, after user's login, users can manually introduce their configuration settings or they can import them by using the import and export function.

During the training phase, the user creates a cluster every time that arrives in a new place, and the application automatically collects location data to learn user's movement patterns and to induce users' habits in their lives.

During the tracking phase, the user is not supposed to do anything. If the current location does not match any movement pattern, the application sends one or more notifications and blocks the phone.

3.4. Demography of participants in our study

We recruited twenty participants, offering a small gift for completion of the study. To assess the effect of our application, we used ten participants as control group, who were asked to express their opinion on privacy concerns without using our application (we will refer to them as cluster 1), whereas ten participants expressed their viewpoints on privacy concerns before and after using it (we will refer to them as cluster 2).

Across both groups, ages ranged between 21 and 41, with 12 men and 8 women from different backgrounds (computer science, marketing, educators and housewives, etc.). The number of years the twenty participants had used a Smartphone varied from 0 to 8 with an average of 4.2 years. Most participants were using smartphones for various purposes, from business to leisure, from social networking to self-entertainment. Most participants have used at least one location-based mobile application (e.g., Google map, weather, etc.).

3.5. Focus group data collection and analysis

We conducted six focus group interviews - group size ranging from 2 to 5 people - to ask about user experiences relating to ease of use and privacy issues. For the sake of clarity, we recall that focus groups are a form of group interview where the focus of investigation is on participant communication within the group rather than on alternating questions and responses between the researcher and respondents. Focus groups are widely used and they have been proven an effective research technique for investigating individual's perceptions and attitudes, and exploring the reasons behind these [21,31].

Our focus groups revolved around the same set of questions to explore users' reactions to the concept of protecting privacy by identifying the threats which users are concerned and which pleased users are cared about, and to elicit requirements for a mobile application based on this concept. We aimed at incorporating users' feedback at the early stage of the development process in order to address usability issues and design for positive experience.

Each focus group session began by thanking the participants for being available for the interview. Then the researcher explained the purpose of the study and informed participants that there were no right or wrong answers. All participants were encouraged to express their opinions and ideas freely and openly. We did not prompt participants about any specific context in which they have privacy concerns, but rather asked open questions such as "*Do you feel safe when giving our personal information to a mobile application? Please explain your selection*".

Each focus groups session took place in a relaxing and neutral meeting place. The interviews lasted on average 60 minutes and were camera recorded and transcribed by two researchers to perform data triangulation.

We adopted the "*framework analysis*" to guide our analysis process. Originally used in policy issues, framework analysis is a qualitative method that is aptly suited for research with specific questions, a limited time frame, and a priori issues [37]. It allows the inclusion of a priori as well as emergent concepts and it matched our situation. On the one hand, there were three existing theoretical foundations, namely Smith et al.'s [36] four dimensions of individual's privacy concerns, privacy calculus [14] and Davis's [11] technology acceptance model (which will be explained in details in the following section). On the other hand, we intended to let new perceptions and requirements emerge. A framework analysis method is organized into five key steps [23,37].

1. *Familiarization*: reading of data collected during user interviews. In this step, two researchers listened to the audio recordings and did the transcripts to gain an overview of the data collected.

2. *Identifying a thematic framework*: identifying a set of variables that are developed both from a priori issues and from emerging issues from the first cluster. Two researchers reviewed all transcripts carefully and create categories separately. They then have a face-to-face meeting to compare and combine these categories. Some comments were placed in more than one category while some were lack of sufficient significance so we exclude them.

3. *Indexing:* more commonly regarded as coding in other qualitative analysis approaches, is the process of using codes to identify specific pieces of data. Combining the existing theoretical foundations, the same two researchers worked in parallel to rearrange the categories identified from the second step.

4. *Charting*: using headings and subheadings that are drawn from previous stages into charts that can easily be read across the whole dataset.

