Year : 2014

Adaptive Privacy Management System Design For Context-Aware Mobile Devices

Zhan LIU

UNIL | Université de Lausanne

FACULTÉ DES HAUTES ÉTUDES COMMERCIALES

DÉPARTEMENT DES SYSTÈMES D'INFORMATION

Adaptive Privacy Management System Design For Context-Aware Mobile Devices

THÈSE DE DOCTORAT

présentée à la

Faculté des Hautes Etudes Commerciales
de l'Université de Lausanne

pour l'obtention du grade de
Docteur en Systèmes d'Information

par

Zhan LIU

Directeur de thèse
Prof. Yves Pigneur

Jury

Prof. Alessandro Villa, Président
Prof. Benoît Garbinato, expert interne
Prof. Gang Fang, expert externe
Prof. Jean-Fabrice Lebraty, expert externe

LAUSANNE
2014

UNIL | Université de Lausanne
HEC Lausanne

Le Décanat
Bâtiment Internef
CH-1015 Lausanne

IMPRIMATUR

Sans se prononcer sur les opinions de l'auteur, la Faculté des hautes études commerciales de l'Université de Lausanne autorise l'impression de la thèse de Monsieur Zhan LIU, titulaire d'un Bachelor en Informatique de Gestion de la HES-SO Valais-Wallis, titulaire d'un Master en Systèmes d'Information de l'Université de Lausanne, en vue de l'obtention du grade de docteur en Systèmes d'Information.

La thèse est intitulée :

ADAPTIVE PRIVACY MANAGEMENT SYSTEM DESIGN FOR CONTEXT-AWARE MOBILE DEVICES

Lausanne, le 9 septembre 2014

Le doyen

Thomas von Ungern-Sternberg

Jury

Professor Yves Pigneur
Professor at the Faculty of Business and Economics of the University of Lausanne, Lausanne, Switzerland.
Thesis supervisor.

Professor Alessandro Villa
Professor at the Faculty of Business and Economics of the University of Lausanne, Lausanne, Switzerland.
President of the Jury.

Professor Benoît Garbinato
Professor at the Faculty of Business and Economics of the University of Lausanne, Lausanne, Switzerland.
Internal expert.

Professor Gang Fang
Associate Professor at the Management School of Hangzhou Dianzi University, Hangzhou, China.
External expert.

Professor Jean-Fabrice Lebraty
Professor at the University of Lyon School of Management (IAE Lyon), Lyon, France.
External expert.

University of Lausanne
Faculty of Business and Economics

Doctorate in Business Information Systems

I hereby certify that I have examined the doctoral thesis of

Zhan LIU

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature :  Date : 3 septembre 2014

Prof. Yves PIGNEUR
Director of thesis

University of Lausanne
Faculty of Business and Economics

Doctorate in Business Information Systems

I hereby certify that I have examined the doctoral thesis of

Zhan LIU

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature :  Date : Sept 2014

Prof. Benoît GARBINATO
Internal member of the doctoral committee

University of Lausanne
Faculty of Business and Economics

Doctorate in Business Information Systems

I hereby certify that I have examined the doctoral thesis of

Zhan LIU

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature : Gang Fang Date : 23 September 2014

Prof. Gang FANG
External member of the doctoral committee

University of Lausanne
Faculty of Business and Economics

Doctorate in Business Information Systems

I hereby certify that I have examined the doctoral thesis of

Zhan LIU

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature :  Date : September 3rd 2014

Prof. jean-fabrice LEBRATY
External Expert

Abstract

Version française au verso.

While mobile technologies can provide great personalized services for mobile users, they also threaten their privacy. Such personalization-privacy paradox are particularly salient for context aware technology based mobile applications where user's behaviors, movement and habits can be associated with a consumer's personal identity.

In this thesis, I studied the privacy issues in the mobile context, particularly focus on an adaptive privacy management system design for context-aware mobile devices, and explore the role of personalization and control over user's personal data. This allowed me to make multiple contributions, both theoretical and practical. In the theoretical world, I propose and prototype an adaptive Single-Sign On solution that use user's context information to protect user's private information for smartphone. To validate this solution, I first proved that user's context is a unique user identifier and context awareness technology can increase user's perceived ease of use of the system and service provider's authentication security. I then followed a design science research paradigm and implemented this solution into a mobile application called "Privacy Manager". I evaluated the utility by several focus group interviews, and overall the proposed solution fulfilled the expected function and users expressed their intentions to use this application. To better understand the personalization-privacy paradox, I built on the theoretical foundations of privacy calculus and technology acceptance model to conceptualize the theory of users' mobile privacy management. I also examined the role of personalization and control ability on my model and how these two elements interact with privacy calculus and mobile technology model. In the practical realm, this thesis contributes to the understanding of the tradeoff between the benefit of personalized services and user's privacy concerns it may cause. By pointing out new opportunities to rethink how user's context information can protect private data, it also suggests new elements for privacy related business models.

English version on the front.

Alors que les technologies mobiles peuvent offrir d'excellents services personnalisés pour les utilisateurs mobiles, elles menacent aussi leur vie privée. Un tel paradoxe de personnalisation-vie privée joue un rôle majeur pour les technologies servant aux applications mobiles basées sur les données contextuelles, où le comportement des utilisateurs, leurs mouvements ou habitudes peuvent être associés à l'identité personnelle d'un consommateur.

Dans cette thèse, j'ai étudié les questions de la vie privée dans le contexte mobile, en mettant l'accent sur une conception de système de gestion de la vie privée adapté pour les appareils mobiles sensibles au contexte, et exploré le rôle de la personnalisation et du contrôle sur les données personnelles de l'utilisateur. Cela m'a permis de faire plusieurs contributions, à la fois théoriques et pratiques. Dans le monde théorique, je propose un prototype d'une solution de Single-Sign On adaptative pour Smartphone qui utilise les informations de contexte de l'utilisateur pour protéger ses renseignements personnels. Pour valider cette solution, j'ai d'abord prouvé que le contexte de l'utilisateur est un identifiant unique de l'utilisateur et que la technologie sensible au contexte peut augmenter perception de facilité de l'utilisateur sur l'utilisation du système et la sécurité de l'authentification du fournisseur de services. J'ai ensuite suivi un paradigme de recherche en sciences de la conception et mis en œuvre cette solution dans une application mobile appelée «Privacy Manager». J'ai évalué l'utilité par le moyen de plusieurs entretiens avec des groupes de discussion, et dans l'ensemble solution proposée satisfait les fonctionnalités attendues, et les utilisateurs ont exprimé leur intention d'utiliser cette application. Pour mieux comprendre le paradoxe de personnalisation-vie privée, j'ai établis, en se basant sur les fondements théoriques, un modèle de calculs et d'acceptation technologique pour conceptualiser la théorie de la gestion de vie privée des utilisateurs mobiles. J'ai aussi examiné le rôle de la personnalisation et de la capacité de contrôle sur mon modèle et la manière dont ces deux éléments interagissent avec le calcul de vie privée et le modèle de la technologie mobile. Dans le domaine pratique, cette thèse contribue à la compréhension de l'arbitrage entre le bénéfice de services personnalisés et les préoccupations de la vie privée de l'utilisateur qu'elle peut causer. En signalant de nouvelles possibilités pour repenser la façon dont les informations de contexte de l'utilisateur peuvent protéger les données privées, elle suggère aussi de nouveaux éléments pour les modèles d'affaires liés à la vie privée.

Acknowledgements

The completion of my dissertation has been a long journey. It would not have been possible without the help, support and encouragement of the kind people around me. Over the past five years from 2009 to 2014, they have contributed not only to my academic success, but also to my personal growth.

First and foremost, I gratefully and sincerely thank my PhD dissertation supervisor, **Professor Yves Pigneur** for his help, advice, guidance, and encouragement, as well as his enthusiasm and many valuable contributions to this work. Without him, I would not have been able to complete my thesis. Under his guidance, I successfully overcame many difficulties and learned a lot. His friendship and support has meant more to me than I could ever express.

I also thank my thesis committee members, **Professor Benoît Garbinato**, **Professor Gang Fang**, and **Professor Jean-Fabrice Lebraty** for taking time to review this thesis and for their support and valuable comments. Their suggestions and observations were extremely helpful throughout this thesis.

As well, I thank to my friends and colleagues at HEC Lausanne. I am extremely indebted to **Dr. Riccardo Bonazzi** for his support, guidance, and insightful suggestions. As a senior doctor, he taught me how to conduct effective research and offered advice many times during my PhD study. I want him to know how much I appreciate all that he has done for me. I also am very grateful to **Dr. Fabio Daolio**, we spent a number of hours discussing the research, particularly in data analysis using the machine learning method. I also appreciate **Dr. François Vessaz**'s valuable suggestions and kind help during the data collection and I thank **Dr. Boris Fritscher**, **Alexandre Métrailler**, and **Ulysse Rosselet** who shared the office room with me. I spent wonderful time with them on various topics that allowed relaxation from research.

My heartfelt thanks to my colleagues at HES-SO Valais in Sierre, **Professor Anne Le Calvé**, **Fabian Cretton**, **Professor Nicole Glassey Balet**, and **Dr. Vincent Grèzes**. I am very lucky to have worked with you during my PhD journey. Your warm heart and kindness encouraged to complete this thesis. I am extremely honored and grateful to continue my professional career with you.

Furthermore, I sincerely acknowledge the Lausanne Data Collection Campaign run by **Nokia Research Center Lausanne** for providing a large amount of data pertaining to the behaviour of individuals and social networks that helped me to achieve the research objectives.

My parents, **Qingmin Yan** and **Shusheng Liu**, are the most remarkable people I have ever met. I thank them for their unconditional support and the confidence and love they have shown to me. I wish I could show them just how much I love and appreciate them. I also thank my parents-in-law, **Yuewen Zhou** and **Bingrui Shan** for their sincere encouragement and support.

Finally, and most importantly, I am most sincerely grateful to my wife **Dr. Jialu Shan**. I know how very fortunate I am to have you in my life. You are my greatest strength and I appreciate all your support, encouragement, and unwavering love. I am so lucky to share my life with you, and have our lovely daughter **Zixin Lisa Liu**. I hope that this thesis has made you proud.

A number of other people not mentioned here also made significant contribution to this research. I thank all of them.

Contents

List of Figures

List of Tables

Glossary

Adaptive single-sign on	The way is to use mobile user's context-aware based privacy information as a unique identifiable pattern to protect personal information in the mobile device.
Authentication security	The number of true positives and true negatives obtained by the system. In other words, to minimize the number of occurrences in which the user is not allowed to access the system (false negative) or an unauthorized person is allowed to access the system (false positive).
Context	Any information that can be used to characterize the situation of a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves (Dey and Abowd, 2000).
Context-aware application	A context-aware application has three main components: a set of sensors for detecting and capturing contextual information, a set of rules that governs behavior according to context, and a set of actuators for generating responses (Biegel and Cahill, 2004).
Control	Degree to which a mobile user perceives that mobile service companies give him or her procedures for control of information privacy and make him or her aware of the procedures (Son and Kim, 2008).
Ease of use	Reducing the number of human-computer interactions required for authentication (Venkatesh, 2000).
Perceived benefits	Either monetary or non-monetary, had a positive influence on their intention to disclose personal information (Dinev and Hart, 2006).

Perceived ease of use	The degree to which a person believes that using a particular system would be free of effort (Davis, 1989, p.320).
Perceived enjoyment	The degree to which fun can be derived through the use of technology or a particular service (Xu et al., 2013).
Perceived risks	The expectation of losses associated with the release of personal information to the service provider (Xu et al., 2010, p.149).
Perceived usefulness	The degree to which a person believes that using a particular system would enhance his or her job performance (Davis, 1989, p.320).
Personalization	The ability to proactively tailor products and product purchasing experiences to tastes of individual consumer based upon their personal and preference information (Chellappa and Sin, 2005).
Privacy	The interest people have in controlling, or at least significantly influencing, the handling of information about themselves (Belanger and Crossler, 2011, P.1018).
Privacy calculus	Cost-benefit tradeoff analysis in which personal information is given in return for certain economic or social benefits (Dinev and Hart, 2006).
Privacy concerns	Four kinds of privacy concerns are identified by Smith et al. (1996): collected and stored, unauthorized secondary use, improper access and errors.
Security	The protection against threats from potential circumstances, conditions, or events that cause economic hardship.
Single Sign-On	A property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.
Support vector machines	A type of supervised learning models with associated learning algorithms that analyze data and recognize patterns, used for classification and regression analysis.

TAM	The technology acceptance model (TAM) is an adaptation of the theory of reasoned action (TRA), which was specifically tailored for modeling user acceptance of information systems (Davis et al., 1989).
User's payoff	Degree to which a mobile user perceives as fair the benefits he or she receives from mobile service companies in return for the release of personal information (Son and Kim, 2008).

References

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information System," *Management Information Systems Quarterly* (35: 4), pp.1017-1041.

Biegel, G., and Cahill, V. 2004. "A Framework for Developing Mobile, Context-Aware Applications," In Proc. of the 2nd IEEE Conference on Pervasive Computing and Communications, Percom 2004, pp. 361-365.

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

Davis, F. D. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *Management Information Systems Quarterly* (13:3), pp. 319-340.

Dinev, T. and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," Information Systems Research (17:1), pp. 61-80.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *Management Information Systems Quarterly* (20:2), pp. 167-196.

Son, J. Y., and Kim, S. S. 2008. "Internet users' information privacy-protective responses: A taxonomy and a nomological model," *Management Information Systems Quarterly* (32:3), pp. 503-529.

Xu, H., Teo, H-H., Tan, B. C. Y., and Agarwal, T. 2010. "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.

Xu, J. D., Benbasat, I, and Cenfetelli, R. T. 2013. "Integrating Service Quality with System and Information Quality: An Empirical Test in the E-Service Context," *Management Information Systems Quarterly* (37:3), pp.777-794.

Venkatesh, V. 2000. "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information systems research* (11:4), pp. 342-365.

Chapter 1

Introduction

1.1 Research Context

Just as computers have radically changed almost every field of people's lives, so too has the revolution in smartphone use. Along with the development of new technologies such as Global Positioning System (GPS), smartphones not only make it possible to access information, but they also allow individuals to stay connected "everywhere, anytime" (Pallapa et al., 2013). More significantly, however, they support people's daily activities. Since smartphones first came into use in 2007, they have been experiencing unprecedented rates of adoption. According to Euromonitor, in 2012 over half (55%) of American adults owned a smartphone. Such a high penetration rate enables users to conveniently access mobile services via various mobile applications.

Smartphones have been found to have positive effects in terms of maintaining and building social relationships, as well as enhancing and improving communication, giving quick accessing to information, providing entertainment, increasing productivity, and more (Addo, 2013; Keith et al., 2013). The advantages of using mobile phones include rich information, competitive pricing and convenience. As a consequence, mobile business, including advertising, shopping and other mobile services, has exploded. A study carried out by Forrester Research has predicted that mobile commerce sales in US will grow from $3 billion in 2010 to $31 billion in 2016. It also reported that revenue sales from smartphone and tablet retail purchases by European and US shoppers in 2015 are expected to reach $67.1 billion (Business Insider, 2013). Such phenomena demonstrate that customers are increasingly dependent on mobile devices to search information and make purchases.

Whilst mobile phone use can bring advantages to users, it can also have negative influences. The proliferation of smartphones and the wide-spread use of mobile applications in our society, together with the abundance of information available on mobile phones, raise questions about citizens' privacy. The personal information that companies gather can be misused; for example, they may send unwanted emails or sell information to third parties. Dhilon and Moores (2001) identified the most important privacy concerns of Internet users. These include companies' use of spam, the selling of personal information, the prevention of theft of personal information, the elimination of the risk of losing personal files, and the maximization of security. Mobile users may have similar or even stronger concerns about these issues because mobile phones use a similar mechanism but are more personal and portable. Wu and Wang (2005) argued that business concerns, privacy protection, security, and a risk-free environment are the breakpoints for mobile commerce popularity. Privacy concerns become one of the essential factors considered by consumers when deciding whether to use mobile services and mobile commerce.

Regardless of people's privacy concerns over mobile phone use, the market for mobile commerce is booming. Personalization is considered the key factor for the success of mobile services and mobile applications. It can be generally defined as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumer based upon their personal and preference information" (Chellappa and Sin, 2005). Mobile users always have their mobile devices with them. Thus, instead of thinking about how to make their next sale, companies need to focus more on personalizing their efforts to reach their audience more effectively.

One basic element used in personalization is the context of the user. When a service is regarded as context-aware, this means that it uses context to provide relevant information and/or services to the user. Such relevancy depends on the task being carried out by the user (Dey, 2001). Thanks to GPS technology, a user's location can be measured accurately, and thus becomes the key contextual element. Consequently, location-based services (LBS) are now considered as an important source of revenue opportunity for multiple stakeholders in the mobile value chain (Rao and Minakakis, 2003).

However, some of this contextual information may be considered to be of a sensitive nature. To mobile users, the use of a location-based mobile application and its relevant services seems a double-edged sword, or a "*personalization-privacy paradox*" (Sutanto et al., 2013; Xu et al., 2011). On the one hand, users may identify great value in receiving personalized services for which the contents and design are adapted; on the other hand, they may be afraid of the potential privacy risks associated with disclosed personal information.

So far, location-based applications have mainly been studied from a technical point of view; thus, the user dimension has received little attention from the Information System community. In recent years, Anderson (2001) has advocated that information security should result from the alignment of technical, business and regulatory dimensions. This understanding is consistent with contingency theory, which claims that the optimal course of action is contingent upon both the internal and external situations. Bonazzi et al. (2011) added a fourth dimension – a user dimension. They argued that user awareness of privacy involves both external and internal factors. Mobile users are different and they may use the same services for many different tasks, sometimes for tasks that were not anticipated in the design (Kaasinen, 2003). Hence, to get a better understanding of dynamic privacy management, it is important to understand users' perceptions of the privacy issues involved.

Consequently, the balancing of information privacy concerns against the advantages of LBS and the way in which mobile users make privacy-related decisions has become an interesting topic for researchers. After reviewing information privacy research, however, I found that the majority focus intensively on an online setting. What is missing is the application of research to the mobile world. Bélanger and Crossler (2011) called for greater consideration of design and action with an emphasis on building actual implementable tools to protect information privacy. Inspired by this, I had the idea of developing an adaptive privacy management system based on context-aware technology. I also wished to examine the factors that influence individuals' use of technology and their reactions to information privacy in a mobile context.

1.2 Theoretical Background

Before moving to the framework of my doctoral thesis, it is important to first take a step back to examine the nature of privacy and identify the state-of-the-art in information system research.

1.2.1 Privacy at a Glance

What is privacy? Initial legal opinions, which date back to the late nineteenth century, identify privacy as "the right to be let alone" (Warren and Brandeis, 1890). Although privacy is usually contextually dependent (i.e., Sheng et al., 2008), people place a high value on it as an expression of their dignity. Therefore, in the context of mobile services, I have adopted the economic perspective of information privacy, defining it as "the interest people have in controlling, or at least significantly influencing, the handling of information about themselves" (Bélanger and Crossler, 2011, P.1018).

1.2.2 Information Privacy Concerns

Information privacy concerns refer to an individual's subjective concerns within the context of information privacy (Malhotra et al., 2004). Variations in individuals' privacy concerns depend on many factors. According to Ackerman (2004), such concerns can be classified by the type of concern held or the degree of concern felt. Smith et al. (1996) identified four kinds of privacy concerns. First, people are concerned about too much personal information being *collected and stored*. Second, people are concerned about the risk of *unauthorized secondary use*. In other words, the information is collected from individuals for one purpose, but it is reused for another purpose – either internally within a single organization or externally with a third party – without authorization from those individuals. Third, people have a general anxiety about *improper access*. Finally, they are also concerned about their inability to correct *errors* in their personal data. Individuals also differ in their levels of privacy concerns. For example, some people might be indifferent to privacy, whereas some are extremely uncompromising. Ackerman et al. (1999) considered these two groups as *marginally concerned* and *privacy fundamentalist*; another group – the *pragmatic majority* – is positioned in between the two. Sheehan (2001) further divided the pragmatists into two groups: *circumspect* internet users and *wary* internet users. He rated the former's total concerns as being lower than the latter.

Other personal factors that may influence privacy concerns include gender (Chen et al., 2013; Kuo et al., 2007), age (Gervey and Lin, 2000; Graeff and Harmon, 2002) and other demographic factors. Overall, male and young consumers tend to exhibit fewer information privacy concerns, and show a higher level of willingness to disclose personal data than female and older consumers.

Apart from personal characteristics, which are usually considered as internal factors, environmental impacts focus more on external influences that occur over time. Such impacts may come, for example, from cultural differences (e.g., Dinev et al., 2007; Zhang et al., 2007), or national regulations (e.g., Milberg et al., 1995).

1.2.3 Privacy Calculus

Boritz and No (2011) identified five approaches to the gathering of personal information. Traditional ways include registration or an ordering process, the capturing of IP addresses and using "cookies" to track users' preferences and behavioral information. They argued that more recently, two other means of gathering personal information have become available: (1) through social networks such as Facebook and Twitter; and (2) through the use of other new and emerging technologies such as global positioning systems, which are embedded in mobile devices and cloud computing. These new tracking technologies may help companies to provide more customized products and services; however, they

may also create privacy issues for customers. Such personal data collection is often seen as an invasion of privacy because of concerns by mobile users that companies may sell, trade or share their information to other third parties without their knowledge or consent. As a consequence, customers may choose to provide none, some, or extensive information to a website or service provider. When they perceive that privacy concerns are high, customers tend to provide as little information as possible. Indeed, sometimes customers give false data intentionally (Awad and Krishnan, 2006; Dinev and Hart, 2007). In some extreme cases, privacy concerns may even lead to the avoidance of giving information. However, such concerns also pose problems for advertisers and marketers who seek to use such data to tailor their products and services and target future campaigns. In fact, an individual's decision making about privacy often involves a cost-benefit tradeoff analysis in which personal information is given in return for certain economic or social benefits. Such a cost-benefit analysis is usually referred to as a *privacy calculus* (e.g., Culnan and Armstrong, 1999; Dinev and Hart, 2006). Within this framework, users determine whether to disclose information after weighing up the benefits that will be gained against any risks in terms of the way in which their information will be used. The anticipation of benefits, either monetary or non-monetary, is expected to have a positive influence on users' intentions to disclose personal information. The expected potential risk is predicted to be negatively related to the intention to provide personal information. Only in cases in which perceived benefits exceed the risks will individuals be willing to provide information to a company and use the services provided by that company.

In order to reduce fears that personal information will be disclosed, consumers may look for privacy information by searching for a privacy policy statement (e.g., Meinert et al., 2006; Wu et al., 2012), privacy seals of approval (e.g., Miyazaki and Krishnamurthy, 2002) and other similar information. There is some evidence that privacy concerns may be reduced if websites present comprehensible privacy policies. These privacy policies actually increase a customer's ability to take control of their personal information; that is to say, users have the ability to determine the sort of information they will share, with whom they will share it, and the way in which the dissemination of information will be controlled.

While there exist numerous studies on privacy calculus in an online setting, research in the mobile context is notably lacking. Thus, I intend to provide the relevant evidence to fill this gap.