5. *Mapping and interpretation*: the final stage involves the search for patterns, associations, concepts, and explanations. We will discuss it in the next session.

4. Findings and Discussion

In this section, we present the qualitative analysis of the focus group discussions. We refer to participants using the following code: C=Cluster, G=Group, P=Participant. The analysis presented in table 2, illustrates how we extend previous literature and it can be divided into three categories: (1) privacy concerns; (2) privacy calculus; and (3) evaluation of utility.

Table 2. New concepts for context-aware application

Categories	Existing Concepts	New concepts
(1) Smith et al.'s [36] factors of individual's privacy concerns	(1.1) Collection (1.2) Errors (1.3) Unauthorized secondary use (1.4) Improper access	(1.5) Legal consideration (1.6) Reputation consideration (1.7) Agreement on information releasing
(2) Dinev and Hart's [14] extended privacy calculus model	(2.1) Risk beliefs (2.2) Confidence and enticement beliefs (2.3) Benefit beliefs (2.4) Willingness to act	(2.5) Control over disclosed information (2.6) Personalization
(3) Davis's [11] model of technology acceptance	(3.1) Perceived ease of use (3.2) Perceived usefulness	(3.3) User's mobility (3.4) User's risk attitude

Existing concepts are derived from the original articles, whereas new concepts are induced from the results, which we obtained. In the table, some concepts overlap across two categories that is "risk beliefs" and "user's risk attitude", leading us to believe that causal or cross-loadings effects among concepts might exist.

4.1. Privacy concerns

The first line of table 2 summarizes the dimensions related to mobile users' privacy concerns. We found some support for Smith et al.'s [36] four factors of individual privacy concerns in the context of mobile users.

Concerns about collection (1.1) were the most frequently mentioned concerns when people use their smartphones. These concerns are about extensive amounts of personally identifiable data that are collected and stored in databases [36]. A common opinion among all participants was that in general they do not like to share things with applications, especially for very private information like name, home address, and so forth. Moreover, users treated mandatory and non-mandatory information differently. As C1G2P2 explained: "*I will not provide the application with any information as long as it is non-mandatory.*"

Concerns about *inaccurate data (1.2)* were mentioned only once: "*It's quite annoying that our office phone number is displayed on a website as a restaurant phone number so I can always get calls for table reservations at the office*" (C2G1P4). Nevertheless, this can possibly lead to serious consequences if it actually takes place. Therefore we include it in our analysis.

Concerns about unauthorized secondary use (1.3) - defined as concerns that information is collected for one purpose but is used for another, within or outside of the organization [36] - were also mentioned frequently. Participants differentiated such misrepresentation concerns between the application provider and third parties. Respondents fear that data from the application provider are misused: "*Once you download one application, you cannot delete it completely. Even if you delete it, sometimes something is still remaining on your phone.*" (C2G2P1). "*Facebook and Gmail get free customers, but they make money from ads. Actually, ads are tailored based on your activity*" (C2G1P2). Other concerns came from the usage of information by third parties. For example, a user stated that "*companies are always selling data to others, like marketing companies.*" (C1G1P3).

Furthermore, participants were *concerned about improper access (1.4).* This refers to concerns that data about individuals are readily available to people not properly authorized to view or work with this data [36]. "*The fact is that we are now sharing everything. You never know maybe one day you install one application, it can access your Gmail account, for example, as well.*" (C2G3P1).

Beyond adhering to Smith et al.'s [36] four key factors of an individual's privacy concerns, more concerns emerged. It was suggested that *legal consideration (1.5)* have an influence on a mobile user's privacy concerns. For example, one participant stated: "*I would like to sign a legal statement (with the provider), which could constraint the service provider not to collect and use my information when I use this application. This will make me feel safer.*" (C1G2P5).

Another important issue raised by participants is *reputation considerations (1.6).* "*If I don't know where this application comes from, I will not share any of my personal information because I do not trust it.*" (C2G3P3). "*If you are a small company, you have less IT capability in the sense that you know you cannot afford the whole team of people only in charge of security, while Google and Facebook can. It sounds more risky to give my information to you than Google and Facebook.*" (C2G2P1). People tend to provide information to big companies because they think big companies can afford good services without selling information to others, and big companies have more IT capability.

Our focus groups have also shown *concerns on agreement on information releasing (1.7).* "*Once the application is installed, and then suddenly one day you can decide to collect all the information on clouds, without notifying people; people even do not go to check what changes on the agreements are*" (C2G2P1). This dimension of privacy concern is somehow new in the mobile context as applications need to be updated constantly in order to improve services. Once users

click on "yes", they probably do not pay attention to the changes of agreement.

Analyzing of the focus groups helped us to get an in-depth understanding of mobile user privacy concerns. In addition to the traditional four key concerns of an individual's concerns, we also found legal considerations and reputation considerations and agreement on information releasing are sources of privacy concerns.

4.2. Privacy calculus

The main objective of our application is to protect mobile user personal information on mobile phones, by using an adaptive single sign on solution. Based on context-aware technology, such a solution is expected to achieve the proper trade-off between dynamic authentication and ease of use [5]. In the context of our study, all participants agreed that the concept has the potential to protect privacy, but several conditions much be met. We summarized key dimensions of privacy calculus in Table 2.

In addition to privacy concerns, perceived privacy risk is the next *risk belief (2.1)* reported by our participants. It is defined as perceived risk of opportunistic behavior related to the disclosure of personal information submitted by mobile users in general [14]. As one participant said: "*It is dangerous to give information to them (application provider), because you never know how they will use your information.*" (C1G1P1). Such risk belief is more likely to have a negative impact on an individual's willingness to provide personal information. In addition, one participant mentioned that if the application went well, new risks would emerge. "*If this (Privacy Manager) is going out, and this is good thinking, then it is going to be very valuable for people to want to hack it. Like LinkedIn, they got hacked recently: millions of their passwords came out...*" (C2G2P2).

It was also suggested that *confidence and enticement beliefs (2.2)*, that is, mobile applications are reliable and personal information provided to these applications is used and kept in safe environments should increase the willingness to use mobile application, and vice versa. This factor is related to trust on mobile applications. "*The phone is just a technology, I do not trust technology so there is no personal information on my phone…. Then why should I provide more very personal and detailed information to this application?*" (C2G2P4). "*I usually do not go to these accounts (Facebook, Gmail) with my phone. It is dangerous to do it because the phone is so easy to lose… Let me be in charge of taking care of my phone's security, and let me be in charge of convenience or inconvenience.*" (C2G2P2). Lower trust in mobile applications and smartphones in general should negatively influence users' willingness to disclose personal information to our application, and in turn influence their intentions to use it. This is consistent with Dinev & Hart's [14] finding that a lower level of interest was related to a lower level of willingness to provide the Internet with personal information.

We also include the concept of *benefit beliefs (2.3)* of "privacy manager" in our analysis. As mentioned earlier, this application is aimed at protecting the user's private information on their mobile phones. The greater the perceived benefit, the higher possibilities users want to use. "*I like this application because it can protect my personal information and security I think I'd love to take a try because I am a person who loses things very easily.*" (C2G1P3). In cases in which users do not care must about their information on their mobile phone, or the information on mobile phone is not very personal, the benefit of our application should decrease. This will result in lower intention to use our application. One participant confirmed this argumentation: "*Since I don't really care about keeping the information I store on my smartphone secret, I will not need such an application at the moment.*" (C1G3P2).

In the current study, the dependent construct, *willingness to act (2.4)*, falls into two categories: willingness to provide information and willingness to use the application. The former is an assessment about willingness to provide information to applications in general, whereas the latter reflects the individual's intention to use this specific application. A factor that affects user willingness to use this application and falls under the category of confidence and enticement beliefs was personal interests over applications. This refers to personal interest or cognitive attraction to mobile applications overriding privacy concerns. As one participant said: "*I usually grant access to a lot of information, thinking their worst use will not be so bad and because of curiosity…therefore I would like to try if this application is available on Google play.*" (C1G3P1).