1.2.4 Technology Acceptance Model (TAM)

The intention to use products and services via mobiles is influenced not just by privacy calculus; it can also be explained by the *technology acceptance model* (TAM) (Davis,

1989; Davis et al., 1989). After all, in essence a smartphone is a mobile computer and, thus, is a type of information technology. According to this model, the intention to use an information system is primarily dependent on two particular beliefs: perceived usefulness and perceived ease-of-use. It has been proved that the former construct is a stronger determinate of usage intentions. Nevertheless, in the mobile context, which typically involves a location-based environment, users are more engaged. A greater amount of personal information such as contacts, messages and photos is stored in mobile phones, which may bring new risks for mobile users. It is therefore necessary to re-visit the TAM and to examine new antecedents of users' intentions to provide personal information and use mobile services.

1.3 Organisation and Structure

This thesis is composed of a collection of articles published in proceedings of conferences and journals in the field of information systems during my doctoral study. The advantages of this structure are that each article can be read independently while keep them interrelated with each other under my research framework. Three articles (chapter 2 to chapter 4) describe my core research, and another two articles which are situated in the appendix represent my preliminary research. The roles of my preliminary research are to explore the characteristics of a privacy management system for using a context-aware mobile device, as well as to observe the user's behavior (e.g., user's tradeoff) when using the privacy related mobile application. Therefore, the preliminary research can be considered as a good theoretical foundation to lead the departure of the core research in my thesis. Therefore, in this section, I firstly introduce the summary of my preliminary research, and then I describe the core thesis research with the main objectives and research questions. My thesis framework gives a sold structure and illustrates the focus areas and interdependency between each essay.

1.3.1 Preliminary Research

1.3.1.1 User's Perspective[1]

Designing a privacy risk management system is a dynamic process that is affected by both external and internal factors. Hence, a privacy risk management application should take into account the three main contingency factors suggested by Anderson (2001):

[1] The full research paper, "A Dynamic Privacy Manager for Compliance in Pervasive Computing", was published in *Privacy Protection Measures and Technologies in Business Organization: Aspects and Standards,* IGI Global, edited by G.O.M. Yee, 2012, pp. 285-307. The published version is included in the Appendix A.

- *Technology awareness*: i.e., an understanding of the technological options for privacy management that are offered to the user in a determined moment.
- *Business awareness*: i.e., the acknowledgment of prescriptive studies in the economic literature, which can improve privacy management.
- *Regulatory awareness*: i.e., the continuous assessment of laws and standards those apply to a determined environment.

The Wireless World Research Forum has developed a vision of I-centric communication in which the individual user, "I", has to be put at the center of service provisioning. This is in contrast with the offering of inflexible services that do not take into the account the actual needs of consumers (Arbanowski et al., 2004). As a result, it is important to add a fourth dimension - user awareness - to the list of contingency factors, because it involves both external and internal factors:

- *User awareness*: from a social point of view, two levels of analysis can be investigated. One could consider user behavior as an external contingency factor that affects the privacy of a specific user, e.g., different cultures and countries are said to behave differently in terms of privacy concerns (e.g., Japanese people are more likely to share data than Swiss users). Yet, at a personal level, user awareness is also an internal factor.

To date, the user dimension has received little attention from the information system community. Thus, in this thesis, I will investigate the implications of user awareness for privacy management system design.

1.3.1.2 Personalization and Control in the Mobile Context[2]

In the context of personalized services and applications for smartphones, users also crave contextually relevant and targeted information. The reasons are twofold: on the one hand, customers are not willing to deal with huge amounts of information and complex functionalities and personalization, even if the latter allow them to access potential cost savings (e.g., searching costs). This is especially true in today's business environment in which a plethora of choices is available. On the other hand, mobile customers can get contextualization value from, for example, relevant promotion information based on their interests, activities, identity, location, and time of the day (Junglas and Watson, 2006). However, such personalization also triggers customers' privacy concerns (Culnan and Armstrong, 1999).

[2] The full research paper "Privacy-Friendly Business Models for Location-Based Mobile Services" was published in the Journal of *Theoretical and Applied Electronic Commerce Research*, Vol. 6, Issue 2, 2011, pp. 90-107. The published version is attached in the Appendix B.

To date, much research has focused on understanding the relationship between users' privacy concerns and the willingness to disclose personal information to online companies (e.g., Chellappa and Sin, 2005; Dinev and Hart, 2007; Malhotra et al., 2004). However, few researchers have sought to examine the issues that can arise in a mobile context. Regardless of the fact that there are some similarities between online and mobile settings, location-based mobile services have their own unique features, which set them apart from their online counterparts. Therefore, one question need to be raised before I can move to the main topic of my research: what is the specificity of privacy management in location-based mobile services?

Most existing studies have found that privacy concerns are a major predictor of people's willingness to provide personal information. Here, the decision as to whether or not to disclose personal information is considered as a component of user payoff. User payoff can be regarded as the degree to which a mobile user perceives as fair the exchange of personal information disclosure in return for benefits (Son and Kim, 2008). This understanding is also consistent with the theory of privacy calculus, where customers trade off the privacy costs associated with sharing information against the value obtained from personalized information and services (Dinev and Hart, 2006).

How do I increase users' payoff? Such payoff comes from two main sources: an increase in the benefits they can receive and the reduction of risks related to the release of their personal information. As mentioned previously, an efficient way of improving the usability of mobile phones and increasing users' perceived value of LBS is to design the contents and services to directly meet the needs of individual users. To achieve this, mobile users have to disclose accurate personal information such as their locations, lifestyle habits, and behaviors. This kind of disclosure, however, leads to a potential loss of mobile users' privacy. Research has suggested that this kind of risk can be offset by an increase in users' ability to control their disclosure of personal data (e.g., Malhotra et al., 2004). Lack of such control may decrease mobile users' trust in the service provider. Here, two important factors can be identified: personalized services and mobile users' control over their information. The question that remains is: what is the role of these two factors in terms of the personal data disclosed and users' payoff?

To test the effect of the data disclosed, service personalization and data control over user payoff, I designed a 2X2X2 scenario-based survey, with each construct given a low level and a high level. A total of 187 students voluntarily participated in the survey. The sample was selected for reasons of availability and cost-effectiveness. It fulfills the research purpose as this study can be seen as preliminary research into the specificity of privacy issues in the mobile service context.

Several regression tests were conducted. The results revealed that: (1) the personal data disclosed by users has a negative effect on user payoff; (2) the amount of personalization available has a direct and positive effect, as well as a moderating effect, on the relationship of personal data disclosed and user payoff; and (3) the amount of control over a user's personal data has a direct and positive effect on user payoff. Thus, the proposed model was supported overall. The results of the regression tests are shown in Figure 1.1.

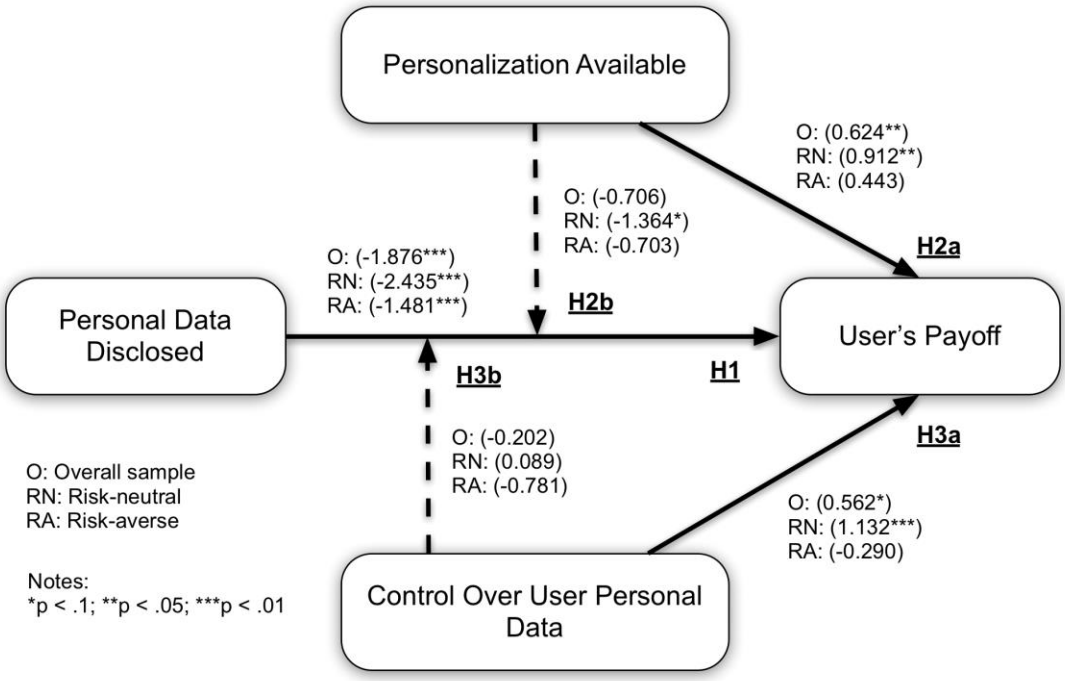


Figure 1.1. Theoretical model of user payoff

This simple model extends privacy management into a mobile business setting. It also suggests that both personalized services and control over a user's ability have a strong and positive impact on user payoff. Therefore, in this thesis, if I am to better understand privacy issues in the mobile context, it is important to consider these two factors.

1.3.2 Core Research

1.3.2.1 Main Objective and Research Questions

Although several researchers have addressed privacy issues in e-commerce, far fewer studies have empirically examined issues surrounding LBS smartphones. As Boritz and

No (2011) noted following their review of 116 key studies from four journal databases (AAA Digital Library, ACM Digital Library, ABI Inform (ProQuest), and ScienceDirect) between 1993 and 2009, "research on e-commerce privacy published in the four research databases covered by the review peaked in the early 2000s. Thus it has not addressed many of the privacy issues arising from technological advances during the past decade such as Internet access through mobile devices…." (p.12). Even fewer researchers have taken a theoretical approach in order to manipulate the relevant variables, or used experiments to establish causalities. Studies of privacy issues that use a design science approach (e.g., building on a mobile application artifact) are also notably lacking.

Therefore, this doctoral thesis seeks to gain a better understanding of privacy issues in a mobile context through an adaptive privacy management application. More precisely, I intend to first take a look at the role of context-aware services from a completely different perspective. In most studies, users' privacy issues that rise in context-aware services are usually considered as a burden. But can such privacy information actually be beneficial in protecting users' privacy information? Can such an idea be achieved via a real mobile application? How do mobile users perceive information privacy when using a location-based application? Do they build on this understanding of "privacy", and, if so, how does it affect their intentions to use such an application? Can mobile users' privacy concerns be moderated or reduced to some extent by changing a location-based application's characteristics? What can mobile service providers do in order to minimize mobile users' privacy concerns? Can I identify a new element in the mobile technology acceptance model, and, if so, how does this relate to privacy calculus?

Accordingly, this thesis intends to answer the main research question: *what is the user's perception of privacy issues in a mobile context through the design of an adaptive privacy management application by using context-aware technologies?* This main research question presents three main focuses as shown in the Figure 1.2: user's perception of privacy issues, mobile application and context-aware technologies. User's perception of privacy issues examines what are the user's perceived payoff when using privacy related mobile application. In this thesis, it mainly focus on user's perceived benefits and the associated risk of using a mobile application to explain user's willingness to act, as well as the determinants of user's behavioral intention to use such mobile application. Mobile application refers to the characteristics of privacy management application for mobile devices. And the context-aware technologies represent why the corresponding algorithms and solutions that could help to protect user's privacy. Each essay emphasizes on one element but linked with other two elements. Therefore, my main research question can be divided into three sub-research questions by three steps accordingly. At the first step as shown on the left of Figure 1.2, I focused on *context-aware technologies* based adaptive single sign-on (ASSO) solution to improve

authentication security for application services and ease of use of mobile user. So my first sub-research question is:

- *How can context-awareness technologies be used in a privacy management system for mobile phone devices in order to improve authentication security and maintain ease of use?*

At the second step as shown on the middle of Figure 1.2, I focused on the design and develop a context-aware *mobile application* to protect user's personal information. So my second sub-research question is:

- *How can design a context-ware mobile application that protects users' personal information by considering personalization and control?*

The third step mainly discussed on the mobile *users' perceptions of privacy issues* by using location-based application on mobile devices (as shown on the right of Figure 1.2). Thus, my third research question is:

- *How do mobile users perceive about information privacy related issues when using location-based mobile application, and what is the role of personalized services and control over personal information in such context?*

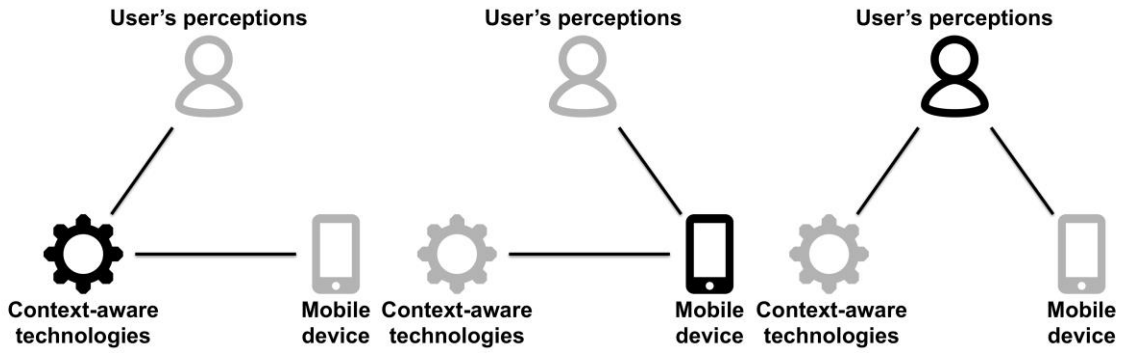


Figure 1.2. Three elements and the corresponding sub-research questions

These questions have not been considered comprehensively in existing literature relating to information systems. This thesis intends to fill the research gap.

1.3.2.2 Thesis Framework

Building on the results of the preliminary research, the research framework used in this thesis is described in Figure 1.3.

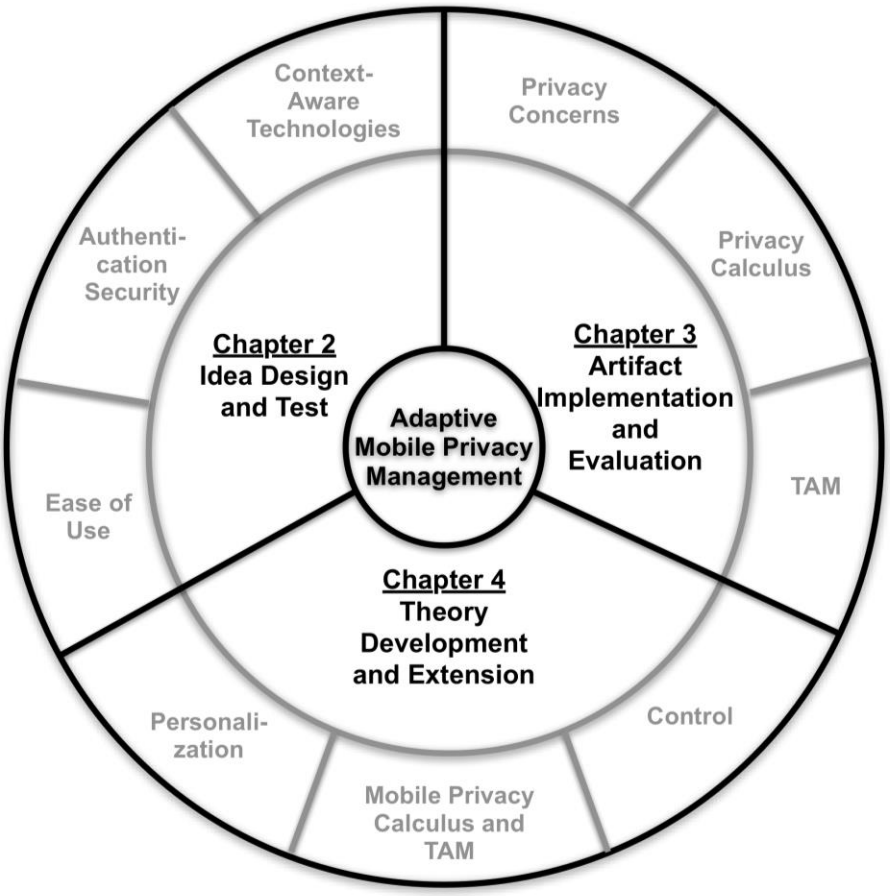


Figure 1.3. Thesis framework

As shown above, this doctoral thesis explores the question of how to achieve adaptive mobile privacy management. To do so, I first proposed an *idea* of an ASSO for mobile users, by assuming that each mobile user has a unique pattern of behavior (*Chapter 2*). This solution uses *context-awareness technologies* and is expected to increase user perception of the system's *ease of use* and the service provider's *authentication security* of the application. In particular, I assessed ways of using a context-aware mobile application to authenticate a mobile user using Personal Identifiable Information (PII). However, the existing solutions often involve a tradeoff between the system developer's efforts to implement privacy-enabling technologies (e.g., authentication security) and the cognitive effort required to use such technologies (e.g., ease of use, flexibility). I therefore proposed the use of context awareness to achieve the proper tradeoff between dynamic authentication and ease of use; I called this an ASSO. Using location and time data, I tested and proved that context is a unique user identifier, thus supporting the validity of my solution.

Based on this finding, I then implemented the ASSO solution in a mobile application called Privacy Manager, which aims to protect users' personal information on an Android operating system by using context-aware technology (*Chapter 3*). Preliminary research suggested that personalization and control play an important role in the assessments that users make of the costs and benefits associated with the disclosure of private information. Thus, I carefully implemented these two elements in the design of the artifact, allowing users to freely choose their preferred options with regard to different levels of personalization and control ability. I evaluated a number of important performance issues. In particular, I carried out several focus group interviews before using this application in order to examine whether the designed artifact would fulfill expectations regarding its appropriateness and utility. This step was also used to discover potential defects and identify new characteristics that should be included in the application. Based on feedback from the evaluation, I designed Privacy Manager. Focus group discussions were again conducted with participants who were asked to use the application for a certain period of time in order to test the utility of the designed artifact. The main objective of this application is to protect users' private information; however, at the same time, the location of users and any time information needs to be disclosed to the application in order to achieve the study's goal. In turn, this led to an increase in users' privacy concerns. This kind of privacy "dilemma" offers interesting theoretical insights in terms of users' *privacy concerns, privacy calculus* and the *TAM*.

The third article (*Chapter 4*) also adopts a user's perspective. From existing literature and the findings in my second paper, I developed a theory of mobile privacy management for users. This combines the *privacy calculus model* and the *TAM*. My theory has several theoretical implications: first, it is expected to be able to predict and explain users' privacy concerns and their intentions to disclose information. Second, it aims to provide empirical evidence for a TAM in a mobile setting. Further, both the preliminary research and second paper have shown the importance of *personalized service availability* and *users' control ability* in users' payoff. Thus, I also intend to examine the role of personalization (e.g., personalized services) and control (e.g., the ability of users to control their disclosed information) using the model, and how these two factors interact using the privacy calculus and mobile TAM.

1.4 Methodology

This thesis consists of three inter-related essays (chapters 2 to 4) in which various research methodologies have been employed, including design science, qualitative and quantitative approaches, along with different analytical techniques, such as content analysis, structural equation modeling, hierarchical multiple regression and other statistical methods. In order to maintain the logic and independence of each paper, some

of the content overlaps. A detailed description of the methods used in each paper is given in Table 1.1.

Table 1.1. Methods used in each chapter

	Method	Data	Analysis
Chapter 2	Support vector machine (SVM)	168 participants over a period of one year (collected by Lausanne Data Collection Campaign from Nokia research center Switzerland)	Quantitative (precision and recall)
Chapter 3	Design Science and focus group interview	10 participants before using application; 10 participants after using application	Qualitative (content analysis)
Chapter 4	Scenario-based survey	308 participants	Quantitative (structural equation modelling, regression analysis)

1.5 Three Essays

The rest of this doctoral thesis is organized as follows:

1.5.1 Chapter 2: Privacy-Based Adaptive Context-Aware Authentication System for Personal Mobile Devices

Chapter 2 aims to answer the first research question. It addresses an adaptive single sign-on (ASSO) solution that envisages the use of context-aware technology for mobile users. The proposed privacy-based ASSO is expected to increase mobile users' perceived ease of use of the system as well as service providers' authentication security of the application. The study was based on location and time data collected from 168 participants as part of the Lausanne Data Collection Campaign at the Nokia Research Center in Switzerland. Participants used Nokia N95 phones. According to the analysis of the SVM, the context-aware ASSO can increase the level of usability without sacrificing the level of protection offered. Moreover, this paper proposes a new instantiation of the business model pattern to a third party in charge of managing the privacy of mobile users, and third-party and mobile service providers. This new business model has privacy at the

core of its value proposition; thus, it opens up new avenues for future research into privacy and privacy practices.

1.5.2 Chapter 3: Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications

Chapter 3 explores new elements of privacy issues in the mobile context by using a design science approach. It does so in order to address the second research question. Using the *Design Science* framework put forward by Hevner et al. (2004), I introduced a new artifact in the form of a mobile application, called Privacy Manager. Its development was based on the findings given in Chapter 2, namely that context awareness can help to achieve a proper tradeoff between adaptive authentication and utility. I began by examining the relevance of the research and by reviewing existing literature on privacy to identify any problems. I then went on to look at an instantiation of a context-aware application for smartphones based on the Android operating system, where users' private information is protected. Two elements – personalization and control – were implemented in the artifact's design, because the preliminary research showed their importance in terms of user payoff. I then carried out two iterations, before and after having used this application, in order to test the application's usability. Any privacy concerns were addressed by performing several focus group interviews. The evaluations and refinements offer an interesting insight into both the theoretical and practical perspectives. The results obtained confirm the utility of the artifact and provide support for the theoretical model. Given the rapid development of mobile technologies and applications, as well as the popularity of mobile device use, there is an urgent need to understand mobile users' perceptions and acceptance. Thus, this study further discusses users' privacy concerns, privacy cost-benefit tradeoff (privacy calculus) and users' acceptance of context-aware technology with regard to Privacy Manager. The results confirm previous models but suggest new dimensions for each model. Thus, this study is an extension of existing literature in all three domains.

1.5.3 Chapter 4: The Role of Personalized Services and Control: An Empirical Evaluation of Privacy Calculus and Technology Acceptance Model in Mobile Context

Chapter 4 is an empirical study that aims to respond to the third research question. In particular, it uses a quantitative method to examine the relationship between users' perceptions about information privacy and their disclosure intentions in a mobile context. More importantly, it explores the possible impact on these relationships of users' control over the release of private information and personalized services provided by the mobile

application. The way in which personalized services and mobile users' ability to control their information affects users' valuation of an application and their intention to disclose information. They can be investigated by combining privacy calculus with a user-based TAM. Thus, in this study, I built a theoretical model that uses privacy calculus and a TAM as its basis. Later, this model incorporates personalization and control over personal information, both of which are important factors. My research was carried out using a scenario-based survey. In addition, structural equation modeling and a multiple regression analysis were employed for the analysis. Based on the analysis of 308 participants, the results strongly support the proposed framework. Furthermore, they confirm the importance of personalized services and users' control ability on the way that individuals weigh up the utility gained from disclosing personal information against the disutility of any adverse effects. This study is one of the first to attempt to examine the privacy issues in a mobile context. It suggests that some new elements (e.g., perceived enjoyment) need to be included in a mobile TAM.

1.5.4 Chapter 5: Conclusion

The final chapter concludes with limitations of the thesis, and suggestions for future research.