Participants also highlighted other factors that have an impact on application adoption. We observed that the *control over information (2.5)* and *personalized features (2.6)* were frequently mentioned in the investigation. While other dimensions in privacy calculus are difficult to change, these two factors are possible for us to manipulate. We therefore incorporate participant feedback mainly on these two factors in order to design a positive user experience.

Consistent with previous findings, *control over information (2.5)* played an important role in privacy context. Typical comments include "*If my personal*

information is only stored on my phone, and not stored on the server, I will feel safe to give my information to this application." (C1G2P5). "*If I know clearly how my information will be used, I can share my information.*"(C1G2P3). As a result, participants suggested that the data (time and location) should not involve any third party. "*I just do not trust any third party, because they will use my information for money – even big companies, their employees may sell my information for money.*" (C1G1P3). Instead, "*I prefer my personal information to be only stored on my phone, and not on the server, so I, and only myself can access my information.*" (C1G2P1). Finally, it is also suggested to adopt an import/export option since "*recently, it is quite normal that one person has several mobile phones, and people change their mobile phones very often*." (C1G3P1)

Participants valued *personalized features (2.6)* in the application. For example, when talking about the notification mode in case where the Privacy Manager detects your phone is under an unusual circumstance, one participant said: "*I want to receive a ring to warn me, so I can use the password to unblock the phone if the phone is actually with me. In case I lose my phone then I prefer to receive an email, because otherwise I would not know.*"(C1G1P3). Another participant commented: "*I want the vibrate option, because it's in my pocket, nobody knows that, and I can check it later if I am busy at that particular moment*." (C1G2P4). Finally, some general comments: "*I think emails, the vibrate and alarm options are basic notifications, it would be nice to have them all. Hopefully, (they are) not exclusive.*" (C1G2P3) another participant in the same group agreed: "*Yes, these three functions are different but complementary. It is good for the user to choose and activate one or three notifications.*" (C1G2P2). Participants from other groups had a similar conclusion: "*I use both GPS and WiFi, so it should automatically switch one to another to get the efficient but precise location information.*" (C1G3P1). Other personalized features included location data collection. The first consideration is the data collection mode. Most participants suggested using WiFi if possible, because "*it can save battery*" (C1G1P1). Further, one participant recommended: "*It would be great if this application could automatically switch from 3G in case there is no WiFi, as WiFi is not available everywhere.*" (C1G1P3). Similarly, participants from another group said: "*I do care the battery of my phone, so normally I will not use GPS when there is WiFi. I would like this application to have the 'switch function' so that I don't have to change it by myself.*" (C1G2P1). The second consideration is comparison mode: Privacy Manager will compare the current location and time dimensions with the values stored in the training mode. The match between the current location and the expected location derived from training data can be an exact match or a fuzzy match, depending on the value "precision of localization" set by the user in the user's preferences. A common opinion among all participants was that it should use ambiguous comparison. For example, participants noted: "*The ambiguous comparison function is a must*" (C1G2P4). "*I need a rough range. If I go to the cafeteria to have a coffee, the exact coordinates are not useful, and I do not want to be bothered by this application frequently.*" (C1G1P2). Despite the location measure, another participant said: "*Of course with ambiguous, better with both time and distance*." (C1G1P3). Although she admitted that it might create new concerns: "*If it is not that precise, then other people, for example my colleagues can easily manipulate my phone with this application's notice.*" Finally we decide to provide both the distance option and the time option for users to select their preferences.

4.3. Evaluation of utility

This analysis focuses only on users from cluster 2. Our evaluation of utility is based on Davis's [11] technology acceptance model. According to this theory, technology usages depend on two variables: *perceived ease of use and perceived usefulness*.

Ease of use (3.1), which was defined as the degree to which a person believes that using a particular system would be free of effort [11], has been recognized as a crucial element towards the acceptance of the application [40]. Overall, participants found the Privacy Manager was easy to use. Typical comments include: "*It's a convenient tool for people who are interested in protecting their personal information and who have a regular life, like me.*" (C2G3P3).

Perceived usefulness (3.2), in contrast, refers to the degree to which a person believes that using a particular system would enhance his or her job performance. Some participants expressed interest in this application. "*To me, this application is useful because it can protect my information from someone else and help me to find my phone in case I lose it.*" (C2G1P3). "*I like the single sign on so that I do not have to enter my password for each services, plus my personal information is also protected.*" (C2G1P1). "*The application is very impressive. I have so many phones and contacts on my phone, it would be very useful to block my phone in case I lose it, so that others cannot access all of my personal stuff.*" (C2G2P3).

Nevertheless, both perceived ease of use and perceived usefulness have some restrictions, with respect to: (1) *user's mobility (3.3)* and (2) *user's risk attitude (3.4)*. On the one hand, our application might

be more applicable for people who have a regular life. One participant explained her concerns after using this application: "*The idea of this application is very attractive; however, my life is quite flexible. If it is going to pop up every time I go some places new, then that is too much: it means I have to change the profile in advance, otherwise the phone would get blocked and receive a notification… then I will get annoyed.*" (C2G2P1). On the other hand, it was also suggested that when the individual's private concerns are very high, our application is less attractive. "*I am afraid I would not use it. The tradeoff is too high. I mean the benefit that you give, I do not think it matches the convenience and also the information that we provide.*" (C2G2P2). Therefore user's risk attitude plays an important role in their acceptance.

As a consequence, 7 out of 10 participants in the second cluster of our study believed that Privacy Manager was useful for their life and expressed their willingness to continue to use it.

5. Conclusion and future research

In this study we have focused on privacy calculus for context-aware mobile applications and we have asked ourselves what the role played by personalization and control in design a context-aware mobile application to protect user's personal information would be. Our focus group investigation provided us with new insights about privacy calculus in the mobile context and how personalization and control over information can influence it.

Based on focus group interviews, our findings provided strong support for Smith et al.'s [36] four key factors of individual privacy concerns in the mobile context. In addition, we found three new dimensions of mobile user privacy concerns: (1) legal considerations, (2) reputation considerations and (3) agreement of information release.

Moreover, our results show the important roles of personalization and control over personal information in privacy calculus done by smartphones users.

Finally, we have introduced a new context-aware mobile application, which takes into account privacy concerns, personalization and data control, and we proved that our application is easy to use and perceived as useful. In addition, the user's mobility and the user's risk attitude have the strong influence on perceived usefulness.

There are two important limitations that should be taken into account prior to generalizing our results: (1) the common sample selection bias and (2) the common method bias. On the one hand, participants in our study tend to be young adults, and mobile users. Although we tried to recruit people from different backgrounds and different educational levels, we do not have a sample that is very representative of the population. For example, all participants are from Switzerland, a country where the possibility that a phone get stolen would rather low. On the other hand, while focus groups were a good way to achieve the research goal, individual interviews could also be conducted to provide compensatory and in-depth evidence. Moreover, as the extant literature shows, privacy concerns differ from person to person, and from situation to situation. Though our research was conducted in a real-life circumstance, it would be interesting to learn details about participants' situations when using our application by means of a diary study or experience-sampling method. Finally, privacy concerns are application dependent, and that implies that the data collected in our study is only relevant to the application being tested. Therefore, future research could address privacy calculus from a larger quantitative study with a more representative and heterogeneous population.

6. References

[1] Awad, N.F., and M.S. Krishnan, "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization", MIS Quarterly, 2006, pp. 13–28.