1.6 Contributions

Each essay offers some interesting insights. Together, they enable to build a comprehensive picture of adaptive mobile privacy management. Thus, this doctoral thesis makes a rich contribution to both the literature and privacy practice in several ways.

1.6.1 Theoretical Contribution

The principal theoretical contribution of this doctoral thesis is the presentation of the adaptive mobile privacy management model. This model was built by recognizing that context is a unique identifier. It was achieved by designing a mobile application called Privacy Manager, which uses the concept of an ASSO. Contributions to this analysis are twofold:

- Firstly, information privacy research focuses largely on explaining and predicting any theoretical contributions; however, few studies have focused on design science (Bélanger and Crossler, 2011). This thesis contributes to information research on privacy concerns by adopting a design science approach. The designed artifact,

which takes the form of a mobile application, has proved to be useful in protecting users' private information.

- Second, it builds on existing information research in the field of privacy issues by considering that privacy information, such as location and time, can be viewed as unique personal identifiable information which can be used to protect private information per se. This new understanding of privacy opens up new avenue for future research.

The second most important contribution is that this thesis serves as an initial examination of issues relating to privacy by investigating whether or not personalization and users' control ability influence privacy concerns and personal information disclosure, as well as the intention to use mobile applications. To date, little attention has been given to their interrelationships in the mobile context. Indeed, to the best of my knowledge, this thesis is one of the first attempts to fill this research gap. It seeks to do so by identifying the effects of personalized services and control ability on privacy calculus and technology acceptance attitudes. The findings, both from qualitative and quantitative data analyses, have shown the importance of these two factors.

The third central contribution is the development of a theory of mobile users' privacy concerns and behavioral intention by combining privacy calculus and an extended TAM. It provides a framework that shows the various aspects of mobile users' privacy concerns, including their intention to disclose information and intention to use mobile applications. It also shows how these aspects are interrelated. The results address two current gaps in the knowledge of privacy issues in the mobile context:

- First, this thesis provides preliminary theoretical insights and empirical evidence into the structural relationships of the antecedents that affect mobile users' intentions to use applications. Thus, it extends on the understanding of a mobile TAM. The original goal for a TAM is to explain computer usage behavior, but whether the same model would work in a mobile setting remains unknown. This thesis demonstrates that, though perceived usefulness still acts as a strongest predictor, perceived ease of use has an insignificant impact on users' intentions to use mobile applications. Instead, its role has been replaced by another element – perceived enjoyment. Thus, this thesis enriches my understanding of an individual's intention to use mobile applications.

- Second, while the bulk of previous research has examined willingness to share information and consumer disclosure behavior in either an offline setting or online setting, this paper adds empirical results from a mobile context. The findings support the premise that personal information disclosure involves a cost-benefit tradeoff analysis in the mobile privacy calculus.

1.6.2 Practical Contribution

The use of mobile devices and smartphone applications impacts on the daily life of users by facilitating relationships and interactions between individuals. However, as seen in my research, it is necessary to consider the privacy factors to provide proper services for users. Thus, this doctoral thesis provides several practical implications.

First, the integrated conceptualization of mobile privacy management allows mobile service providers to evaluate the relative importance of the different factors that affect users' disclosure and usage intentions. Practitioners are then able to identify key aspects in a particular context, allowing them to focus their attention on the corresponding features.

Second, the results for personalization offer important implications for application designers and service providers. The findings suggest that personalized services are recognized as useful features; thus, they should be continued so as to attract new users and satisfy existing users. However, the study also shows that every new personalization is likely to increase users' anxieties about the risks associated with providing personal data. Thus, application designers should pay careful attention to the tradeoff between the potential benefits that personalized services can offer to users, and any related privacy problems that may occur.

Third, it should also be noted that it is not possible to practice personalization without using mobile users' information. To this end, service providers should build a secure environment for mobile users. For example, allowing users to have greater control over their personal data will strongly reduce users' perceptions of the risks associated with using mobile applications. Marketers in this sector need to ensure such control ability for users.

Finally, this study has highlighted several opportunities for researchers and practitioners to rethink how users' context information can protect private information. With all this in mind, this thesis can be used as a first step towards an understanding that privacy is not always inversely proportionate to functionality.

1.7 References

Ackerman, M. S. 2004. "Privacy in Pervasive Environment: Next Generation Labeling Protocols," *Personal and Ubiquitous Computing*, (8), pp.430-439.

Addo, A. 2013. "The Adoption of Mobile Phone: How Has It Changed Us Socially?" *Business Management and Economics*, 1(3), pp. 47-60.

Anderson, R. 2001. "Why Information Security Is Hard: An Economic Perspective," In Proceedings 17th Annual Computer Security Applications Conference, presented at the ACSAC, New Orleans, Louisiana: IEEE, pp. 358-365.

Arbanowski, S., Ballon, P., David, K., Droegehorn, O., Eertink, H., Kellerer, W., van Kranenburg, H., Raatikainen, K., and Popescu-Zeletin, R. 2004. "I-Centric Communications: Personalization, Ambient Awareness, and Adaptability for Future Mobile Services," *IEEE Communication Magazine*, September, pp. 63-69.

Awad, N. F., and Krishnan, M. S. 2006. "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *Management Information Systems Quarterly* (30:1), pp. 13-28.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information System," *Management Information Systems Quarterly* (35:4), pp. 1017-1041.

Bonazzi, R., Liu, Z., Ganiere, S. and Pigneur, Y. 2011. "A Dynamic Privacy Manager for Compliance in Pervasive Computing," In Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, Edited by Yee. G.O.M. and Aptus Rsearch Soltions Inc., pp. 285-307.

Boritz, J. E., and No, W. G. 2011. "E-commerce and privacy: Exploring What We Know and Opportunities for Future Discovery," *Journal of Information Systems*, 25(2), pp. 11-45.

Business Insider, 2013. "BII Report: Why Mobile Commerce Is Set to Explode", available at http://www.businessinsider.com/bii-report-why-mobile-commerce-is-set-to-explode-2013-1

Chellappa, R.K, and Sin, R. 2005. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, 6(2), pp. 181-202.

Chen, X., Ma, J., Jin, J., and Fosh, P. 2013. "Information Privacy, Gender Differences, and Intrinsic Motivation in the Workplace," *International Journal of Information Management* (33), pp. 917-926.

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

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*," Management Information Systems Quarterly* (13:3), pp. 319-340.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982-1003.

Dey, A.K. 2001. "Understanding and Using Context," *Personal and Ubiquitous Computing* (5), pp. 20-24.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I, and Colautti, C. 2006. "Privacy Calculus Model in E-Commerce – A Study of Italy and the United States", *European Journal of Information System* (15), pp. 389-402.

Dinev, T. and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61-80.

Dinev, T., and Hart, P. 2007. "Privacy Concerns and Levels if Information Exchange: An Empirical Investigation of Intended e-Service use," *e-Service Journal*, (4:3), pp.25-61.

Dhillon, G.S., and Moores, T. T. 2001. "Internet Privacy: Interpreting key issues," *Information Resources Management Journal*, (14:4), pp. 33-37.

Hevner, A., March, S., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *Management Information Systems Quarterly* (28:1), pp. 75-105.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp.336-355.

Meinert, D. B., Peterson, D. K., Criswekk, J. R., and Crossland, M. D. 2006. "Privacy Policy Statements and Consumer Willingness to Provide Personal Information," *Journal of Electronic Commerce in* Organization (4:1), pp.1-17.

Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. 1995. "Values, Personal Information Privacy, and Regulatory Approaches," *Communication of ACM*, 38(12), pp. 65-74.

Miyazaki, A. D., and Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *The Journal of Consumer Affairs* (36:1), pp.28-49.

Junglas, I, and Watson, R.T. 2006. "The U-Constructs: Four Information Drives," *Communications of AIS* (17), pp.569-592.

Kaasinen, E. 2003. "User Needs for Location-Aware mobile services", *Personal and Ubiquitous Computing* (7), pp. 70-79.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B. and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior," *International Journal of Human Computer Studies* (71), pp. 1163-1173.

Kuo, F.-Y., Lin, C. S., and Hsu, M.-H. 2007. "Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices," *Journal of Business Ethics* (73), pp. 145-460.

Pallapa, G., Das, S. K., Di Francesco, M., and Aura, T. 2013. "Adaptive and Context-Aware Privacy Preservation Exploiting User Interactions in Smart Environment," *Pervasive and Mobile Computing*, n.d.

Rao, B., and Minakakis, L. 2003. "Evolution of mobile location-based services," *Communications of the ACM* (46), pp.61-65.

Sutanto, J., Palme, E., Tan, C-H., and Phang, C.W. 2013. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *Management Information Systems Quarterly* (37:4), pp. 1141-1164.

Son, J. Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and A Nomological Model," *Management Information Systems Quarterly* (32:3), pp. 503-529.

Warren, S. D., and Brandeis, D. 1890. "The Right to Privacy," *Harvard Law Review*, (4:5), pp. 193-220.

Wu, J. H., and Wang, S. C. 2005. "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model," *Information and Management* (42), pp. 719-729.

Wu, K.W., Huang, S.Y., Yen, D.C., and Popova, I. 2012. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust," *Computers in Human Behavior* (28), pp. 889-897.

Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. 2011. "The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing," *Decision support systems* (51:1), pp. 42-52.

Zhang, X., Sakaguchi, T., and Kennedy, M. 2007. "A Cross-Cultural Analysis of Privacy Notices of the Global 2000". *Journal of Information Privacy and Security*, (3:2), pp. 18-36.

Chapter 2

Privacy-Based Adaptive Context-Aware Authentication System for Personal Mobile Devices

Extended from the paper: From "security for privacy" to "privacy for security", published in the proceedings of the Third International Workshop on Business Models for Mobile Platforms
Berlin, Germany, October 4-7, 2011
Publisher: IEEE Computer Society
ISBN: 978-1-61284-319-3

Abstract Over the past decade, mobile devices such as smartphones have become increasingly common as a form of handheld computing platform. The use of mobile applications on these mobile devices is experiencing unprecedented rates of growth. However, when using mobile applications, users are often requested to give context information. Such requests have led to growing privacy concerns. This paper proposes the use of context-awareness to improve single sign-on (SSO) solutions so that mobile users can protect their private information. A privacy-based adaptive SSO (ASSO) may be able to increase users' perceived ease of use of the system and give service providers the necessary authentication security for their applications. The study was based on data gathered from 168 participants as part of the Lausanne Data Collection Campaign. This was led by the Nokia research center in Switzerland and used Nokia N95 phones. The analysis of SVM showed my expectations to be correct. Consequently, a new business model for mobile platforms has been proposed to reinforce my claim that privacy-friendly value propositions are possible and can be used to obtain a competitive advantage.

Keywords: Adaptive Single Sign-On, Authentication Security, Ease of Use, Context-Aware, Privacy, Security, Business Model

2.1 Introduction

In recent years, the penetration of smartphones has reached particularly high levels. As one of the defining technologies of our time, they have had a pervasive influence on the personal lives of individuals in many ways, including giving competence in communications and connectedness, and in terms of privacy issues, confidentiality, and individuality (Addo, 2013). On the negative side, however, the use of smartphones has created many privacy concerns, especially with regard to the context-based services that often accompany users' Personal Identifiable Information (PII). As a consequence, security problems have arisen, namely in the form of privacy protection.

Information security systems are required to protect PII and ensure users' privacy. Existing research on information security has implied that such security implies a tradeoff between the system developers' efforts to implement privacy-enabling technologies and the cognitive effort required to use such technologies. Let us consider a mobile user trying to access a set of web services, as shown in the top part of Figure 2.1. The user has to pass a set of access controls for authentication, identification, authorization, and accountability. This security procedure increases users' perceived performance of the protection application, but it negatively affects the ease of use of the system. Inglesant and Sasse (2010) have shown how low perception of ease of use can lead to a lack of user compliance with security policies. A SSO solution can increase ease of use, as shown in the middle part of Figure 2.1. Solutions such as Firefox's built-in password manager increase ease of use. However, they also reduce the amount of effort needed by attackers to access users' accounts, because only the master password has to be broken.

In order to offer stronger authentication, an SSO solution usually requires a shift from an access control list system (e.g., passwords) to a capability-based system (e.g., biometric controls or multi-factor authentication). However, this approach to security lacks flexibility, because a user's biometry cannot be changed over time. To this end, this paper aims to achieve the correct tradeoff between dynamic authentication and ease of use. I am looking for a system that can transparently authenticate a user and dynamically adapt to that user's behavior.

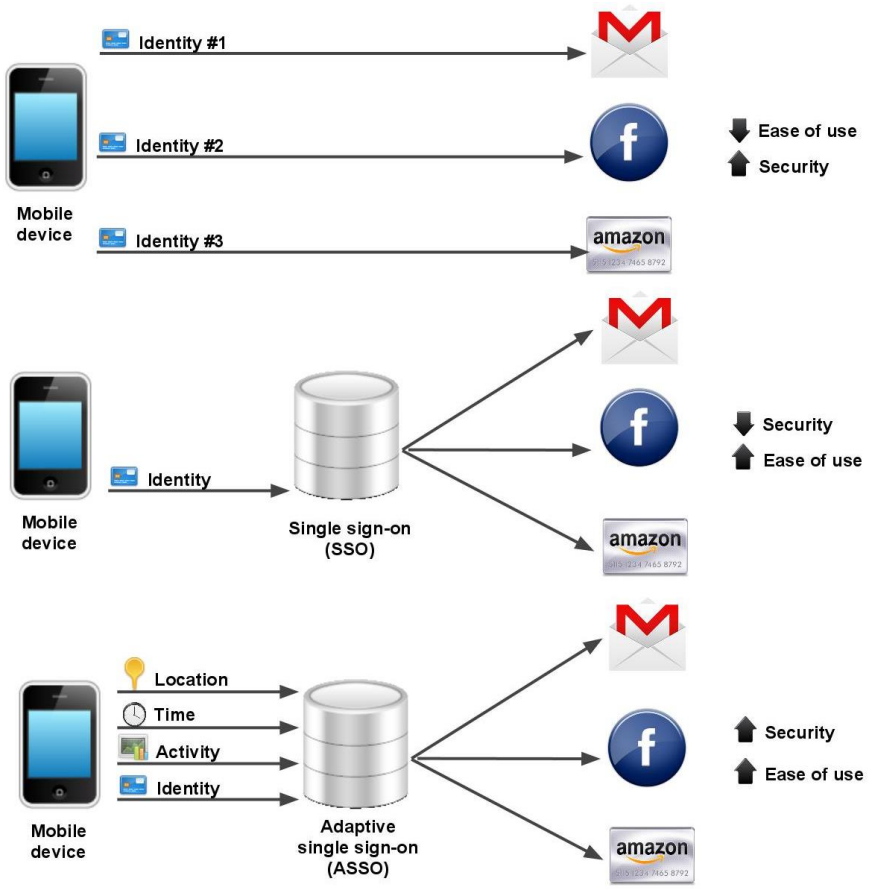


Figure 2.1. Adaptive Single Sign-On (ASSO) solution for security and ease of use

Since the early 1990s, context-aware mobile services have been of interest to scholars (e.g., de Vos et al., 2008; Dey and Abowd, 2000; Rao and Minakakis, 2003; Schilit et al., 1994). These studies have basically treated context awareness as a trigger for privacy concerns. However, this study takes a different approach. I intend to utilize users' context information to protect their private information, thereby decreasing mobile users' privacy concerns. For the purpose of this paper, I refer to context as *any information that can be used to characterize the situation of [...] a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves* (Dey and Abowd, 2000). Based on this definition, there are four types of primary context: location, identity, activity, and time. These types characterize a situation by answering where, who, what, and when, respectively. Such contextual information can help to identify users' behavior patterns, which in turn would be useful for protecting their private information. Therefore, my research question is: *how can context-awareness technologies be used in a privacy management system for mobile phone devices in order to improve authentication security and maintain ease of use?*

To answer the research question, I first examined state-of-the-art studies on context awareness and SSO solutions. I then proposed an adaptive SSO (ASSO) that utilizes context awareness to help achieve authentication and ease of use, as shown in the bottom part of Figure 2.1. A methodology was executed, together with an SVM supervised learning algorithm-based approach. The latter necessitated the collection of huge amounts of location and time data from real mobile users over the course of one year. I found that users' context information is a unique identifier, therefore verifying my proposed solution. This paper further describes the business model of an ASSO and its implications for business practitioners. The audience addressed is mainly composed of stakeholders in mobile services who seek guidelines to develop privacy-friendly business models. In this regard, minimal research has failed to successfully capture the design of business models for mobile services. This study aims to fill this research gap.

The rest of this paper is organized as follows. The section 2.2 discusses the differences between privacy and security in the extant literature. I then introduce the methods used to carry out this study, including an illustrative scenario, hypothesis development, the scope and magnitude of data collected, and the analysis applied in section 2.3. The section 2.4 discusses the findings of my research, and the 2.5 section illustrates a set of business model considerations that relate to the application of my solution. The section 2.6 lists the contributions made by this paper and the research avenues it opens up.

2.2 Literature Review

2.2.1 Privacy and Security

The concept of "privacy" is usually considered a human right; in other words, it is "the right of the individual to decide what information about himself should be communicated to others and under what condition" (Westin, 1967). Based on this understanding, Smith et al. (1996) identified four factors of online privacy: the unauthorized secondary use of personal information, improper access to personal information, the over-collection of personal information, and errors made when collecting personal information. Mobile devices can be seen as more personal than, for example, a traditional desktop computer. In particular, mobile phone users generate even more personal data, including geographic location data about the physical movement of their mobile devices (King and Jessen, 2010). However, such location information often reveals the position of a person in real time, rendering the potential intrusion of privacy a critical concern (Xu et al., 2010). Mobile devices also store additional personal information such as personal contacts, photos, messages and emails. Combined with such personally identifiable information, location information may have consequences relating to the extent of access, collection, the use or disclosure of personal identifiable information, and privacy concerns in the

form of data protection. In the current study, the privacy of personal identifiable information refers to the ability of an individual to control the way that personal identifiable information is gathered or used by an unauthorized party.

An information security system can be defined as one that offers protection against threats from potential circumstances, conditions, or events that cause economic hardship; for example, data transaction attacks and the misuse of financial and personal information (Belanger et al., 2002). According to Pennanen et al. (2006), information security consists of three main parts: confidentiality, integrity, and availability. The current study focuses on confidentiality, which refers to limitations in information access and disclosures to authorized parties, as well as the prevention of access by or disclosure to unauthorized parties.

Privacy and security concerns are not new concepts. Indeed, they have been viewed by some researchers as one construct in online purchasing for a number of years (e.g., McCole et al., 2010). While online privacy and security concerns are sometimes inextricably linked, Belanger et al. (2002) have argued that these two notions are two distinct constructs and that there is a lack of understanding about their true relationship. Security is sometimes described as a necessary tool for building privacy. In other words, privacy cannot be achieved without a good security foundation.

In context-aware applications, however, a security issue may take place without the occurrence of privacy violations. For example, some cases may lead only to a security issue because only location data is collected by an untrustworthy party. Here, users' identity information is not associated with location information; thus, there is no privacy issue. If location information is linked to users' information, however, then a privacy issue does exist.

It is important to note that privacy and security are not absolute concepts – users hold very different opinions about their level of privacy concerns. Some might not care about their privacy at all. This study assumes that mobile users are *pragmatists* (Ackerman et al., 1999) who often have specific concerns and particular tactics for addressing them. Therefore, protecting their privacy is a valuable benefit for them.

2.2.2 Context and Context-Aware Applications

In the literature, a lot of researchers have attempted to define context, and the precise nature of context-awareness. The term context-aware first appeared in a study by Schilit and Theimer (1994), who described context as locations, the identities of nearby people and objects, and the changes that occur to those objects over time. Later, Schilit et al. (1994) offered three categories: who you are, who you are with, and the objects that are

around you. Such examples of context were often used in early research into context-aware systems. Hull et al. (1997) described context as the environmental aspects of the entire current situation. Dey (1998) defined context as the emotional state of users, the focus of their attention, their location and orientation, date and time, and the objects and people in their environment. Chen and Kotz (2000, p.3) referred to context as the set of environmental states and settings that either determine an application's behavior or in which an application event occurs and is interesting to the user. These definitions are often too broad and difficult to apply in specific systems. The definitions given by Ryan et al. (1997) and Dey and Abowd (2000) are similar, and correspond withthe own beliefs. Ryan et al. (1997) claimed that context involved not only a user's location and identity information, but also his/her environment and time information. However, Dey and Abowd (2000) went on to argue that the term "environment" should be replaced with "activity". They thought that activity can answer a fundamental question of what is occurring in a particular situation, whereas environment cannot. This study followed Dey and Abowrd (2000)'s definition; thus, context characterizes users' situations by answering where, who, what, and when, respectively.

With the technological advances of today's hand-held devices, collecting context information is no longer an issue (Mizouni, et al., 2014). As a result, mobile context-awareness focuses on building applications that can take advantage of contextual information. A context-aware application must have a large and significant ability to perceive the surrounding environment. According to Biegel and Cahill (2004), a context-aware application has three main components: a set of sensors for detecting and capturing contextual information, a set of rules that governs behavior according to context, and a set of actuators for generating responses. Accordingly, my ideas on the development of context-aware applications are based on privacy protection in a mobile environment, which not only defines the sensors and actuators, but also provides the corresponding rules that drive behavior. Sensors are the sensor components fitted to mobile devices, such as GPS, Bluetooth, real-time, and WiFi. Actuators, also known as opacity tools, are privacy protection tools. They aim to protect the identity of users, and minimize the effects of revealed personal data by, for example, encrypting private information and blocking potential attacks. Rules are applied to a specific environment. From a regulatory point of view, data privacy laws are present in different business sectors and in different countries, leading to a complex multitude of overlapping and sometimes conflicting regulations that change over time. In this study, I refer to the concept of rules in order to determine which actuator should be used in a given context. As a computing platform, however, a smartphone is both pervasive and personal. The personal nature indicates two important implications. On the one hand, all the elements vary a lot in the mobile environment: users are different and they may use different services or activities at different times and in different places. On the other hand, smartphones store our most personal information, such as photos and passwords, and contain important associated

private information (i.e., clues about current location). This increases mobile users' privacy concerns. Therefore, this paper proposes to use the contextual information of mobile phone users to protect their private information.

2.2.3 Single Sign-On Solution

Traditionally, systems have used databases as their authentication mechanism. In such solutions, the users are given a login name and a password for accessing each system. With heterogeneous systems, users have to manage a set of passwords for each system and log in separately. All the passwords have to be remembered, and even worse, changed frequently, so this is hardly an ideal situation. More recently, single sign-on (SSO) technology has become more widely used for authentication solutions. As the name implies, SSO systems are designed to authenticate once, without further manual interaction; thus, users do not have to repeat the log in process for each system. Several research studies (Suriadi et al., 2009; Radha and Hitha, 2012; De Clercq, 2002) have also argued that SSO solutions reduce administrative work by resetting forgotten passwords over multiple platforms and applications, and improving on convenience, because users need only to remember a single set of credentials. Recently, new variations of SSO authentication have been developed using mobile devices as access controllers. Users' mobile devices can be used to automatically log them into multiple systems by, for example, building access control systems and computer systems through the use of authentication methods. Such methods include OpenID Connect (Sakimura et al. 2013) and SAML (Lewis and Lewis, 2009), which associates the mobile device with an access server. In general, the main advantage of designing an SSO-based system is the ability to retain ease of use whilst also providing improved user-controlled privacy capabilities.

However, SSO is not yet a universal solution. Without careful planning, implementation and verification, SSO products may introduce new security holes. For example, if an SSO account is hacked or an account password is copied, all others under that authentication will be hacked as well (Anchan and Pegah, 2003). This risk may be reduced when choosing SSO credentials that are not knowledge-based (e.g., when a classic password is used) but are biometric-based (e.g., users' unique behavior movements) or possession-based (e.g., NFC smart cards). my solution, which is intended to further reduce this risk, focuses on the use of multi-factor adaptive authentication solutions for SSO.

2.3 Methodology

In this section, I start by presenting an illustrative scenario to address gaps in the literature. I then go on to describe my theoretical model, including the constructs and hypotheses. Finally, I show how the data was collected, as well as offer a description of

the method and procedure used for data analysis.

2.3.1 An Illustrative Scenario

Figure 2.2 offers a simple scenario to present the ASSO solution.

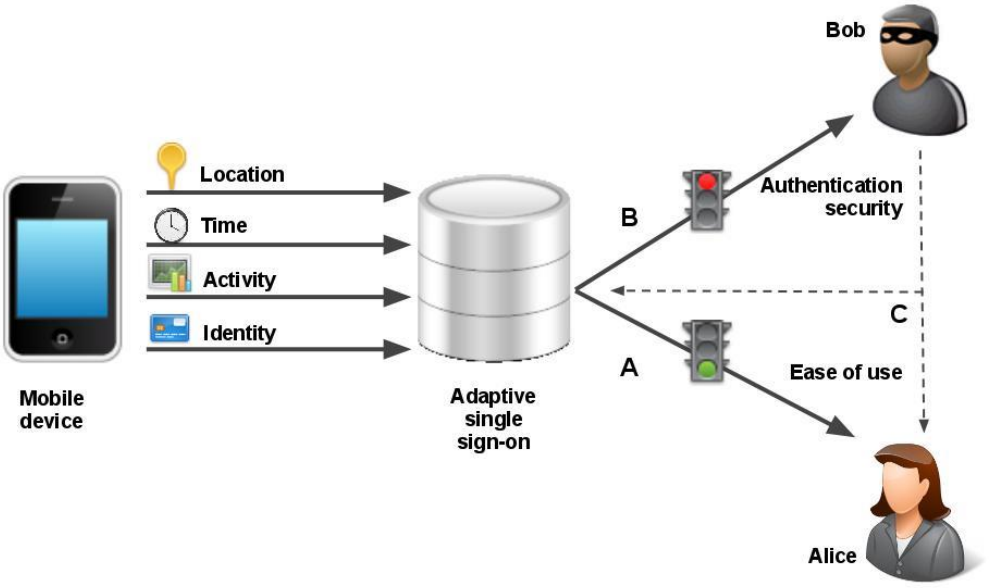


Figure 2.2. Process involved in an ASSO solution for a context-aware mobile device

A. Alice accesses her Internet accounts

The end user, Alice, has a mobile device with an application called Privacy Manager. This application uses adaptive authentication to combine real-time transaction data with Alice's behavioral profile. The real-time transaction data used to identify Alice includes her current location, speed (activity), and time. Once the data analysis application returns a positive authentication result, Alice can check her e-mail and bank accounts online through the protected channel. Thanks to Privacy Manager she can access her email and bank accounts without having to enter any passwords, as long as the data analysis returns a positive result.

B. Bob cannot access Alice's accounts

Let us assume that a thief (Bob) plans to steal Alice's mobile device to access Alice's bank account. Once Bob steals the device, the real-time transaction data does not match the data stored in Alice's profile. Suppose that Bob knows this authentication method, and tries to follow Alice before stealing the phone. Bob would note her location at any given time and collect personal information about Alice in order to copy her behavior.

However, the Privacy Manager applies state-of-the-art obfuscation techniques so that no information about the activity and the identity of Alice is disclosed. This leaves Bob with only half of the information required.

C. Alice goes on holiday

When Alice goes to another city to see a friend, Privacy Manager detects that the behavior disclosed does not match Alice's older profiles. Nevertheless, Alice possesses a trusted means of identification (e.g., a password) to provide user identification. After identification, Privacy Manager creates a new profile and stores data to include Alice's behavior on this day. When Alice comes to this city again to see her friends, her behavior data will be matched with this profile.

2.3.2 Hypothesis Development

From a cognitive point of view, usability issues arise when users cannot properly manage the information required to sign in to different web services using a large set of different pseudonyms and passwords. The possibility of capturing a change in the identity of a real user (using the features of his or her everyday life behavior) has only been considered as a threat to that user's privacy. I propose to shift from a discretionary access control approach to an attribute-based approach, where the attributes are features of the user's environment and his or her behavior in that context.

This approach assumes that each user has a unique pattern of behavior to provide a high level of control over access to mobile services whilst still maintaining a high level of usability. In previous studies, context-aware technology evoked concerns about privacy. Location-based applications track users automatically on an ongoing basis, generating an enormous amount of potentially sensitive information. From this information, the identity of the owner of the mobile device can be implicitly obtained from the analysis of its location (Beresford and Stajano, 2003; Freudiger et al., 2009). However, I see great potential in such a threat, and believe that context is a unique user identifier.

Context-based authentication is currently used for credit card fraud detection. It relies primarily on artificial intelligence techniques and uses unsupervised learning methods (Bolton and Hand, 2002). Machine learning usually refers to evolved behaviors that are based on empirical data, such as that gathered from sensor data or databases associated with artificial intelligence. The information is acquired during authentication through a learning process which authenticates the mobile user. The asserted advantages of machine learning are a level of accuracy that is comparable to that achieved by human experts. Also of benefit are considerable savings in terms of expert labor power, because no intervention from either knowledge engineers or domain experts is needed for the

construction of the classifier or for its porting to a different set of categories (Sebastiani, 2002). User data clustering can be performed on two levels: on the one hand, the best matches and the corresponding data points can be automatically or manually grouped into several clusters so that outliers can be easily detected. The alert will be activated once the number of outliers exceeds the predefined threshold. On the other hand, new trends can be found when regions on the map representing a cluster are identified and used for the classification of new data. To test my hypotheses, I propose a system that collects a set of mobile sensor data and compares them with a known set of users' profiles. Moreover, this study suggests using an escalating procedure to minimize the computational effort of the system for most authentication cases. Thus, in this study, a limited amount of phone sensor data was collected by the context-awareness component. Through machine leaning, the mobile phone can determine whether or not it is dealing with an authorized user. If the result is positive, the user is authorized to access the services (e.g., Amazon, Gmail, Facebook); otherwise, additional contextual information about the user (ranging from time and location through to activity and, eventually, identity) is collected and analyzed before access to any services is granted. Figure 2.3 presents the structural model. A rectangular element is associated with a variable that can be directly measured, whereas an oval represents a latent concept that has to be measured indirectly by summing the variables with which it is associated.

A high level of authentication security minimizes the number of occurrences in which the user is not allowed to access the system or an unauthorized person is allowed to access the system. I have already stated that location data can be used to infer much about a person, even without the user's name being attached to the data (Krumm, 2009). In this case, let us suppose that the user goes to work every day and comes back following the same routine. In this case, the system would assess the user's location at a certain frequency against the expected pattern (home-work-home). Thus, I derive my first hypothesis: the conjoint effect of time and location increases authentication security (H1).

There may be cases when the home-work-home pattern lacks sufficient variance to discriminate the user from other people. For example, someone physically close to the user could take the phone while it is unattended and access a number of services. Since the phone does not change location, unauthorized access would be possible, even if for a limited amount of time. To address this problem, the system detects when the variance among the collected data is too small, and in this case collects the user's activities (e.g., web pages visited) against known activity patterns. However, due to the complexity of the user's activity information, it is difficult to define such activity patterns. Data on the activity patterns are also difficult to obtain. For this reason, this study has only focused on the combined effect of location and time in this study.

The fourth contextual dimension (i.e., identity) is used when sensor data do not fall into

any known pattern. To update the behavioral patterns, access rights are granted to the user following proper identification (e.g., by means of a password, biometric control, or near-field communication card). This kind of identification has already been used by a large set of services; for example, banks make contact with all credit card users following an unexpected buying pattern, and Facebook asks for users to answer a secret question when they try to gain access from a foreign country. If authentication cannot be achieved by the other three dimensions of context, then identity serves as a final step to increase authentication security.

A final consideration is related to how to handle ease of use. It is believed that SVM learning techniques for the classification and eventual use of available solutions for identification would reduce the number of human-computer interactions required for authentication. This would, thus, increase perceived ease of use, and is in line with similar research currently undertaken by banks to develop mobile payment devices that do not use passwords (Sterngold, 2001). Thus, I derive my second hypothesis: the conjoint effect of time and location increases ease of use (H2).

The theoretical model is shown in Figure 2.3.

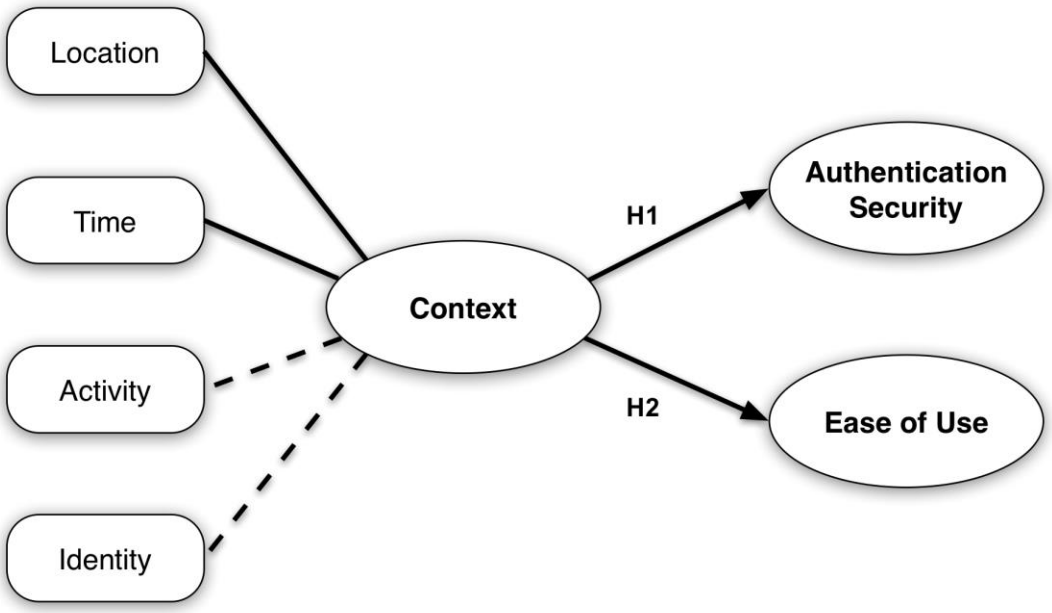


Figure 2.3. Theoretical Model

2.3.3 Data Collection and Participants

Users' behavioral data were collected using the Nokia Smartphone N95 and a heterogeneous sample of 168 participants from Lausanne – a second-tier city in Switzerland – over the course of one year. Data collection was carried out as part of the Lausanne Data Collection Campaign (LDCC). Specific data collection mobile software was used. This runs in the background of mobile phones in real time and in a non-intrusive manner, which means that no actions are dependent on the mobile phone itself. This specific software was aimed at making data collection invisible to the participants whilst, at the same time, optimizing the ratio between data collected and power consumed. The mobile application was designed to meet the operating times of one full day, thus enabling participants to use their devices normally during the day and charge the batteries over the night. The objective was to disclose rich and comprehensive data from each individual participant. All collected data was then stored to the mobile device and automatically uploaded to the SQL database server that handles the data when the device detects a known WLAN access point, as well as during the battery charging process.

Four categories of data were collected: (1) social interaction data, such as call logs, short message logs and Bluetooth scanning results; (2) location data, including data from GPS, cellular network information, and WLAN access point information; (3) media creation and usage data containing information on the locations where images have been captured, video shot or music played; and (4) behavioral data, such as application usage, activity detection based on acceleration sensor, and regular device usage statistics based on call and short message logs. This study focuses on the location and the corresponding time data in the quantitative research.

Our sample included 168 participants, of which 65% were males and 35% females. The majority of participants were young people aged between 22 to 33 years old. They included a heterogeneous set of real-life social networks with individuals from mixed backgrounds. According to statistical results from LDCC, 63.1% of participants were employed, 8% were not presently employed, 26% were students, and 3% were categorized as 'other'. Moreover, all the participants mentioned that they had prior experience of using a mobile phone and 97% of the sample saw themselves as active Internet users. Table 2.1 represents the demographic data for the participants.

Table 2.1. Demographics

		Number	Percentage
Gender	Male	109	64.9%
	Female	59	35.1%
Age	>50	4	2.4%
	44-50	2	1.2%
	39-44	12	7.1%
	34-38	29	17.3%
	28-33	44	26.2%
	22-27	58	34.5%
	16-27	12	7.1%
	<16	2	1.2%
Occupation	Yes	106	63.1%
	No	13	7.7%
	Student	44	26.2%
	Other	5	3.0%
Active Internet user	Yes	163	97.0%
	No	5	3.0%

The participants were asked to use the experimental phone as their primary phone during the course of the study. They were encouraged to stay in the campaign area for twelve months. Considering that a huge amount of sensitive personal data would be collected from each participant, and stored in the secure databases, the raising of privacy concerns became more important. Some privacy policies were applied to the experimental study to protect the participants' personal information. In addition, participants could always access the data records collected and delete part or all of their data. They could also view social patterns inherent to their behaviors using an online visualization tool.

2.3.4 Classification Algorithm

Our classification algorithm was designed and developed by using SVM with a predict function. SVMs are supervised learning models that have associated learning algorithms to analyze data and recognize patterns. They are widely used for classification and regression analysis (Cortes and Vapnik, 1995). SVM can maximize the margin between two classes, and use non-linear transformations to separate non-linearly separable objects (Vladimir and Vapnik, 1995). With the help of an appropriate non-linear kernel function, the algorithm also allows the maximum-margin hyperplane to be fitted into a transformed feature space.

I measured the quality of classifications resulting from an SVM by using the notions of precision and recall. According to the definition of Lingras and Butz (2007), in a classification task precision measures the percentage of objects that are correctly classified as "true" as a ratio of all the objects that should really be "true". Recall describes the proportion of objects that should be classified as "true" and are in fact classified as "true".

Precision and recall are complementary measures that are commonly used to promote information retrieval system effectiveness. Both precision and recall are based on an understanding and measure of relevance for information retrieval theorists and practitioners. As shown in formula (1), precision is calculated as the number of relevant items retrieved by an information system (i.e., true positives) divided by the total number retrieved (i.e., the sum of true positives and false positives).

$$Precision = \frac{True\ positives}{True\ positives + False\ positives} \qquad (1)$$

As shown in formula (2), recall is calculated as the number of relevant items retrieved divided by the total number of relevant items available (i.e., the sum of true positives and false negatives). According to Pevzner and Marti (2002), precision can be interpreted as the percentage of boundaries identified by an algorithm that are indeed true boundaries, whilst recall can be interpreted as the percentage of true boundaries that are identified by the algorithm. Thus, I computed precision to test authentication (H1) and recall to test ease of use (H2).

$$Recall = \frac{True\ positives}{True\ positives + False\ negatives} \qquad (2)$$

True positive and false negatives in the formula can be explained by the following example. Consider the scenario of Alice and Bob I discussed above, in which it was important to determine whether the mobile phone is being used by the mobile's owner Alice. Suppose that in Figure 2.4, in the training mode, all data are marked with different shapes: the shape of each point is its class (the triangle represents Alice and the circle represents Bob) and the location and time are its data. The SVM can help split these points with a non-linear line, of which the left side is predicted as being Alice (i.e., positive) and the right as Bob (i.e., negative) when new data is received. Cases where the user is Alice are labeled as true; however, when the real user is Bob, they are labeled as false. Therefore, I have the four following scenarios as illustrated in Figure 2.4.

- **True positive:** when the data comes into the left class and the user is Alice;
- **False positive:** when the data comes into the left class and the user is Bob;
- **True negative:** when the data comes into the right class and the user is Bob;
- **False negative:** when the data comes into the right class and the user is Alice.

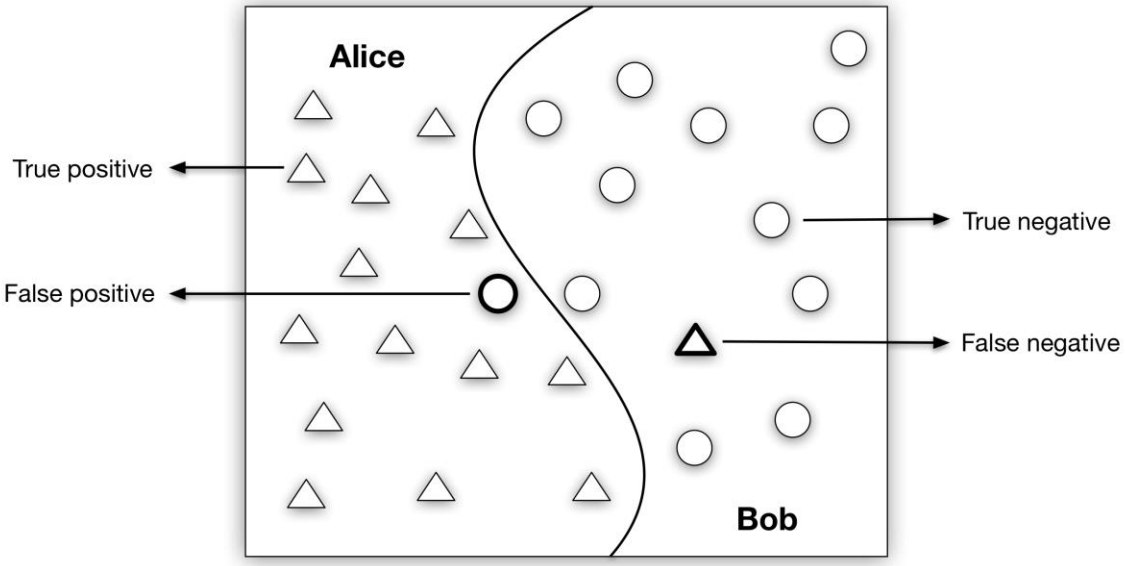


Figure 2.4. An example of classification with four cases

To acquire a user's location and time data from the central Nokia databases server, I sent SQL queries over a secure HTTPS prototype. However, this required to store a large amount of data because the results contain all users' location and time information during one year. In order to reduce both the implementation complexity and meet the storage requirements, I requested the information with individual context and stored each user's data in a single CSV file. Thus, I collected 168 users' location and time data into 168 CSV files. I then built the algorithm based on these data files. The script below describes the core of functions and execution process used to obtain the results.

Algorithm: Classification based system's security authentication and ease of use

```
1  foreach user's data u1 in u168 do
2        Divide the first user dataset into a train and a test set:
3        idxtrain_u1<-1:round(nrow(all)/10)
4        idxtest_u1<-(round(nrow(all)/10)+1):nrow(all)
5        trainSet_u1<-all[idxtrain_u1,]
6        testSet_u1<-all[idxtest_u1,]
7        Divide the second user (first compare user) dataset into a train and a test set
```

```
8       if u1 != u2 Then
9               idxtrain_u2<-1:round(nrow(all)/10)
10              idxtest_u2<-(round(nrow(all)/10)+1):nrow(all)
11              trainSet_u2<-all[idxtrain_u1,]
12              testSet_u2<-all[idxtest_u1,]
13      end if
14      else go to next user
15      Combine two users' data frame by rows
16      train<-rbind(trainSet_u1, trainSet_u2)
17      test<-rbind(testSet_u1, testSet_u2)
18      trainDataCall<-subset(train,select=c(-X,-Class))
19      trainClassCall<-subset(train,select=Class)
20      testDataCall<-subset(test,select=c(-X,-Class))
21      testClassCall<-subset(test,select=Class)
22      Running the model again using the train set and predicts classes using the test set in
        order to verify if the model has good generalization.
23      model <- svm(trainDataCall, trainClassCall, type='C',kernel='radial')
24      pred <- predict(model, testDataCall)
25      A cross-tabulation of the true versus the predicted values yields (the confusion matrix):
26      Tab<-table(pred,t(testclasscall))
27  end foreach
```

I included four main steps in my algorithm. The first step was to divide the user and compare user data in the training dataset and test dataset. In the experiments of this study, the data collection lasted for one year; thus, I decided to use one month's user data as a training dataset. The second step presented a combination of two users' training and test datasets. In the third step, I used an SVM to create a non-linear classification model. Moreover, the predict function predicts values based on a model trained by the SVM, and returns a vector of predicted labels. In the last step, a cross-tabulation was built to produce the confusion matrix type, which contains the values of true positive, false positive, true negative, and false negative. In order to reduce the algorithm execution time, I used four computers with quad-core processors to calculate in parallel, simultaneously. It took a total of 12 hours to obtain the complete results.

2.4 Results

The resulting precision and recall are shown in Figure 2.5 and Figure 2.6 respectively. These two figures show the frequencies of precision and recall with an interval of 2.5%. I have excluded the ranges that are less than 50% because all results exceed that percentage. The average of precision and recall are indicated as a broken line. As can be seen, the majority of the precision values are between 80% and 100%, with an average of 88.4%.

This implies that from among the 100 positive values that were returned from the application, 89 cases were actually the truth (i.e., they correctly identify the real mobile holder). However, on 11 occasions the mobile user was not the real mobile holder. Similarly, most of the recall values were located between 80% and 100%, with an average of 87.7%. Thus, for every 88 true positive values (i.e., correctly identify the real mobile holder), there were 12 false negative values (i.e., fail to identify the real mobile holder). The results suggest that a high level of authentication and ease of use can be achieved. Thus, both H1 and H2 are supported.