[2] Barkhuus, L., and A. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns", Proc. Interact, 2003, pp. 709–712.

[3] Benisch, M., P.G. Kelley, N. Sadeh, T. Sandholm, L.F. Cranor, P.H. Drielsma, and J. Tsai, "The impact of expressiveness on the effectiveness of privacy mechanisms for location sharing", DTIC Document, 2008.

[4] Beresford, A.R., A. Rice, N. Skehin, and R. Sohan, "MockDroid: trading privacy for application functionality on smartphones", Proceedings of the 12th Workshop on Mobile Computing Systems and Applications, 2011, pp. 49–54.

[5] Bonazzi, R., B. Fritscher, Z. Liu, and Y. Pigneur, "From 'security for privacy' to 'privacy for security'", The Third International Workshop on Business Model for Mobile Platforms, 2011.

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

[7] Christin, D., C. Roßkopf, and M. Hollick, "uSafe: A privacy-aware and participative mobile application for citizen safety in urban environments", Pervasive and Mobile Computing 84(11), 2012, pp. 1928–1946.

[8] Culnan, M.J., and P.K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", Organization Science 10(1), 1999, pp. 104–115.

[9] Culnan, M.J., and R.J. Bies, "Consumer privacy: Balancing economic and justice considerations", Journal of Social Issues 59(2), 2003, pp. 323–342.