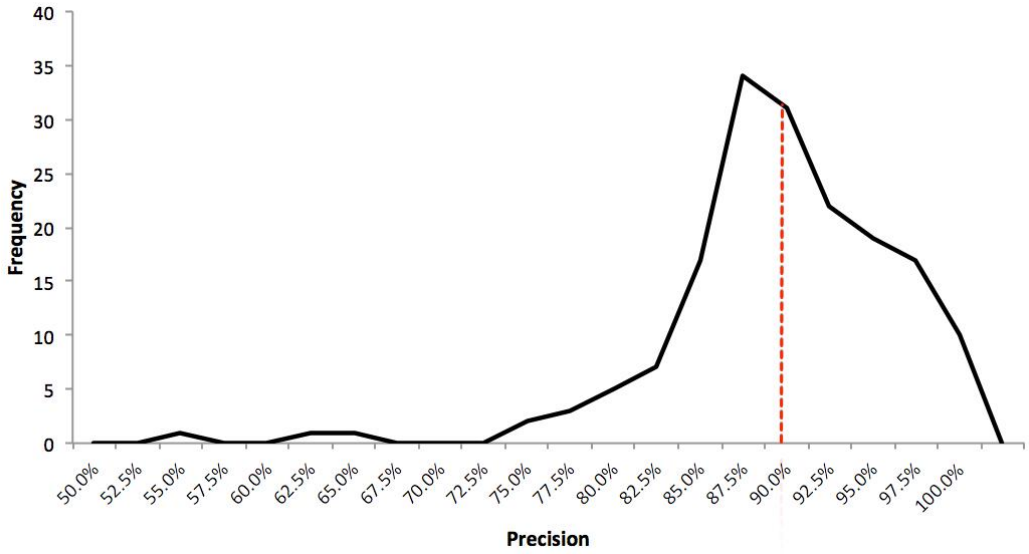


Figure 2.5. Frequency distribution of relative precision for authentication security

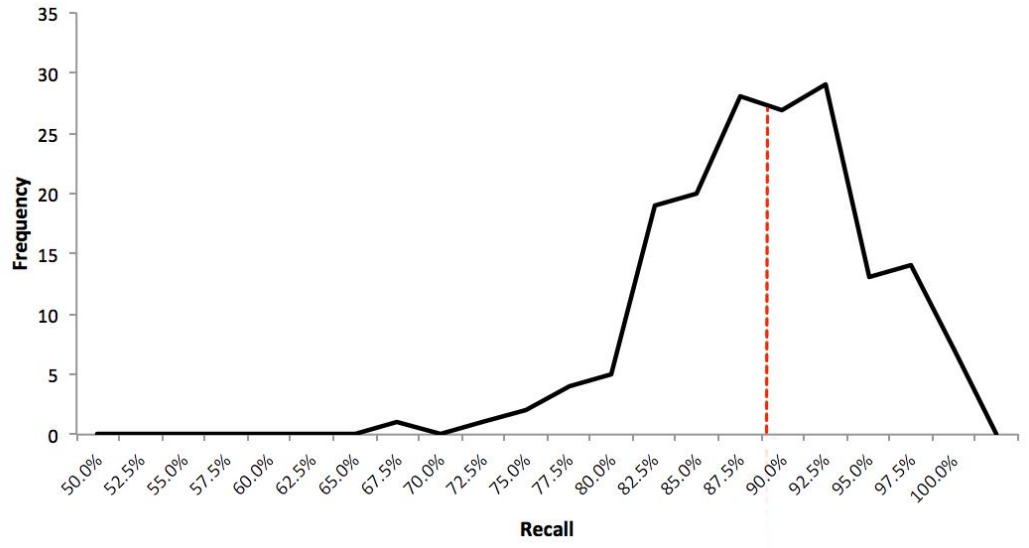


Figure 2.6. Frequency distribution of relative recall for ease of use

2.5 Business Model Discussion

The digital economy has provided firms with the potential to experiment with novel value creation mechanisms (Zott et al., 2011). Such mechanisms are networked in the sense that they delineate their roles and the economic agents that participate in value creation. In explaining the value chain, the concept of the business model is usually involved. A business model is "*a conceptual tool that contains a set of elements and their relationships and allows expressing a company's logic of earning money. It is a description of the value a company offers to one or several segments of customers and the architecture of the firm and its network of partners for creating, marketing and delivering this value and relationship capital, in order to generate profitable and sustainable revenue streams"* (Osterwalder, 2004, p.15). Therefore, a business model is related to a number of other managerial concepts: it is not just a company's economic model, but also includes operational elements, strategy elements, as well as other key parties in the value chain.

A considerable amount of research about business models has been conducted and reported within the various domains, including business, information systems and strategy. Over the past decade, this is especially true with the growing popularity of digital technologies such as the Internet. More recently, mobile devices have challenged many traditional sectors; consequently, there has been increasing interest in the field of e-business (e.g., Amit and Zott, 2001; Osterwalder and Pigneur, 2002; 2003), context-aware mobiles (e.g., Al-Qirim, 2012; Reuver and Haaker, 2009), mobile service delivery platforms (e.g., Becker et al., 2012) and so on.

Despite such rising interest, academics still fail to agree on exactly what constitutes a business model (Morris et al., 2005; Zott et al., 2011). Many researchers have focused on the business model components that are needed to achieve specific goals. However, there are a few basic components that do emerge in a business model. Based on some key questions that a business model has to address, Osterwalder and Pigneur (2002) identified four basic elements: product innovation (what a company has to offer), customer relationships (a company's target customers), infrastructure management (how the proposition can be realized), and financials (the revenue model). Morris et al. (2005) identified six components, drawing upon the business model literature: factors related to the offering, market factors, internal capability factors, competitive strategy factors, economic factors and growth/exit factors. In a more recent and relevant study, Reuver and Haaker (2009) summarized four key issues in the business model design of context-aware mobile services, namely service domain (i.e., targeting), technology domain (i.e., security), organizational domain (i.e., network openness) and financial domain (i.e., pricing).

To enable business people to easily understand the nature of their business and the essential elements of which it is composed, I used a framework that was proposed by Osterwalder and Pigneur (2009). In this framework, value creation is at the core. The business model canvas can be described by looking at a set of nine building blocks. These blocks were derived from an in-depth literature review of a large number of previous conceptualizations of business models. The framework can serve as a good strategic management and entrepreneurial tool, allowing to test the business model upfront.

This section discusses the business model pattern for a third party in charge of managing the privacy of mobile users and mobile service providers. The following paragraphs use the nine business model elements defined by Business Model Ontology (BMO) to assess the strategic contribution of the ASSO solution for context-aware mobile devices, as shown in Figure 2.7.

Value proposition: This lies at the center of the business model. It describes which customer problems are solved and why the offer is more valuable than similar products or services from competitors.The context-aware ASSO solution helps to *protect customers' privacy* without sacrificing the level of protection offered. According to Nokia's survey (2009), which was drawn from 14 countries and 9,200 mobile phone and Internet users, 82% of respondents viewed privacy as an important topic, whilst more than three quarters of people were concerned about privacy violations. The solution in this study offers value to customers, allowing them to implement privacy in their application, thus reducing their concerns. A second set of values can be drawn from the two performance criteria: *authentication security* and *ease of use*. On the one hand, a mobile device can authenticate the mobile user through an accurate learning process that has no other costs. Therefore, security authentication is associated with service providers as a main value proposition in the privacy-friendly business model pattern. On the other hand, based on user data analysis associated with the mobile user, ease of use helps manage a privacy profile in one location for multiple services and helps reduce the loss of control that is felt by users when they need a different profile for each service.

Customer segments: In the BMO, customers are analyzed and separated into groups to help identify their needs, desires, and ambitions (e.g., singles, families). In my pattern, there are two distinct customer segments: the *mobile user who seeks ease of use* and the *service provider who seeks authentication security*. Since the solution can benefit both mobile users and service providers, my business model pattern is similar to an infomediary between two customer segments.

Customer relationship: This specifies the type of relationship expected by the customer and describes the way it is established and maintained (e.g., promotion, support, individual, or en masse). The key to attracting users is to promote the importance of

privacy protection and to build a strong *trust relationship* with the customer. In this study, it is defined trust as a willingness to rely on an exchange partner in whom one has confidence (Moorman et al., 1992). A trust relationship may be built on physical, social, economic, or emotional characteristics. The privacy agent has to demonstrate an awareness of the high value a user has for personal data; it must also show that it cares a great deal for keeping data safe. This relationship is very similar to that of a bank and its customers.

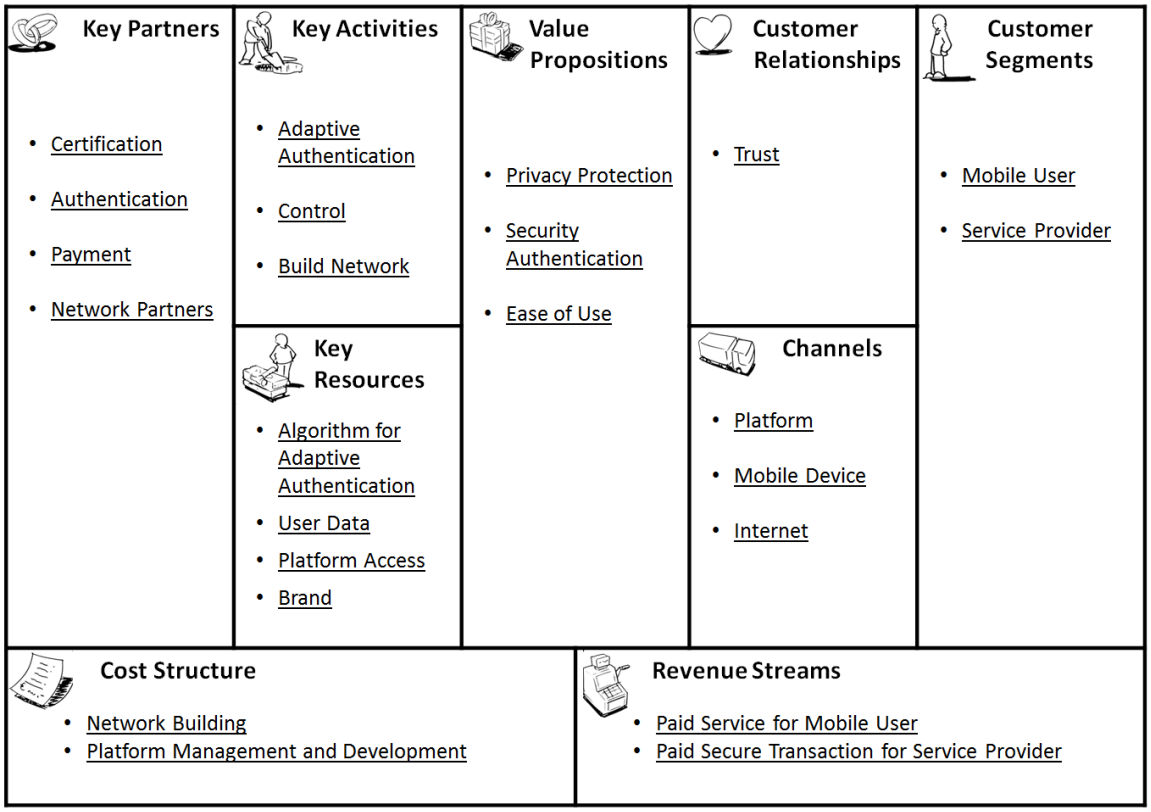


Figure 2.7. Business models for the adaptive single sign on (ASSO) solution

Channel: This illustrates how the customer wants to be reached and by whom the customer is addressed (e.g., the Internet, a store). Service can be personalized either by means of a *platform*, which could be either a *mobile application* or the *Internet*. The ASSO application is based on the mobile device for an end user. Authentication technology would be provided in the form of a service that offers an Application Programming Interface (API) or an application made with a Software Sevelopment Kit (SDK).

Key activities: These are used to transform all resources into the final product or service (i.e., through development, production, proprietary process). The key activity of a multi-

sided business model is to build and promote a *network* of users for its platform. To ensure compliance with the users' policies, the privacy risk can be mitigated by implementing and maintaining a set of *controls* according to security frameworks such as CobiT and ISO 270001, together with privacy guidelines (Nokia's survey, 2009) Moreover, I have introduced the important concept of *adaptive authentication*, which implies unsupervised rule generation. The user can be authenticated by identifying of the user's behavior pattern through machine learning, but if the context-based authentication fails, an adaptive authentication is required.

Key resources: Staff, machines, and proprietary knowledge are required to deliver the value proposition. The most important element for the third party is *user data* and control over access to the *data-sharing platform*. An additional resource is represented by the *brand value*, which allows a trusted relationship with the customer segments. Furthermore, the *algorithm for adaptive authentication* is added as a key resource.

Key Partners: For resources or activities, most businesses depend on an *external partner network* (e.g., logistics, financial), which can offer better quality or a lower price on non-essential components. In order to guarantee the trustworthiness and security of the solution and to be able to certify that the application made for this platform is compliant, I had to gain *certification* by an external provider. The third party also had to develop partnerships with a mobile device manufacturer or network operators in order to realize and deploy the product. To offer additional services, my solution also needed to develop a relationship with a mobile user and a service provider.

Revenue streams: These reflect the value that customers are willing to pay and the way in which they will perform the transaction. In my pattern, two revenue streams associated with the two selected customer segments were switched: thus, the end user pays a *fee to use the application*, and the service provider pays a *fee for each secure transaction* (alternatively, it could buy a license to develop a set of ASSO applications).

Cost structure: This comes under the heading of financial information and should be aligned to the core ideas of the business model. *Network building*, *platform management* and *development activities* are all costly services.

2.6 Implications and Contributions

This research offers several theoretical contributions, as well as practical implications. First, I present an improved solution for SSO using the attributes of mobile users; in other words, contextual information. The findings reveal that the conjoint effect of location and time information would increase authentication, whilst retaining a high level of ease of use. In other words, the ASSO solution increases the level of usability in terms of

protecting users' privacy without sacrificing the level of protection on offer. To the best of my knowledge, the study is the first to offer empirical evidence that users' context information can be used to protect their private information. Hence, it opens up new understanding about the current literature in this domain.

Second, whilst I am aware that context is about much more than just location, its other elements are still difficult to identify or measure. As a result, most existing studies only focus on location information or location-based features. This study extends the context concept by combining location and time information. I have utilized real mobile users' data to prove that context data is a unique identifier, thus opening up a new avenue for future research on mobile context-awareness.

Third, this paper proposes a new instantiation of the business model pattern that has valuable implications for practitioners. The new model has privacy at the core of its value proposition, whereas previous instantiations considered privacy as a complementary service to be aggregated with other value propositions. Thus, I present new ways to use privacy as a key component of mobile business models.

Finally, the results of this study also have important implications for managerial practices. The findings suggested a radically approach to reignite the growth and innovation capabilities of their enterprises. In most studies, users' privacy issues that rise in context-aware services are usually considered as a burden. However, the ASSO solution made the privacy as a new value proposition in the core of the BMO. On one hand, it will help to build a strong trust relationship with the customer, and this strong trust relationship will increase the revenue. On the other hand, this value proposition increases the key activities construction, but also increases the cost to build these activities. As a result, the revenue increases the profit, and the cost reduces the profit at the same time. Moreover, my research focused on the new instantiation of the business model pattern which would be of great interest and value in understanding the role of intention of management and customer needs in the context of mobile privacy issues. The proposed suggestions highlighted the objectives such as enterprise's vision, core competencies, strategies, infrastructure, organizational structures, trading principles, as well as operational processes and policies.

2.7 Conclusion

This paper proposed an ASSO for mobile users to protect their private information by using their contextual information. The contextual data for 168 real mobile users was collected by the Nokia Research Center in Switzerland over the course of one year. My findings revealed that context, which was measured by combining time and location

information, could be viewed as a unique identifier. In previous studies, context-aware technology has evoked concerns about privacy. As location-based applications track users automatically on an ongoing basis, it generates an enormous amount of potentially sensitive information about the owner of the mobile device. However, my solution has proved its great potential in terms of this kind of "threat". Indeed, I have demonstrated that it can increase authentication at a high level of ease of use, therefore suggesting important implications for business practitioners. The new instantiation of the business model pattern that was proposed by Osterwalder and Pigneur (2009) is presented in this thesis, together with a discussion of the nine building blocks for the third party in charge of managing the privacy of mobile users and mobile service providers. The new model has the protection of privacy at its core. It also has two performance criteria (i.e., authentication security and ease of use), which make it different from most previous instantiations. In these, privacy was considered a complementary service.

In the current stage of project development, I acknowledge a set of limitations. The first one concerns the choice of the approach to represent the business model. It should be acknowledged that alternative business model frameworks exist, such as that put forward by Bouwman et al. (2008) and Wegmann (2003). These frameworks may be more geared to the mobile context since they can use the mobile device or ICT service as a unit of analysis. I also acknowledge that IBM and Vodafone are currently developing a software solution that is similar to the one proposed here. However, since their solutions are proprietary, I could not include information about their performance.

As future extensions of the solution, I intend to use context-aware technology to implement the ASSO in a mobile application to protect users' personal information on the Android operating system. I bring to mind the mobile device versus central server debate presented in existing research (Liu et al., 2011). Thus, it would be interesting to explore two what-if scenarios that arise when one of the two agents takes the lead.

(1) What if the ASSO is owned by services providers in a situation of coopetition? In this case, the application would mostly reside in the central servers of service providers. These providers would use an ASSO API to develop new applications or they would define an ASSO standard. The mobile user would use a client application on the mobile device that would send the context information needed to obtain authentication. This approach would increase the performance of the authentication algorithm, which could take advantage of the central server's power. It could also decrease learning time by having access to a larger pool of users' data. Moreover, the updating of a client's application would be easier to perform and users' data could reside on the server, so as not to leave any private information on the mobile device in case of malicious attack.

(2) What if a device-centric authentication is preferred to an ASSO platform? In this case, the ASSO would mostly reside on the users' mobile devices. The authenticating algorithm would be stored within a mobile application that would establish a secure connection with the service provider after user authentication. This approach would address privacy concerns that might arise under the centralized solution, because in this case users' data are not stored on the server. Additionally, this approach may act as less of a drain on battery power, because the increased computational effort would be compensated for by the reduction of client-server data exchanges required in the first scenario. In a possible extension of this scenario, users could authenticate each other without the need for a third party. This solution would spread users' data among peers, thus reducing the success of malicious attacks (Pathak and Iftode, 2006).

2.8 References

Ackerman, M., Darrell, T., and Weitzner, D. J. 2001. "Privacy in Context," *Human-Computer Interaction* (16), pp. 167-176.

Addo, A. 2013. "The Adoption of Mobile Phone: How Has It Changed Us Socially?" *Business Management and Economics* (1:3), pp. 47-60.

Al-Qirim, N. 2012. "Context-Aware Mobile Business Model Discovery," *Procedia Computer Science* (10), pp. 1180-1187.

Amit, R., and Zott, C. 2001. "Value Creation in E-Business," *Strategic Management Journal* (22), pp. 493-520.

Anchan, D., and Pegah, M. 2003. "Regaining Single Sign-On Taming the Beast," in Proceedings of the 31st annual ACM SIGUCCS conference on User services. San Antonio, TX, USA, pp. 166-171.

Becker, A., Mladenow. A, Kryvinska, N., and Strauss, C. 2012. "Evolving Taxonomy of Business Models for Mobile Service Delivery Platform," *Procedia Computer Science* (10), pp. 650-657.

Belanger, F. Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11), pp. 245-270.

Beresford A. R., and Stajano, F. 2003. "Location Privacy in Pervasive Computing," *Pervasive Computing* (2:1), IEEE, pp. 46-55.

Biegel, G., and Cahill, V. 2004. "A Framework for Developing Mobile, Context-Aware Applications," In Proc. of the 2nd IEEE Conference on Pervasive Computing and Communications, Percom 2004, pp. 361-365.

Bolton, R. J., and Hand, D. J. 2002. "Statistical Fraud Detection: A Review," *Statistical Science* (17:3), pp. 235-249.

Bouwman, H., Zheng, J. M., Duin, P. V. D., and Limonard, S. 2008. "A Business Model for IPTV Service: A Dynamic Framework," *Info* (10:3), pp. 22-38.

Chen, G., and Kotz, D. 2000. "A Survey of Context-Aware Mobile Computing Research," Technical Report. Dartmouth College, Hanover, NH, USA.

Cortes, C., and Vapnik., V. 1995. "Support-Vector Network," *Machine Learning* (20), pp. 273-297.

De Clercq, J. 2002. “Single Sign-On Architectures”, Infrastructure Security, International Conference, InfraSec 2002, Bristol, UK, Springer-Verlag, pp. 40-58.

De Vos, H., Haaker, T., Teerling, M., and Kleijnen, M. 2008. “Consumer Value of Context Aware and Location based Mobile Services,” in Bled 2008 Proceedings, Austria, pp. 50-62.

Dey, A. K. 1998. “Context-Aware Computing: The CyberDesk Project,” AAAI 1998 Spring Symposium on Intelligent Environments, Technical Report SS-98-02, pp. 51-54.

Dey, A. K. Abowd, G. D. 2000. “Towards a Better Understanding of Context and Context-Awareness,” CHI 2000 Workshop on the What, Who, Where, When, and How of Context-Awareness, pp. 304-307.

Freudiger, J., Manshaei, M., Hubaux, J. P., and Parkes, D. C. 2009. “On Non-Cooperative location privacy: A Game-Theoretic analysis,” in Proceedings of the 16th ACM conference on Computer and communications security, New York, USA, pp. 84-98.

Hull, R., Neaves, P., Bedford-Roberts, J. 1997. “Towards Situated Computing,” 1st International Symposium on Wearable Computers, pp. 146-153.

Inglesant, P. G., and Sasse, M. A. 2010. “The True Cost of Unusable Password Policies: Password Use in the Wild,” in Proceedings of the 28th International Conference on Human Factors in Computing Systems, New York, USA, pp. 383-392.

King, N. J., Jessen, P. W. 2010. “Profiling the Mobile Customer – Privacy Concerns when Behavioral Advertisers Target Mobile Phones – Part1,” *Computer Law and Security Review* (26), pp. 455-478.

Krumm, J. 2009. “A Survey of Computational Location Privacy,” *Personal and Ubiquitous Computing* (13:6), pp. 391-399.

Lewis, K. D., and Lewis, J. E. 2009. “Web Single Sign-On Authentication using SAML,” *International Journal of Computer Science Issues* (2), pp. 41-48.

Lingras, P., and Butz, C. 2007. “Precision and Recall in Rough Support Vector Machines,” in Proceedings of the international conference on granular computing, pp. 654-658.

Liu, Z., Bonazzi, R., Fritscher, B., and Pigneur, Y. 2011. “Privacy-Friendly Business Models for Location-Based Mobile Services,” *Journal of Theoretical and Applied Electronic Commerce Research* (6:2), pp.90-107.

McCole, R. Ramsey, E., and Williams, J. 2010. “Trust Considerations on Attitudes towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns,” *Journal of Business Research* (62), pp. 1018-1024.

Mizouni, R., Abu Matar, M., Al Mahmoud, Z., Alzahmi, S. Salah, A. 2014. "A Framework for Context-Aware Self-Adaptive Mobile Applications SPL," *Expert Systems with Applications* (41:16), pp. 7549-7564.

Moorman, C., Zaltman, G., and Deshpande, R. 1992. "Relationships between Providers and Users of Market Research: The Dynamics of Trust within and between Organizations," *Journal of marketing research* (29:3), pp. 314-328.

Morris, M., Schindehutte, M., and Allen, J. 2005. "The Entrepreneur's Business Model: Toward A Unified Perspective," *Journal of Business Research* (58), pp. 726-735.

"Nokia Siemens Networks: Privacy Survey 2009," Available at http://nsn.com/system/files/document/SDM_PrivacyStudy_Brochure.pdf

Osterwalder, A. 2004. "The Business Model Ontology - A Proposition in A Design Science Approach," Dissertation, University of Lausanne, Switzerland.

Osterwalder, A., and Pigneur, Y. 2002. "An e-Business Model Ontology for Mobile E-Business," the 15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy, Bled, Slovenia.

Osterwalder, A., and Pigneur, Y. 2003. "Modeling Value Proposition in E-Business," in Proceeding of the 5th International Conference on Electronic Commerce, pp. 429-436.

Osterwalder, A., and Pigneur, Y. 2009. "Business Model Generation: A Hand book for Visionaries, Game Changers, and Challengers," New York, USA: Wiley.

Pathak, V., and Iftode, L. 2006. "Byzantine Fault Tolerant Public Key Authentication in Peer-to-Peer Systems," *Computer Networks* (50:4), pp. 579-596.

Pennanen, K., Kaapu, T., and Paakki, M-K. 2006. "Trust, Risk, Privacy, and Security in E-Commerce," Proceedings of the ICEB + eBRF Conference, Tampere, Finland.

Pevzner, L., and Marti A. H. 2002. "A Critique and Improvement of An Evaluation Metric for Text Segmentation," *Computational Linguistics* (28:1), pp. 19-36.

Radha,V., and Reddy Hitha, D. 2012. "A Survey on Single Sign-on Techniques," *Procedia Technology* (4), pp. 134-139.

Rao, B., and Minakakis, L. 2003. "Evolution of Mobile Location-based Services," *Communications of the ACM* (46:12), pp. 61-65.

Reuver, M., and Haaker, T. 2009. "Designing Viable Business Models for Context-Aware Mobile Sevices," *Telematics and Informatics* (26:3), pp. 240-248.

Ryan, N., Pascoe, J., Morse, D. 1997. "Enhanced Reality Fieldwork: the Context-Aware Archaeological Assistant," Gaffney,V., van Leusen, M., Exxon, S. (eds.), *Computer Applications in Archaeology*, Oxford.

Sakimura, N., Identity, P., Jones, M., De Medeiros, B., and Mortimore, C. 2013. "OpenID Connect Basic Client Profile 1.0 draft 28", OpenID Connect Specs. Available at http://openid.net/specs/openid-connect-basic-1_0-28.html

Schilit, B., Adams, N., and Want, R. 1994. "Context-aware Computing Applications," in First workshop of Mobile Computing Systems and Applications, Santa Cruz, California, USA, pp. 85-90.

Schilit, B., Theimer, M. 1994. "Disseminating Active Map Information to Mobile Hosts," *IEEE Network* (8:5), pp. 22-32.

Sebastiani, F. 2002. "Machine Learning in Automated Text Categorization," *ACM Computing Surveys* (34:1), pp. 1-47.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *Management Information Systems Quarterly* (20:2), pp. 167-196.

Sterngold, J. 2011 "Say Goodbye to All Those Passwords," *BusinessWeek*: Online Magazine.

Suriadi, S., Foo, E., and Josang, A. 2009. "A User-Centric Federated Single Sign-On System," *Journal of Network and Computer Applications* (32:2), pp. 388-401.

Vladimir, N., and Vapnik, V. 1995. "The Nature of Statistical Learning Theory," Springer-Verlag New York.

Wegmann, A. 2003. "On the Systemic Enterprise Architecture Methodology (SEAM)," in Proceedings of the International Conference on Enterprise Information Systems (ICEIS), pp. 483-490.

Westin, A. 1967. *Privacy and Freedom*, New York: Atheneum.

Xu, H., Teo, H-H., Tan, B. C. Y., and Agarwal, T. 2010. "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.

Zott, C., Amit, R., and Massa, L. 2011. "The Business Model: Recent Developments and Future Research," *Journal of Management* (37:4), pp. 1019-1042.

Chapter 3

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

Extended from the paper: Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications, published in the proceedings of the 47th Annual Hawaii International Conference on System Sciences (HICSS 2014)
Waikoloa, Hawaii, USA, January 6-9, 2014
Publisher: IEEE Computer Society
ISBN: 978-1-4799-2504-9/14

Abstract Evidence collected from smartphone users shows a growing desire for the personalization services offered by mobile devices. However, the need to accurately identify users' contexts has important implications for their privacy. Users have to be able to place more trust in the service providers themselves. In this paper, I refer to Hevner et al. (2004)'s design science framework to present a new artifact in the form of a context-aware application for smartphones that is based on the Android operating system. With this application, personalization services and control are implemented to protect users' private information. Focus group interviews were conducted to examine users' privacy concerns both before and after having used my application. The results obtained confirm the utility of my artifact and provide support for the theoretical model. My research builds on previous literature about privacy calculus and users' acceptance of context-aware technology.

Keywords: Privacy Manager mobile application, Privacy concerns, Privacy calculus, Mobile TAM, Design science, Personalization, Control, Context awareness, Focus group

3.1 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" (Chellappa and Sin, 2005, pp. 181). The market for LBS, which offer service personalization according to the location of users, is enjoying strong growth, along with wider coverage offered by smartphones and higher speeds of data transfer 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 for companies that adopt the practice of personalization, LBS allows for the creation of tremendous benefits for consumers such as increased convenience, task efficiency, individualization, and the motivation to make intended purchases. Thus, it seems like a win-win situation for both consumers and providers.

Nonetheless, personalization also triggers privacy concerns for consumers (Culnan and Armstrong, 1999). In the competitive global marketplace, privacy has emerged as an important issue. Personalization is partly dependent on consumers' willingness to share their personal information (e.g., Awad and Krishnan, 2006). Thus, fundamental tension exists between a company's interests and consumer interests. On the one hand, companies need to collect users' personal information to offer them more customized products. On the other hand, consumers of personalized products or services consider personal data collection as an invasion of their privacy; indeed, they often give as little information as possible to the service provider (Sheng et al., 2008).

Accordingly, a significant body of research in privacy and information systems has suggested that information privacy and consumer concern have become important issues in today's information-intensive environment (Smith et al., 1996; Stewart and Segars, 2002; Lee et al., 2011). Service users and service providers have conflicting goals; thus, a "personalization-privacy paradox" is created, where consumers share their private information with a subjective expectation of personalized services, while assuming that the service provider will not indiscriminately use their personal information to increase its revenues (Awad and Krishnan, 2006; Xu et al., 2011). The control that consumers have on who can access their information and on how their information is exploited becomes a crucial element. Such control can alleviate their privacy concerns.

Consequently, consumers are expected to make decisions based on "privacy calculus" (Culnan and Armstrong, 1999; Dinev and Hart, 2006), a cost-benefit analysis that assesses the outcomes of private information disclosure. The calculus perspective

suggests that consumers tend to trade privacy when they can maximize the expected benefits from disclosing personal information, while minimizing the expected harm that may come from disclosing that information.

This study seeks to address concerns by researchers and practitioners regarding the design of context-aware applications. Furthermore, it aims to provide a set of guidelines to improve location-based service design, which are based on a better understanding of privacy issues in the mobile business sector. Existing studies tend to overlook consumers' privacy calculus by assuming that their personal information is exogenously given to companies and that costs are incurred (e.g., loss of privacy) simultaneously. In reality, this is not always the case. 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, my research question is: *how can design a context-aware mobile application that protects users' personal information by considering personalization and control?*

The remainder of this paper follows the structure of design science research methodology presented by Peffer et al. (2007). The next section reviews the extant literature and related works in the area of information privacy. O then present the methodology of this study in section 3.3. Section 3.4 describes the process of designing and implementing my artifact in the form of a mobile application system, as well as relevant functions. I introduce how my artifact is used in the case study and experiment described in section 3.5. Section 3.6 details the findings and evaluations of the focus group interviews. Finally, I conclude the research work by discussing the implications of the study and possible future research.

3.2 Theoretical Background and Related Work

In this section I derive a set of gaps in the literature by: (1) introducing the notions of privacy concerns, personalization and controls, (2) discussing users' willingness to provide information from a privacy calculus perspective, and (3) assessing the existing literature on a TAM.

3.2.1 Privacy Concerns, Personalization and Control

3.2.1.1 Privacy Concerns

Concern over privacy is receiving increased attention because of the huge amount of personal information being collected, stored, transmitted and published on the Internet (Hong and Thong, 2013). Recent studies have addressed privacy concerns in different contexts, such as behavioral advertising (King and Jessen, 2010), scheduling (Bilogrevic et al., 2011) and tourist web sites (Lee and Cranage, 2011). Smith et al. (1996) identified four dimensions of an individual's concern about privacy, namely: *(1.1) collection*, *(1.2)* errors, (1.3) unauthorized secondary use and (1.4) improper access (refer to Table 3.1). These four factors provide a framework for explaining concerns over information privacy (Stewart and Segars, 2002). The likelihood of privacy breaches can occur in any of the following cases: (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.

Table 3.1. Theory models and key concepts

Categories	Existing concepts
(1) Smith et al.'s (1996) factors of an individual's privacy concerns	(1.1) Collection (1.2) Errors (1.3) Unauthorized secondary use (1.4) Improper access
(2) Dinev and Hart's (2006) extended privacy calculus model	(2.1) Risk beliefs (2.2) Confidence and enticement beliefs (2.3) Benefit beliefs (2.4) Willingness to act
(3) Davis's (1989) model of technology acceptance	(3.1) Perceived ease of use (3.2) Perceived usefulness

Consumer privacy concerns vary dramatically by information type. For instance, both Phelps et al. (2000) and Ward et al. (2005) 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 exchange for values or services that these companies would provide.

It is worth noting that privacy concerns may differ from person to person. Junglas et al. (2008) examined consumers' personality traits and concerns about privacy, showing that agreeableness has a negative effect on privacy concerns, whereas they are positively affected by conscientiousness and openness. Even in situations in which perceived usefulness is the same, people may exhibit different levels of privacy concern for different types of services. For instance, a study conducted by Barkhuus and Dey (2003) found that location-tracking services generated more concerns about privacy than position-aware services, despite the fact that these two types of LBS use similar technology.

3.2.1.2 Privacy Concerns and Personalization

An effective way of improving the usability of mobile applications is to adapt the content and service to meet the needs of each individual user. Thanks to new technologies, large amounts of detailed data about consumer behavior information can now be collected, stored and used in an electronic and networked environment. As a result, companies can accurately match their product or service offerings to the needs of their customers, enabling them to develop loyalty programs or other benefits, and even to serve their customers individually (Culnan and Milberg, 1999). Implied here is a reflection that consumer preferences create benefits for both the companies and the consumers themselves. However, this development faces a serious barrier: the lack of trust which is generated primarily by the inappropriate use of consumers' information by companies. This leads to increasing customer concerns about information privacy.

According to some authors, privacy concerns are not absolute concepts (Sheng et al., 2008). 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 of value to them. This is consistent with expectancy theory in marketing (Oliver, 1974), where users will behave in ways that maximize positive outcomes and minimize negative outcomes (Dinev and Hart, 2006). Therefore, consumers may be willing to disclose and share their personal information for the benefit of personalization if the perceived overall value is balanced with, if not outweighed by, the loss of information privacy. On the one hand, Chellappa and Sin (2005) 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 (2003) argued that individuals are more likely to accept the loss of privacy, so long as benefits exceed the perceived risks of information disclosure. A more recent study conducted by Liu et al. (2011) found that personalized services play a significant moderating effect on the relationship between users' disclosed information and their perceived benefits. Moreover, privacy concerns may vary according to the purpose or

context of use; thus, they can be seen as situation dependent. For example, Sheng et al. (2008) 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. Similarly, Mallat (2007) suggested that mobile users are more likely to use mobile payment in situations that lack other payment methods or are considered to be urgent. In addition, cultures may serve as a moderator in information privacy concerns. Dinev et al. (2006) revealed the existence of a cross-cultural difference in the privacy calculus model in e-commerce between Italy and the United States, indicating that culture values can play a significant moderating effect on consumers' privacy concerns. In addition, empirical results have provided evidence that consumers are usually willing to share their information with another party if they have trust in them. For example, Chellappa and Sin (2005) found that consumers' intentions to use personalization services are positively influenced by their trust in the service provider. Ajami et al. (2012) came to a similar conclusion in the context of mobile social interactions.

3.2.1.3 Privacy Concerns and Control

Privacy concerns may arise from a lack of adequate control over the disclosure of personal information. Users take high risks when they submit their personal information to companies (Malhotra et al., 2004). They feel more threatened if technology has the capability to access, collect and use their personal information without their consent. For this reason, privacy concerns arise from the feeling that their personal information is vulnerable and they have no control over it (Dinve and Hart, 2004). Hence, loss of control over information is a kind of invasion of privacy.

According to Goodwin (1991), consumers' control can be divided into two categories, namely control over an unwanted presence in the environment, and control over information obtained during market transactions. The first category relates to control that is present, whereas the latter relates to control over who knows about the transaction or behavior. In a mobile users' context in particular, the first type of control is the consumers' ability to control the actions of other parties in the environment during an interaction (Hoffman et al., 1999). For example, a mobile user may be worried about giving out credit card information to a small or unknown mobile voice-over IP company. Secure transaction technologies may serve as a common mechanism to gain control over this kind of environmental problem. The second type of privacy concern occurs because the transaction or interaction is not a one-time exchange in a mobile environment. In practice, individuals disclose data about themselves (such as names and email addresses) to the service provider. Thanks to the development of Internet facilities, these huge amounts of data can then be stored on a database for significant periods of time. They may also be shared with other parts of the company or other third-party organizations

(Whitley, 2009), with or without the knowledge of mobile users. Even in cases where the data is not individual-specific, it could raise serious concerns about privacy invasion.

Therefore, privacy losses associated with both issues are of great concern to mobile users. In earlier times, in traditional markets, control over unwanted presences in the environment served as a major deterrent. However, in an Internet-based society, it is increasingly important to understand how disclosed data is being further used and reused subsequent to the transaction in which the information was originally collected (Whitley, 2009).

In the academic world, many privacy surveys have indicated that Internet users find it important to know how their personal information is being used and to have control over this usage (Kobsa, 2007). A number of studies have examined the effect of such privacy controls. For example, Culnan and Armstrong (1999) argued that consumers perceived information disclosure as being 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 (2004) showed 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. (2004) demonstrated that control over personal information served as one of the most important factors in Internet users' information privacy concerns. Hui et al. (2007) 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. (2008) also found that diversified rules of control over the conditions under which users' information is shared may increase efficiency without violating users' personal privacy preferences.

3.2.2 Privacy Calculus Perspective

To better understand the basis of consumer privacy concerns, it is necessary to develop an underlying framework to explain the factors that make consumers willing to disclose their personal information in a transaction. Culnan and Armstrong (1999) argued that an individual's decision process prior to the disclosure of the personal information necessary to complete a retail transaction involves a *privacy calculus.* Under this framework, individuals are viewed as being rational economic agents. As such, they perform a risk-benefit analysis of all the factors related to a particular information disclosure situation in order to assess privacy concerns. Based on such an analysis, people are more likely to accept the loss of privacy that accompanies the disclosure of information so long as an acceptable level of risk accompanies the benefits they pursue (Culnan and Bies, 2003).

While Culnan and Armstrong's privacy calculus relates to transactions with retailers, Dinev and Hart (2006) extended the model to include the context of Internet transactions (see Table 3.1). They documented that Internet users make choices in which they surrender a certain degree of privacy (*2.2 confidence and enticement beliefs*) in exchange for outcomes that are perceived to be worth the risk of information disclosure (*2.1 risk beliefs*). The anticipation of benefits (*2.3 benefit beliefs*), either monetary or non-monetary, had a positive influence on their intention to disclose personal information (*2.4 willingness to act*), while the expected potential risk was negatively related to their intention to provide personal information.

The widespread adoption of smartphones presents an interesting avenue for future information research into information disclosure decisions because of the unique nature of associated privacy concerns. In contrast with most prior research, which applied a privacy calculus framework in an online context, I intend to extend the calculus model to a mobile context in which users are more engaged and privacy concerns are particularly salient.

Mobile devices are, in essence, a form of technology. Thus, I now turn my attention to assessing the existing literature on the TAM. Privacy concerns and privacy protection have been considered an important breakpoint for the popularity of mobile commerce. Examining the mobile application acceptance model would provide a comprehensive picture of privacy concerns.

3.2.3 Technology Acceptance Model (TAM)

Introduced by Davis (1989), the TAM is an adaptation of the theory of reasoned action (TRA), which was specifically tailored for modeling user acceptance of information systems (Davis et al., 1989). Since then, the TAM has been widely tested with numerous empirical studies, which have consistently explained a substantial proportion of the variance (typically about 40%). Consequently, the TAM has become well-established as a robust, powerful, and parsimonious model for predicting user acceptance (Venkatesh, 2000; Venkatesh and Davis, 2000).

According to TAM theory, an individual's behavioral intention to accept (that is to say, use), a new form of IT is determined by two beliefs: *perceived ease of use* and *perceived usefulness* (see Table 3.1). *Ease of use (3.1)* can be defined as the degree to which a person believes that using a particular system will be free of effort (Davis, 1989). In contrast, *perceived usefulness (3.2)* refers to the degree to which a person believes that using a particular system would enhance his or her job performance. This construct defines the prospective user's subjective perception that using a new form of IT would increase his or her performance. Both beliefs have been recognized as crucial elements in

the acceptance of an application (Venkatesh, 2000; Davis et al., 1989; Gefen et al., 2003). Other external variables of intention to use (such as system characteristics), are mediated by these two beliefs. Furthermore, perceived usefulness is also influenced by perceived ease of use because the easier the system is to use, the more useful it can become.

Nevertheless, the TAM's goal is to explain computer usage behavior. In the context of mobile applications, would such a model also work? What are the new elements that impact on a mobile user's intention to use certain applications? In the sections that follow, I attempt to answer these questions.

3.3 Methodology

Based on the relevant literature, I created a new and innovative artifact (March and Smith, 1995) in the form of a context-aware application for smartphones based on the Android operating system. In this application, personalization services and control are implemented to protect users' private information. March and Smith (1995) distinguished between design sciences and natural sciences. The former involves building and evaluating IT artifacts, including: 1) constructs, which are "concepts with which to characterize phenomenon", 2) models, that "describe tasks, situations, or artifacts", 3) methods, as "ways of performing goal directed activities", and 4) instantiations, which are "physical implementations intended to perform certain tasks".

To build and evaluate my artifact, I followed the design science research framework for information systems research presented by Hevner et al. (2004), as illustrated in Figure 3.1. I started with the business need to ensure the goal of research relevance. I then examined the requirements from the contextual environment of the research and described my research artifact through environmental field testing. In order to achieve rigor in my research, I drew on existing theories and knowledge-based methods, adding newly generated knowledge to this knowledge base. The central design cycle focuses on the construction and evaluation of artifacts and processes. These multiple assessments and refinements allowed me to define the contributions to both the environment and the knowledge base.

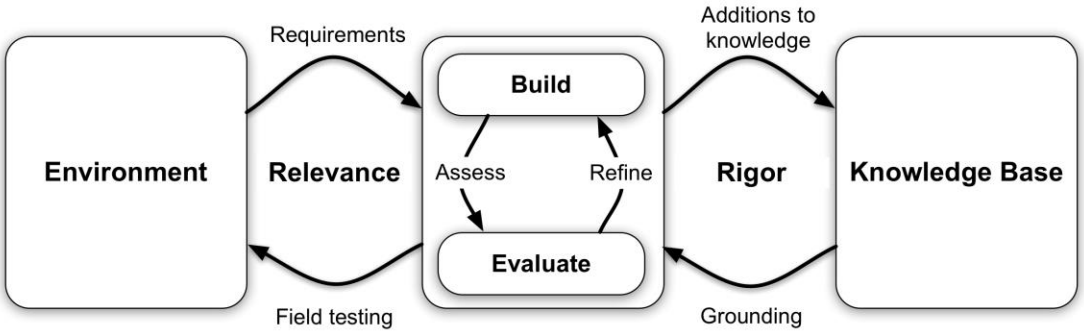


Figure 3.1. Information systems research framework (based on Hevner et al., 2004)

Our design process is in alignment with the seven guidelines put forward by Hevner et al. (2004). In accordance with guideline 1, this study introduced a new artifact in the form of a mobile application called Privacy Manager. In a previous study, I tested the performance of the algorithm of Privacy Manager using location and time data from 168 users during the course of one year. Nonetheless, this study did not perform any usability tests. Therefore, following guideline 2, I stated that Privacy Manager would protect users' mobile phones and their private information by limiting access to their mobile phones, using their location and time of day as authentication. In accordance with guideline 3, I used a qualitative methodology to test the usability of this application by performing focus group interviews with ten participants before the application's use and ten participants after the application's use. I then stated thatmy main research contribution was the context-aware mobile application called Privacy Manager, based on the notion that context awareness could help to achieve proper tradeoffs between adaptive authentication and utility (guideline 4). The results of this study have also confirmed and extended the three kernel theories used, namely: (a) the four key factors of an individual's privacy concerns (Smith et al., 1996), (b) the notion of a privacy calculus model (Dinev and Hart, 2006) and (c) the users' TAM (Davis et al., 1989; Davis, 1989). Later, I applied rigorous methods to collect users' requirements. I also used existing frameworks to develop my mobile application and applied data triangulation while performing an analysis of data collected in the focus groups (guideline 5). In accordance with guideline 6, I performed two main iterations, which were associated with the two main clusters of users interviewed. The results of such iterations were presented in the results section. Finally, I followed guideline 7 and decided to present the results to an audience that was interested in technology details as well as the management implications of this study.

3.4 Artifact Design and Development

This section provides an analytical description of the artifact design and development process. I followed the guidelines put forward by Hevner et al. (2004) for creating a design cycle between the constructions of an artifact. This took the form of a mobile application, its evaluation, and subsequent feedback for further refining my design. In this section, I will first compare and assess the existing literature on privacy management mobile applications. I will then go on to present the design, realization and implementation of my mobile application to address the gap in the literature.

3.4.1 Existing Privacy Management Mobile Applications

A number of research efforts have been conducted in the area of privacy in context-aware 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 3.2 shows examples of mobile applications for each perspective.

Table 3.2. Mobile applications for privacy management

Privacy management mobile applications	CA	AC	UP
Ankolekar et al., 2009; Enck et al., 2010; Mohan et al., 2008; Priyantha et al., 2001	X		
De Montjoye et al., 2012		X	
Kenteris et al., 2009			X
Davidson and Livshits, 2012		X	X
Beresford et al., 2011; Gaonkar et al., 2008; Miluzzo et al., 2008; Toch et al., 2010;	X	X	
Christin et al., 2012; Marmasse and Schmandt, 2000; Raento et al., 2005; Sadeh et al. 2005; Sohn et al., 2005	X		X
Our application «Privacy Manager»	X	X	X

The context approach promotes services that are adaptable to context changes (Maamar et al., 2004). In the current study, the applications in mobile privacy management are defined as being context-aware in accordance with this approach. A number of existing

privacy- related mobile applications have been designed and created using the context-awareness approach. For example, Friednlee (Ankolekar et al., 2009) defined the users' "real" friend by analyzing changes of context in terms of phone behavior. TraintDroid (Enck et al., 2010) tracked the locations of users for real-time analysis in order to monitor potential threats relating to their personal information. Nericell (Mohan et al., 2008) targeted road and traffic services by using mobile smartphones equipped with an array of sensors (e.g., GPS, accelerometer, and microphone). Users could receive notifications when the context of road or traffic was changed. The Crick Compass system (Priyantha et al., 2001) was also based on context-aware technologies; it provided a combination of orientation and position information to determine a mobile phone's indoor and outdoor distances.

The second approach proactively tailors products or services to meet the needs of users, and adapts them according to the personal preferences of users (Roman and Campbell, 2002). Applications that use this approach come within the "personalization" category. One such personalization-based mobile application is called "my Mytilene City" (Kenteris et al., 2009). Users' personal information is used to create personalized portable tourist applications across most available mobile device platforms with rich content that matches user preferences.

The authorization and access control approach promotes policies that constrain what a user can do directly and what the programs that execute on behalf of the users are allowed to do (Sandhu and Samarati, 1994). Applications that use this approach come within the "control" category. The OpenPDS (open-source Personal Data Store) mobile application (De Montjoye et al., 2012) is a good example in this category. This application has enabled users to easily collect, store, and allow access to their data, as well as manage and control fine grained authorizations for third-service services. Users can, therefore, decide whether such services provide enough value compared with the amount of data asked for; the application will then help the user make the best decision.