[10] Davidson, D., and B. Livshits, “MoRePriv: Mobile OS Support for Application Personalization and Privacy”, Microsoft Research, 2012, 3 May.
[11] Davis, F.D., “Perceived usefulness, perceived ease of use, and user acceptance of information technology”, MIS Quarterly, 1989, pp. 319–340.
[12] Dinev, T., M. Bellotto, P. Hart, V. Russo, I Serra, and C. Colautti, “Privacy calculus model in e-commerce–a study of Italy and the United States”, European Journal of Information Systems 15(4), 2006, pp. 389–402.
[13] Dinev, T., and P. Hart, “Internet privacy concerns and their antecedents-measurement validity and a regression model”, Behaviour & Information Technology 23(6), 2004, pp. 413–422.
[14] Dinev, T., and P. Hart, “An extended privacy calculus model for e-commerce transactions”, Information Systems Research 17(1), 2006, pp. 61–80.
[15] Enck, W., P. Gilbert, B.-G. Chun, L.P. Cox, J. Jung, P. McDaniel, A.N. Sheth, “TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones”, Proceedings of the 9th USENIX conference on operating systems design and implementation, 2010.
[16] Hevner, A.R., S.T. March, J. Park, and S. Ram, “Design science in information systems research”, MIS Quarterly 28(1), 2004, pp. 75-105.
[17] Hong, W., and J.Y Thong, “Internet privacy concerns: An Integrated conceptualization and four empirical studies”, MIS Quarterly 37(1), 2013, pp. 275–298.
[18] Hui, K.-L., H.H. Teo, and S.-Y.T. Lee, “The value of privacy assurance: an exploratory field experiment”, MIS Quarterly 31(1), 2007, pp. 19–33.
[19] Junglas, I.A., N.A. Johnson, and C. Spitzmüller, “Personality traits and concern for privacy: an empirical study in the context of location-based services”, European Journal of Information Systems 17(4), 2008, pp. 387–402.
[20] Kenteris, M., D. Gavalas, and D. Economou, “An innovative mobile electronic tourist guide application”, Personal and Ubiquitous Computing, 2009, pp. 103–118.
[21] Kitzinger, J., “Qualitative research: Introducing focus groups”, British Medical Journal 311(7000), 1995, pp. 299.
[22] Kobsa, A., “Privacy-enhanced personalization”, Communications of the ACM 50(8), 2007, pp. 24–33.
[23] Lacey, A. and D. Luff, Qualitative Research Analysis. Sheffield: University of Sheffield, 2007.
[24] Liu, Z., R. Bonazzi, B. Fritscher, and Y. Pigneur, “Privacy-friendly business models for location-based mobile services”, Journal of Theoretical and Applied Electronic Commerce Research 6(2), 2011, pp. 90–107.
[25] Maamar, Z., S. Kouadri, and H. Yahyaoui, “A web services composition approach based on software agents and context”, Proceedings of the 2004 ACM symposium on Applied computing, 2004, pp. 1619–1623.
[26] Malhotra, N.K., S.S. Kim, and J. Agarwal, “Internet users’ information privacy concerns (IUIPC): The construct, the scale, and a causal model”, Information Systems Research 15(4), 2004, pp. 336–355.
[27] Mohan, P., V.N. Padmanabhan, and R. Ramjee, “Nericell: rich monitoring of road and traffic conditions using mobile smartphones”, Proceedings of the 6th ACM conference on Embedded network sensor systems, 2008, pp. 323–336.
[28] De Montjoye, Y.-A., S.S. Wang, A.S. Pentland, “On the trusted use of large-scale personal data”, Data Engineering, 2012, pp. 1–5.
[29] Oliver, R.L., “Expectancy theory predictions of salesmen’s performance”, Journal of Marketing Research, 1974, pp. 243–253.
[30] Phelps, J., G. Nowak, and E. Ferrell, “Privacy concerns and consumer willingness to provide personal information”, Journal of Public Policy & Marketing, 2000, pp. 27–41.
[31] Powell, R.A., and H.M. Single, “Focus groups”, International Journal for Quality in Health Care 8(5), 1996, pp. 499–504.
[32] Raento, M., A. Oulasvirta, R. Petit, and H. Toivonen, “ContextPhone: A prototyping platform for context-aware mobile applications”, Pervasive Computing, IEEE 4(2), 2005, pp. 51–59.
[33] Roman, M., and R.H. Campbell, “A user-centric, resource-aware, context-sensitive, multi-device application framework for ubiquitous computing environments”, Urbana, 2002.
[34] Sandhu, R.S., and P. Samarati, “Access control: principle and practice”, Communications Magazine, IEEE 32(9), 1994, pp. 40–48.
[35] Sheng, H., F.F.-H. Nah, and K. Siau, “An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns”, Journal of the Association for Information Systems, 2008, pp. 344–376.
[36] Smith, H.J., S.J. Milberg, and S.J. Burke, “Information privacy: measuring individuals’ concerns about organizational practices”, MIS Quarterly, 1996, pp. 167–196.
[37] Srivastava, A., and S.B. Thomson, “Framework analysis: a qualitative methodology for applied policy research”, JOAAG 4(2), 2009, pp. 72–79.
[38] Stewart, K.A., and A.H. Segars, “An empirical examination of the concern for information privacy instrument”, Information Systems Research 13(1), 2002, pp. 36–49.
[39] Toch, E., J. Cranshaw, P. Hankes-Drielsma, J. Springfield, P.G. Kelley, L. Cranor, J. Hong, N. Sadeh, “Locaccino: a privacy-centric location sharing application”, Proceedings of the 12th ACM international conference adjunct papers on Ubiquitous computing-Adjunct, 2010.
[40] Venkatesh, V., “Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model”, Information Systems Research 11(4), 2000, pp. 342–365.
[41] Ward, S., K. Bridges, and B. Chitty, “Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information”, Journal of Marketing Communications, 2005, pp. 21–40.
[42] Xu, H., X.R. Luo, J.M. Carroll, and M.B. Rosson, “The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing”, Decision Support Systems 51(1), 2011, pp. 42–52.
[43] Xu, H., and H.-H Teo. “Alleviating consumer’s privacy concern in location-based services: A psychological control perspective”, Proceedings of the Twenty-Fifth International Conference on Information Systems, 2004, pp. 793–806.