In fact, many mobile applications cover more than one perspective (e.g., MockDroid (Beresford et al., 2011), CenceMe (Miluzzo et al., 2008), Micro-Blog (Gaonkar et al., 2008), and Locaccino (Toch et al., 2010)). These mobile applications use both the context-aware approach (CA) and the access control (AC) approach to design and develop their mobile solutions to privacy concerns. MoRePriv (Davidson and Livshits, 2012), is a privacy-based mobile service that focuses not only on the authorization and access control (AC) perspective, but also the user preference (UP) perspective. On the one hand, MoRePriv parses smartphone users' information streams over the Internet with users' authorization – through a users' email, SMS, or a social networking database – to build a user's profile that preserves his/her privacy by providing filter hooks to protect information leaks. On the other hand, MoRePriv empowers a user to organize his/her

preferences in different user applications by exposing the relevant personalization application programming interfaces. To my knowledge, there are some privacy-aware mobile applications (e.g., uSafe (Christin et al., 2012), ContextPhone (Raento et al., 2005), ComMotion (Marmasse and Schmandt, 2000), Place-its (Sohn et al., 2005), and MyCampus (Sadeh et al., 2005)), which use context technologies (CA) and have adapted their personalized preferences (UP) to manage mobile users' personal information.

Although a considerable amount of studies into personalization and privacy, and control and privacy have been carried out, little attention has been paid to the overlap that exists between personalization, control and privacy concerns. In this paper, I try to fill this research gap.

3.4.2 Objectives of the Solution

The main objective of the solution is to create a context-aware application that collects information from the environment by using a mobile phone's sensors. These can be used to induce a user's movement pattern, both in terms of time and location. Such a movement pattern can be used as an unique identifier for a SSO application, which should be easy to use and adaptive, since a user's location and movement patterns may change over time. Accordingly, time and location data should be safely stored within the application to protect a user's privacy. Personalization and control are two significant functions that are integrated in the solution to evaluate the benefits and costs associated with the disclosure of personal information.

3.4.3 Implementation of the Application

Before developing the application I conducted a set of individual interviews to help me develop the questions to be put to the focus group sessions. I used ten participants as a control group; they were asked to express their opinion on privacy concerns without using the application (I will refer to them as cluster 1). Ten different participants were asked to refine their viewpoints on privacy concerns after using the application (I will refer to them as cluster 2). Each of the individual interviews lasted for approximately one hour. Building on the results obtained by the individual interviews, as well as those with cluster 1, I designed and developed a mobile application called Privacy Manager. This application is based on Android (versions 2.1 to 4.1) open source mobile phone platforms, and was developed using the Android SDK, which is a comprehensive set of development tools and user interface frameworks. Android applications are called packages and are executed in a custom Java virtual machine running on a Linux kernel. Each application can access sensors available on the device and acquire raw sensor data by using the Android sensor framework. The sensor framework provides several classes

and interfaces to perform a wide variety of sensor-related tasks. The 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 preferences configuration, (2) training, (3) tracking, and (4) import and export. The *user preferences configuration* uses a SQLite database to store user preferences in Figure 3.2. Means of notification (email, vibration, and alarm) are shown on the left of Figure 3.2: users can select one or more notification mode(s) on the configuration interface, depending on users' preferences and their current environment. For example, the email and vibration notifications could serve as a good option during the working day.

The frequencies for recording data and tracking data can be set between one minute and one hour. The precision of localization can be set between one hundred meters and ten kilometers, as shown on the right-hand side of Figure 3.2. The more users' context data that is disclosed, the more accurate the tracking function will be. Users can define their preferences by changing the value of the recording frequency, the comparison frequency, and distance.

The "Recoding Frequency" describes the frequency (in minutes) that the application records users' time and location. "Comparison Frequency" represents how often the user compares his/her current location information with the data in the profiles; the default value is 5 minutes. Users are free to reduce this value to increase the degree of accuracy, but by doing so, more battery power is consumed. If users set the tracking frequency as less than the recording frequency, the tracking frequency will be replaced by the recording frequency automatically.

The "Distance", which is measured in meters, describes how far the user compares his/her current location with the data in the profile. It allows users to define the circular area that is determined in the configuration setting as the radius from the location data in the profile to identify themselves. Hence, this parameter specifies the accuracy of the location. The default value is 300 meters; however, if the user moves often between different buildings in a certain area (e.g., a postman who distributes mail to several blocks), he/she can increase this value up to 5 kilometers. However, if the user's working area is limited to a specific area, like an office, then he/she can reduce this value to 100 meters to increase the accuracy.

In addition, users can set a password to create a new profile or stop an ongoing tracking function.

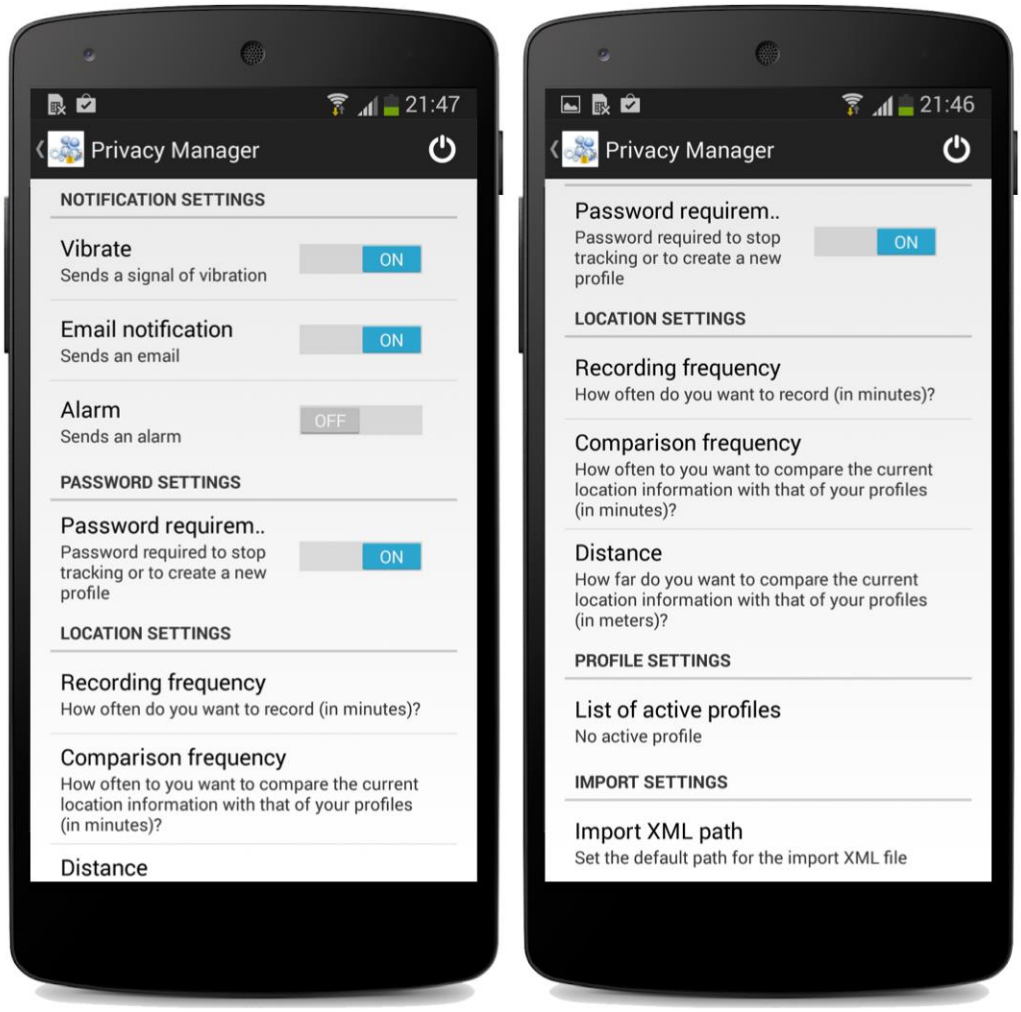


Figure 3.2. Privacy Manager preference configurations

Users are allowed to define different profiles (e.g., weekday) according to different situations. The configuration is shown on the left side of Figure 3.3. In order to use the application, users have to create at least one profile for a minimum 24 hours with the training mode. Of course, as the time spent on the training mode increases, the identification accuracy will also increase. I did not use the machine learning cluster technology to create those profiles automatically because participants in Cluster 1 clearly expressed their intention to control data by defining their own profiles, believing that this makes it more trustworthy and flexible. On the training screen, users can find information about the current profile, their last location, and the corresponding recorded date and time.

In the tracking mode, users can activate one or more profiles, as shown on the right side of Figure 3.3. If a user's location information at a certain time does not match any location coordinates in all profiles, the application then blocks the mobile to protect their

personal information from potential unknown access and sends a notification to the user for each comparison frequency (e.g., every 5 minutes). In the notification message, users can find detailed information including mobile phone's current coordinate and time information. If the mobile phone is used by the right user, he/she can use the password which was defined previously in the application, or a matched NFC equipment to unblock the mobile phone.

Moreover, noticing that GPS signal is lost when the mobile phone is moved to an indoor environment, I have implicitly implemented two modes, which switch between GPS and WiFi for collecting users' information. In cases where the GPS signal is lost, the application will switch from outdoor mode to indoor mode. That is to say, the WiFi will be activated to continue collecting users' location information so as to avoid wasting battery by constantly searching for a GPS signal.

In order to verify the mobile phone user, I designed and developed a new algorithm for clustering users' profiles. The training and tracking data contains users' location and time information. When location information comes with the corresponding time, I can compare it with the closest data in terms of time in the training data. Suppose that a user activates the training mode at 8:00am and records the location every 5 minutes (Recording Frequency = 5 minutes). One day, the user starts the tracking mode at 8:02 am with a Comparison Frequency = 10 minutes. In this case, my algorithm will compare the location information at 8:12 am with the closest data in the profiles: the location information at 8:10 am.

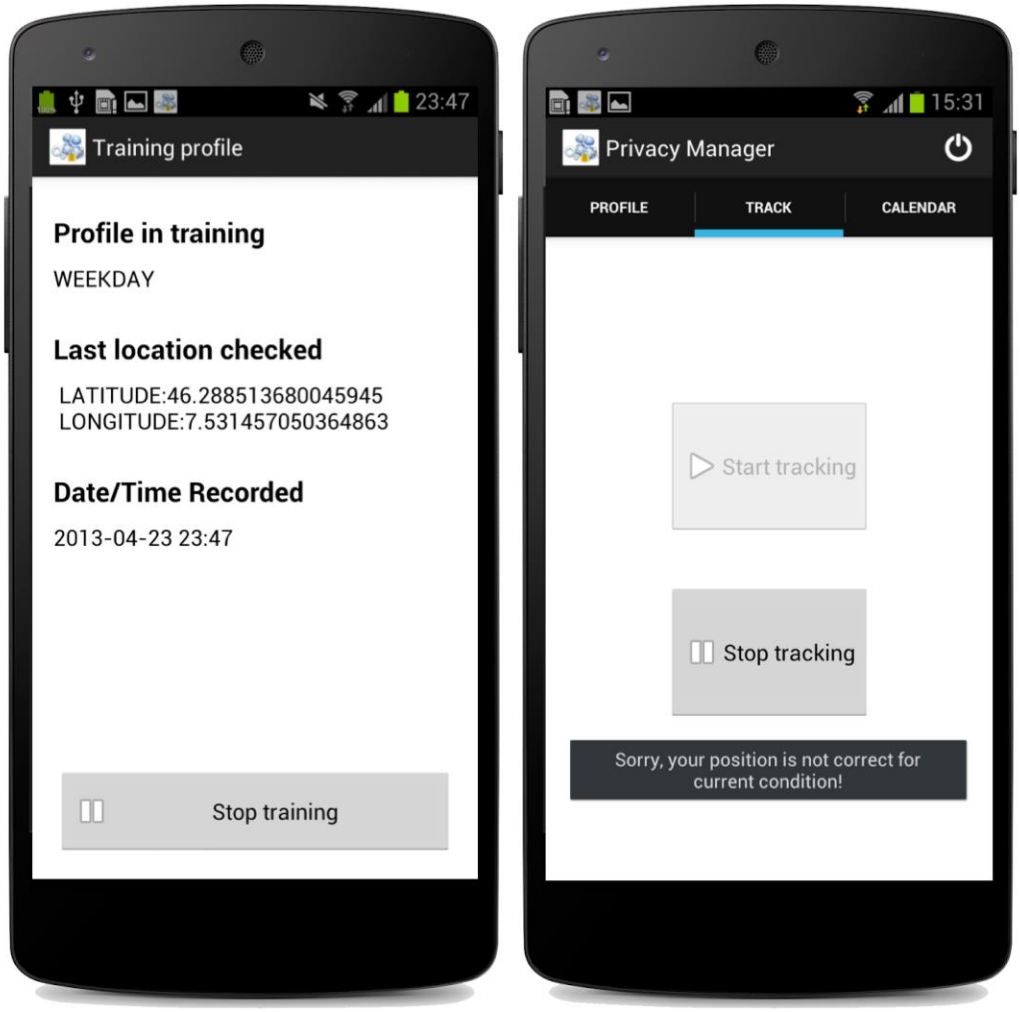


Figure 3.3. Privacy Manager training and tracking functions

The import and export function (on the left side of Figure 3.4) was implemented for exporting all users' data in XML format and importing the data to the phone if users change their mobile phones. According to the feedback from cluster 1, most participants expressed their concerns about disclosing their data to the application provider. If the application server does not store and synchronize users' data, then it will be less convenient to recover users' data, because mobile users have to manually back up their personal data. However, participants insisted on their preference to control their data; they did not want to allow the provider or any third party to store or access it. Thus, I decided to store users' personal data locally, which means that all data will be stored in a database on the mobile phone.

The application can also show users' historical activities by displaying the locations on the map. Furthermore, it can help users to compare the tracking data (red points) with the training data (blue points), as shown on the right side of Figure 3.4.

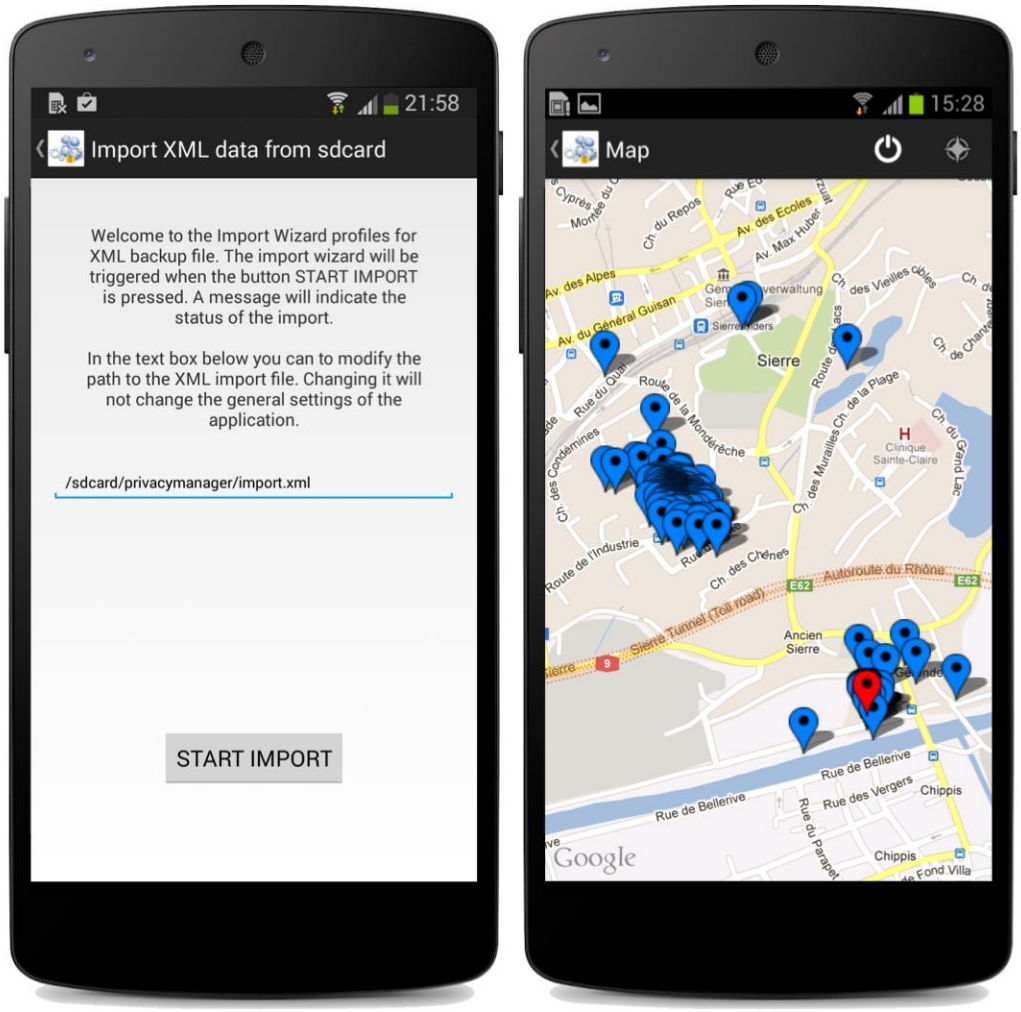


Figure 3.4. Privacy Manager import function and user behavior map

3.5 Demonstration

This section focuses on: (1) how participants used the application, in order to allow to assess their privacy concerns and protect their personal information; (2) the conscription of participants to the study; and (3) the procedure used for data analysis.

3.5.1 Use Case of the Application

Participants in the study 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); and (3) tracking (6 days).

During the configuration phase, after the user has logged in, he/she can manually introduce their configuration settings or import them by using the import and export function.

During the training phase, every time that the user arrives in a new place, a cluster is created and the application automatically collects location data to learn the user's movement patterns and any lifestyle habits.

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

3.5.2 Demography of Participants

This study recruited twenty participants, offering a small gift for completion of the study. In order to ensure the artifact is both useful to practitioners (relevant) and contributes to the IS knowledge base (rigorous), the artifact underwent stringent evaluation. I conducted two iterations before and after using this application to test the usability of this application. It is investigated that users' privacy concerns by performing several focus group interviews.

Twenty participants took part in the study. As explained previously, ten of them were used as a control group. They were asked to express their opinion on privacy concerns without using the application (Cluster 1). The remaining ten participants refined their views on privacy concerns after using the application (Cluster 2).

Ages in both groups ranged between 21 and 41 years with a mean of 30.3. The group comprised of 12 men and 8 women from different backgrounds (e.g., computer science, marketing, educators and housewives). 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, and from social networking to self-entertainment. Most participants had used at least one location-based mobile application (e.g., Google map, weather, etc.). Detailed demographic information is indicated in Table 3.3.

Table 3.3. Demographic data on participants

	Mean (std.)	Range	Percentage
Gender	-	Male	60.0%
		Female	40.0%
Age	30.25 (4.72)	<25	10.0%
		26-30	50.0%
		31-35	30.0%
		36-40	5.0%
		>40	5.0%
Experience of using Smart Phone (years)	4.13 (2.39)	0	5.0%
		41671	30.0%
		41732	20.0%
		41795	25.0%
		>6	20.0%

3.5.3 Focus Group Data Collection and Analysis

I conducted six focus group interviews, with group sizes ranging from two to five people. During the interviews, I asked about users' experiences relating to ease of use and privacy issues.

For the sake of clarity, I 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 have been proven an effective research technique for investigating individuals' perceptions and attitudes, and exploring the reasons behind them (Kitzinger, 1995; Powell and Single, 1996).

Our focus groups revolved around the same set of questions in order to explore users' reactions to the concept of protecting privacy. The aim was to identify the threats that concern users and what users care about, and to elicit requirements for a mobile application based on this concept. I sought to incorporate users' feedback at an early stage of the development process in order to address usability issues and design for a positive user experience.

Each focus group session began by thanking the participants for being available for the interview. The researcher then 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. I 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 out personal information to a mobile application? Please explain your selection*".

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

I adopted a "*framework analysis*" method to guide the analysis process. Originally used in policy issues, framework analysis is a qualitative method that is well suited to research; it asks specific questions, uses a limited time frame, and deals with a priori issues (Srivastava and Thomson, 2009). It particularly matches the situation because it allows the inclusion of a priori as well as emergent concepts. Currently, three existing theoretical foundations exist; namely, Smith et al.'s (1996) four dimensions of individuals' privacy concerns, privacy calculus (Dinev and Hart, 2006), and Davis's (1989) TAM (which will be explained in detail in the section that follows). On the other hand, the intention was to allow new perceptions and requirements to emerge. Thus, I organized the framework analysis method into five key steps (Lacey and Luff, 2007; Srivastava and Thomson, 2009).

1. *Familiarization*: achieved by reading the data collected during interviews with users. In this step, two researchers listened to and transcribed the audio recordings to gain an overview of the data collected.

2. *Identifying a thematic framework*: achieved by identifying a set of variables that were developed both from a priori issues and from issues that emerged from the first cluster. Two researchers reviewed all transcripts carefully and created separate categories. They then had a face-to-face meeting to compare and combine these categories. Some comments were placed in more than one category, whilst others lacked sufficient significance; the latter were excluded.

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

4. *Charting*: achieved by using the headings and subheadings drawn from previous stages in 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. This will be further discussed in the next section.

3.6 Findings and Evaluation

In this section, I present the qualitative analysis of the focus group discussions. I refer to participants using the following code: C=Cluster, G=Group, P=Participant. The analysis presented in Table 3.4 illustrates how I extend existing literature, which can be divided into three categories: (1) privacy concerns; (2) privacy calculus; and (3) evaluation of utility.

Table 3.4. New concepts for a context-aware application

Categories	Existing concepts	New concepts
(1) Smith et al.'s (1996) factors of an 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 (2006) 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 (1989) 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 were derived from the original papers, whereas I derived new concepts from the results. As can be seen in the Table 3.4, some concepts overlap across two categories; namely, "risk beliefs" and "user's risk attitude". This results lead to believe that causal or cross-loading effects among concepts might exist.

3.6.1 Privacy Concerns

The first line of Table 3.4 summarizes the dimensions related to mobile users' privacy concerns. The results found some support for Smith et al.'s (1996) proposition that there are four factors of individual privacy concerns in the mobile context.

Concerns about collection (1.1). Data collection is the concern most frequently mentioned by smartphone users. Their concerns are about extensive amounts of personally identifiable data that are collected and stored in databases (Smith et al., 1996). In this study, a common opinion among all participants was that in general they do not like to share things with applications, especially such highly private information as name, home address, and so forth. Moreover, they users tended to treat 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*". In cases in which users are mandatorily requested to provide certain information, "*I prefer to provide an email address that I do not use often to applications*" (C1G1P3). Another participant from the same session similarly noted that: "*Sometimes I give them fake information such as my email address*" (C1G1P1).

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 could lead to serious consequences if it actually took place. Thus, I have included this concern in the analysis of this study.

Concerns about unauthorized secondary use (1.3) - Unauthorized secondary use can be defined as concerns about information that is collected for one purpose but is used for another, either within or outside of an organization (Smith et al.'s 1996). This concern was also mentioned frequently in this study. The participants differentiated such misrepresentation concerns between the application provider and third parties. In particular, they were afraid that data from the application provider could be 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, one participant stated that "*companies are always selling data to others, like marketing companies. They are making money on my personal information*" (C1G1P3). Similarly, "*Contrast thinking, what if there is another company which offers to buy this application for billions of dollars? Perhaps that company is not interested in the application itself at all, but only cares about the data?*" (C2G2P2).

Furthermore, participants were *concerned about improper access (1.4)*. This refers to individuals' concerns that data about them are readily available to people who are not properly authorized to view or work with this data (Smith et al., 1996). "*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 (1996) four key factors of an individual's privacy concerns, more concerns emerged. *Legal considerations (1.5)* also appear to 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 constrain the service provider not to collect and use my information when I use this application. This will make me feel safer*" (C1G2P5). In the same group, one participant commented: "*I agree. The problem now is that the laws and regulations to protect mobile users' private information are still immature. To sign such a statement also makes me feel better since if one day something unhappy happens, I can accuse the service provider with that document*" (C1G2P4).

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 larger companies because they think these sorts of companies can afford to offer quality services without having to sell information to others. In addition, larger companies have more IT capability.

Our focus groups also identified *concerns about information release agreements (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). In the same group, one participant added: "*Yes, like Facebook has changed their privacy regulations several times*" (C2G2P2). This dimension of privacy concern is relatively new in the mobile context, because of the need for applications to be updated constantly in order to improve services. Privacy regulations might be revised over time between different versions. Once users click on "yes", they probably do not pay attention to the changes of agreement.

An analysis of the focus group discussions helped us to get an in-depth understanding of mobile users' privacy concerns. In addition to the traditional four key concerns, I also found other sources of privacy concerns; namely, legal considerations, reputation considerations and information release agreements. In the next session, I will discuss privacy benefits, and the role of personalization and control in privacy calculus.

3.6.2 Privacy Calculus

The main objective of the application is to protect mobile user personal information on mobile phones by using an ASSO solution. Based on context-aware technology, such a

solution is expected to achieve the proper tradeoff between dynamic authentication and ease of use (Bonazzi et al., 2011). In the context of this study, all participants agreed that the concept has the potential to protect privacy, but several conditions must be met. The key dimensions of privacy calculus are summarized in Table 3.4. It is particularly interested in the relationships between these constructs.

In addition to privacy concerns, the next perceived privacy risk reported by the participants is *risk belief (2.1)*. This is defined as the perceived risk of opportunistic behavior related to the disclosure of personal information submitted by mobile users in general (Hui et al., 2007). As one participant said: "*It is dangerous to give information to them (application providers), because you never know how they will use your information*" (C1G1P1). Such a risk belief is more likely to have a negative impact on an individual's willingness to provide personal information. Later the same participants claimed: "*I don't like to give my information to the application provider. I don't like to share such detailed 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...so basically I would not give my activity information to any application*" (C2G2P2).

It was suggested that *confidence and enticement beliefs (2.2) are also associated with privacy concerns*; that is to say, if mobile applications are seen as reliable and any personal information submitted to these applications is used and kept in a safe environment, then this should increase people's willingness to use mobile applications, and vice versa. This factor is related to people's trust in mobile applications. According to one participant: "*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). Another stated: "*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). Thus, lower levels of trust in mobile applications and smartphones in general should negatively influence users' willingness to disclose personal information to the application, and in turn influence their intentions to use it. This is consistent with Dinev and Hart's (2006) finding that a lower level of interest was related to a lower level of willingness to provide the Internet with personal information.

In the analysis of Privacy Manager, I have also included the concept of *benefit beliefs (2.3)*. As mentioned earlier, this application is aimed at protecting users' private information on their mobile phones. The greater the perceived benefit, the more likely it is that users will want to use it. For example: "*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). The benefits of the application should be reduced for users who do not care much about the information they keep on their mobile phone, or for those who have information on their mobile phone which is not very personal. This will result in lower intentions to use the application. One participant's statement supports this argument: "*Since I don't really care about keeping the information I store on my smartphone secret, I do 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 latter should be directly linked to the former. However, the former is an assessment of willingness to provide information to applications in general, whilst the latter reflects an individual's intention to use this specific application. Personal interest in applications is another factor that determines a user's willingness to use this application under the category of confidence and enticement beliefs. This refers to personal interest in a mobile application or a cognitive attraction to that application, both of which can override a user's 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 had an impact on their adoption of this application. I have already observed that *control over information (2.5)* and *personalized features (2.6)* were frequently mentioned in this study. While other dimensions in privacy calculus are difficult to change, it is possible to manipulate these two factors. Thus, I have incorporated participant feedback 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 the privacy context. Typical comments by participants 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) and "*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 a 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 was also suggested that an import/export option could be adopted, because "*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, with regard to the notification mode in Privacy Manager, which detects that your phone is being used in unusual circumstances, 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 if 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 were made: "*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 came to 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 include the collection of location data. The first consideration is the data collection mode. Most participants suggested using WiFi if possible, because "*it can save the battery*" (C1G1P1). One participant recommended that: "*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 take care of 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" that has been set by the user in the user preferences. A common opinion among all participants was that it should use ambiguous comparison. For example, one participant 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). She did, however, admit that it might create new concerns: "*If it is not that precise, then other people, for example my colleagues can easily manipulate my phone without this application's notice*". In the end, I decided to provide both the distance option and the time option for users to select their preferences.

3.6.3 Evaluation of Utility

This analysis focuses on the second cluster of the empirical study. The evaluation of utility is based on Davis's (1989) technology acceptance model (TAM), which refers as a means of predicting technology usage. According to this theory, intention of technology usages depends on two variables: *perceived ease of use* and *perceived usefulness*, and such behavioral intention fully mediates the effects of these two variables on actual usage behaviors (Davis et al., 1989). Although TAM is usually validated by using a measure of behavioral intention to use rather than actual use, some studies had proved that behavioral intention is likely to be correlated with actual usage (Turner et al., 2010; Venkatesh and Davis, 2000). Hence behavioral intention can be served a good indicator to predict actual usage. The current study focuses on the discussion of behavioral intention.

Ease of use (3.1) has been defined as the degree to which a person believes that using a particular system will be free of effort (Davis, 1989). It has been recognized as a crucial element in the acceptance of an application (Venkatesh, 2000). Overall, participants found that 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).

In contrast, *perceived usefulness (3.2)*, 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). Other participants stated: "*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) and "*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) a *user's mobility (3.3)* and (2) a *user's risk attitude (3.4)*. On the one hand, the application may be more applicable for people who have a life based on routine. 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 to some place 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). It was also suggested that when an individual's privacy concerns are very high, the application is seen to be 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. That is a lot of rich*

information, and privacy information, and the benefits are not clear" (C2G2P2). Thus, a user's attitude to risk plays an important role in their acceptance.

As a consequence, 7 out of 10 participants in the second cluster of my study believed that Privacy Manager could play a useful role in their life and expressed their willingness to continue using it.

3.7 Conclusion and Future Research

This study has focused on privacy calculus for context-aware mobile applications and the role played by personalization and control in the design of a context-aware mobile application to protect users' personal information. The focus group investigation provided with new insights into privacy calculus in the mobile context, and how personalization and control over information can influence it.

Based on focus group interviews, the findings provided strong support for Smith et al.'s (1996) four key factors of individual privacy concerns in the mobile context. In addition, this study found three new dimensions of mobile user privacy concerns: (1) legal considerations, (2) reputation considerations and (3) information release agreements.

Moreover, the results show the important roles played by personalization and control over personal information in the privacy calculus carried out by a smartphone user.

Finally, I introduced a new context-aware mobile application, which takes into account privacy concerns, personalization and data control. I also proved that the application is easy to use and is perceived as useful. In addition, a user's mobility and risk attitude have a strong influence on perceived usefulness. To conclude, Figure 3.5 outlines the design science research framework used in my research, which was based on Hevner et al. (2004).

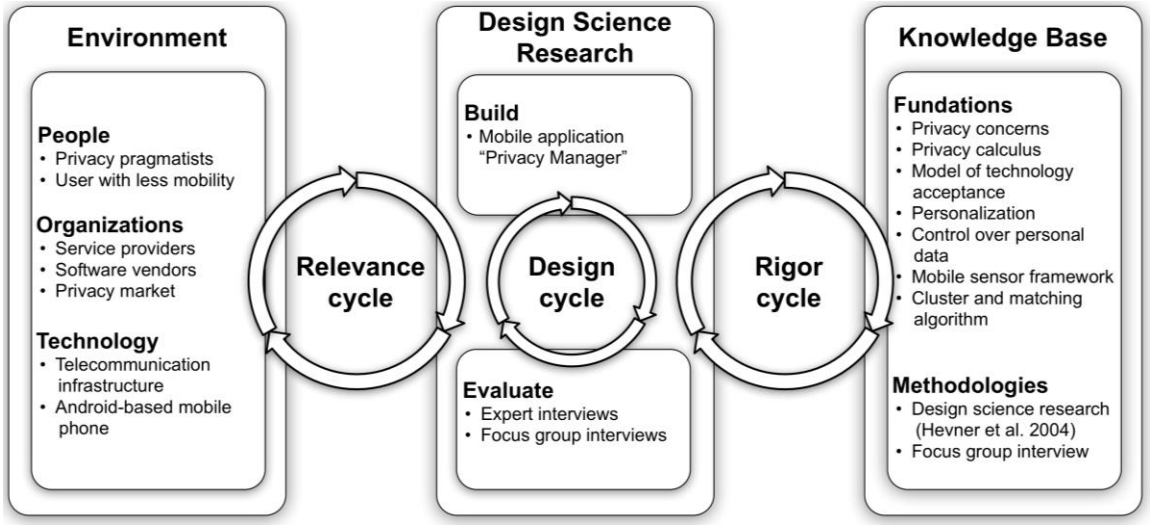


Figure 3.5. Design science research framework, adapted from Hevner et al. (2004)

Two important limitations should be taken into account prior to generalizing the results: (1) the common sample selection bias and (2) the common method bias. First, participants in this study tended to be young adults, and mobile users. Although I tried to recruit people from different backgrounds and different educational levels, the sample in this study is not really representative of the whole population. For example, all participants are from Switzerland, a country in which there is little chance of a phone being stolen. Second, while focus groups were a good way to achieve the research goal, individual interviews could also have been 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. Although my research was conducted in a real-life circumstance, it would be interesting to carry out a diary study or experience-sampling method, which would give the details of participants' situations when using my application. Finally, privacy concerns are application dependent, and that implies that the data collected in this study is only relevant to the application being tested. Therefore, future research could address privacy calculus through a larger quantitative study with a more representative and heterogeneous population.

3.8 References

Ajami, R., Qirim, N. A., and Ramadan, N. 2012. "Privacy Issues in Mobile Social Networks," *Procedia Computer Science* (10), pp. 672-679.

Ankolekar, A., Szabo, G., Luon, Y., Huberman, B. A., Wilkinson, D., and Wu, F. 2009. "Friendlee: a mobile application for your social life," In Proceedings of the 11th international Conference on Human-Computer interaction with Mobile Devices and Services, ACM, pp. 1-4.

Awad, N.F., and Krishnan, M.S. 2006. "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *Management Information Systems Quarterly* (30:1), pp. 13-28.

Barkhuus, L., and Dey, A. 2003. "Location-based services for mobile telephony: a study of users' privacy concerns," In Proceedings of the Interact, Zurich, pp. 709–712.

Benisch, M., Kelley, P.G., Sadeh, N., Sandholm, T., Tsai, J., Cranor, L. F., and Drielsma, P. H. 2008. "The impact of expressiveness on the effectiveness of privacy mechanisms for location-sharing," In Proceedings of the 5th Symposium on Usable Privacy and Security, ACM.

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

Bilogrevic, I., Jadliwala, M., Kumar, P., Walia, S. S., Hubaux, J-P., Aad, I., and Niemi, V. 2011. "Meetings through the cloud: Privacy-preserving scheduling on mobile devices," *Journal of Systems and Software* (84:11), pp. 1910-1927.

Bonazzi, R., Fritscher, B., Liu, Z., and Pigneur, Y. 2011. "From 'security for privacy' to 'privacy for security'," In Proceedings of the Third International Workshop on Business Models for Mobile Platforms, Berlin, IEEE, pp. 319-324.

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

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

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

Culnan, M. J., and Bies, R. J. 2003. "Consumer privacy: Balancing economic and justice considerations," *Journal of social issues* (59:2), pp. 323-342.

Culnan, M. J., and Milberg S. J. 1999. "Consumer privacy", In Information Privacy: Looking Forward, Looking Back, Culnan M. J., Bies, R. J., and Levy M. B. eds. Georgetown University Press.

Davidson, D. and Livshits, B. 2012. "MoRePriv: Mobile OS Support for Application Personalization and Privacy," Microsoft Research, 2012, 3 May.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User acceptance of computer technology: a comparison of two theoretical models," *Management science* (35:8), pp. 982-1003.

Davis, F. D. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *Management Information Systems Quarterly* (13:3), pp. 319-340.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy calculus model in e-commerce–a study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389-402.

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

Dinev, T. and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61-80.

Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. 2010. "TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones," In Proceedings of the 9th USENIX conference on Operating systems design and implementation, pp. 1-6.

Gaonkar, S., Li, J, Choudhury, R. R., Cox, L., and Schmidt, A. 2008. "Micro-Blog: Sharing and Querying Content through Mobile Phones and Social Participation," In Proceedings of the 6th international conference on Mobile systems, applications, and services, pp. 174-186.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in Online Shopping: An Integrated Model," *Management Information Systems Quarterly* (27:1), pp. 51-90.

Goodwin, C. 1991. “Privacy: Recognition of a consumer right,” *Journal of Public Policy and Marketing* (10:1), pp. 149-166.

Hevner, A., March, S., Park, J., and Ram, S. 2004. “Design Science in Information Systems Research,” *Management Information Systems Quarterly* (28:1), pp. 75-105.

Hoffman, D. L., Novak, T. P. and Peralta, M. A. 1999. “Information privacy in the marketspace: implications for the commercial uses of anonymity on the web,” *The Information Society* (15), pp. 129-139.

Hong, W. and Thong, J.Y. 2013. “Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies,” *Management Information Systems Quarterly* (37:1), pp. 275-298.

Hui, K.-L., Teo, H. H., and Lee, S.-Y. T. 2007. “The value of privacy assurance: an exploratory field experiment,” *Management Information Systems Quarterly* (31:1), pp. 19-33.

Junglas, I. A., Johnson, N. A., and Spitzmüller, C. 2008. “Personality traits and concern for privacy: an empirical study in the context of location-based services,” *European Journal of Information Systems* (17:4), pp. 387-402.

Kenteris, M., Gavalas, D., and Economou, D. 2009. “An innovative mobile electronic tourist guide application,” *Personal and ubiquitous computing* (13:2), pp. 103-118.

King, N. J., and Jessen, P. W. 2010. “Profiling the mobile customer–Privacy concerns when behavioural advertisers target mobile phones–Part I,” *Computer Law & Security Review* (26:5), pp. 455-478.

Kitzinger, J. 1995. “Qualitative research. Introducing focus groups,” *British medical journal* (311:7000), pp. 299.

Kobsa, A. 2007. “Privacy-enhanced personalization,” *Communications of the ACM* (50:8), pp. 24-33.

Lacey, A., and Luff, D. 2007. “Qualitative research analysis,” Sheffield: University of Sheffield.

Lee, C. H., and Cranage, D. A. 2011. “Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites,” *Tourism Management* (32:5), pp. 987-994.

Lee, D.-J., Ahnm J.-H., and Bang, Y. 2011. “Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection”, *Management Information Systems Quarterly* (35:2), pp. 423-444.

Liu, Z., Bonazzi, R., Fritscher, B., and Pigneur, Y. 2011. "Privacy-friendly business models for location-based mobile services," *Journal of theoretical and applied electronic commerce research* (6:2), pp. 90-107.

Maamar, Z., Kouadri, S., and Yahyaoui, H. 2004. "A web services composition approach based on software agents and context," In Proceedings of the 2004 ACM symposium on Applied computing, Nicosia, Cyprus, pp. 1619-1623.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research* (15:4), pp. 336-355.

Mallat, N. 2007. "Exploring consumer adoption of mobile payments–a qualitative study," *The Journal of Strategic Information Systems* (16:4), pp. 413-432.

March, S. T. and Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems* (15:4), pp. 251-266.

Marmasse, N. and Schmandt, C. 2000. "Location aware information delivery with ComMotion," In Proceedings of the 2nd international symposium on Handheld and Ubiquitous Computing, pp. 157-171.

Miluzzo, E., Lane, N. D., Fodor, K., Peterson, R., Lu, H., Musolesi, M., Eisenman, S. B., Zheng, X., and Campbell, A. T. 2008. "Sensing meets mobile social networks: the design, implementation and evaluation of the CenceMe application," In Proceedings of the 6th ACM conference on Embedded network sensor systems, pp. 337-350.

Mohan, P., Padmanabhan, V. N., and Ramjee, R. 2008. "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," In Proceedings of the 6th ACM conference on Embedded network sensor systems, pp. 323-336.

De Montjoye, Y.-A., Wang, S. S., Pentland, A. S. 2012. "On the Trusted Use of Large-Scale Personal Data," *IEEE Data Engineering Bulletin* (35:4), pp. 1-5.

Oliver, R. L. 1974. "Expectancy theory predictions of salesmen's performance," *Journal of Marketing Research* (11), pp. 243-253.

Peffers, K., Tuunanen, T., Rothenberger, M., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45-77.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing* (19:1), pp. 27-41.

Powell, R. A. and Single, H. M. 1996. "Focus groups," *International journal for quality in health care* (8:5), pp. 499-504.

Priyantha, N., Miu. A., Balakrishnan. H., and Teller, S. 2001. "The cricket compass for context-aware mobile applications," In Proceedings 6th ACM MOBICOM, Rome, Italy, pp. 1-14.

Raento, M., Oulasvirta, A., Petit, R., and Toivonen, H. 2005. "ContextPhone: A prototyping platform for context-aware mobile applications," *Pervasive Computing, IEEE* (4:2), pp. 51-59.

Roman, M., and Campbell, R. H. 2002. "A user-centric, resource-aware, context-sensitive, multi-device application framework for ubiquitous computing environments," Technical report, Department of Computer Science, University of Illinois at Urbana-Champaign.

Sadeh, N., Gandon, F., and Kwon, O. B. 2005. "Ambient intelligence: The MyCampus experience," Technical Report CMU-ISRI-05-123, Carnegie Mellon University, July 2005.

Sandhu, R. S., and Samarati, P. 1994. "Access control: principle and practice," *Communications Magazine, IEEE* (32:9), pp. 40-48.

Sheng, H., Nah, F. F.-H., and Siau, K. 2008. "An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns," *Journal of the Association for Information Systems* (9:6), pp. 344-376.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information privacy: measuring individuals' concerns about organizational practices," *Management Information Systems Quarterly* (20:2), pp. 167-196.

Sohn, T., Li, K. A., Lee, G., Smith, I., Scott, J., and Griswold W. G. 2005. "Place-its: A study of location-based reminders on mobile phones," In Proceedings of the Fifth International Conference on Ubiquitous Computing (UbiComp 2005), pp. 232-250.

Srivastava, A., and Thomson, S. B. 2009 "Framework analysis: a qualitative methodology for applied policy research," *Journal of Administration Governance* (4:2), pp. 72-79.

Stewart, K. A., and Segars, A. H. 2002. "An empirical examination of the concern for information privacy instrument," *Information Systems Research* (13:1), pp. 36-49.

Toch, E., Cranshaw, J., Hankes-Drielsma, P., Springfield, J., Kelley, P. G., Cranor, L., Hong, J., and Sadeh, N. 2010. "Locaccino: a privacy-centric location sharing application,"

In Proceedings of the 12th ACM international conference adjunct papers on Ubiquitous computing-Adjunct, pp. 381-382.

Turner, M., Kitchenham, B., Brereton, P., Charters, S. and Budgen, D. 2010. "Does the technology acceptance model predict actual use? A systematic literature review," *Information and Software Technology* (52:5), pp.463-479.

Venkatesh, V. 2000. "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information systems research* (11:4), pp. 342-365.

Venkatesh, V., and Davis, F. D. (2000). "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Fiend Studies," *Management Science* (46:2), pp. 186-204.

Ward, S., Bridges, K., and Chitty, B. 2005. "Do Incentives Matter? An Examination of On-line Privacy Concerns and Willingness to Provide Personal and Financial Information," Journal of Marketing Communications (11:1), pp. 21-40.

Whitley, E. A. 2009. "Information privacy, consent and the 'control' of personal data," *Information Security Technical Report* (14), pp. 154-159.

Xu, H., Luo, X.R., Carroll, J.M., and Rosson, M. B. 2011. "The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing," *Decision support systems* (51:1), pp. 42-52.

Xu, H. and Teo, H.-H. 2004. "Alleviating consumer's privacy concern in location-based services: A psychological control perspective," In Proceedings of the Twenty-Fifth International Conference on Information Systems, pp. 793-806.

Chapter 4

The Role of Personalized Services and Control: An Empirical Evaluation of Privacy Calculus and Technology Acceptance Model in Mobile Context

Abstract The last few years have witnessed an explosive growth in the use of smartphones. Such widespread use brings with it concerns over the protection of privacy. The purpose of this study is to better understand such privacy issues in a mobile context. Building upon existing privacy concern literature, this study has developed a theoretical framework that combines a privacy calculus model with a technology acceptance model in the mobile application context. Also examined is the role of personalized services and users' control over personal data in this domain. Based on a study of 308 participants, the results reveal that perceived enjoyment has replaced perceived ease-of-use as a main predictor of perceived behavioral intentions in a mobile TAM. The findings also showed that personalized services and users' control over personal data have a strong effect on both a privacy calculus and mobile TAM.

Keywords: Personalization, Control, Privacy concerns, Privacy calculus, Mobile TAM, Mobile context, Perceived enjoyment

4.1 Introduction

The recent explosive growth in information technology and digital networks, particularly the prominent growth in the popularity of smartphones and tablets, has fuelled the debate that surrounds the issue of privacy protection (Dhar and Varshney, 2011; Dinev and Hart, 2004; Keith et al., 2013). Unlike traditional market transactions, exchanges in the mobile context usually do not involve face-to-face interactions. Rather, the behavioral intentions of companies that collect personal data are not always clear to mobile users. A recent study conducted by Sutanto et al. (2013) indicated that smartphones such as iPhones and Android phones can secretly track user information; indeed, half of all iPhone applications are capable of so doing. As a result, concerns over information privacy have become a real issue in m-commerce. In particular, they have attracted the attention of information system researchers.

Information privacy usually refers to the interest that people have in controlling, or at least significantly influencing, the handling of information about themselves (Belanger and Crossler, 2011; Clarke, 1999). As e-commerce and more recently m-commerce continue to grow worldwide, companies collect increasingly large amounts of personal information from Internet and mobile users. This consumer data is then used to develop more efficient and effective marketing strategies. To build these databases, however, customers are required to share their personal information with companies, whether voluntarily or involuntarily (Graeff and Harmon, 2002; Nam et al., 2006). In fact, consumers can reasonably expect to have to provide companies with a certain level of personal purchase information in order to enjoy individualized and personalized transactions. New advances in tracking technologies in m-commerce enable marketers to construct personal profiles and use them to tailor their advertising messages for mobile users even more precisely than for other online customers (King and Jessen, 2010).

The majority of research has been based on online commercial exchanges. As such, it has not examined whether such operations give rise to the same consumer privacy concerns as transactions that take place in the mobile context. From both theoretical and practical perspectives, it is important to better understand the personalization-privacy paradox in the context of mobile activities, because Internet use in general might not completely reveal the perceptions and attitudes that are associated with the use of different smartphone applications.

Thus, the purpose of this paper is to examine the relationship between beliefs about information privacy and mobile application usage intentions. Specifically, *how do mobile users perceive information privacy when using location-based applications, and how do such perceptions affect their intention to use these applications?* Moreover, in this paper,

I will also consider the possible impacts of users' control over the release of private information and the personalized services provided by applications in these relationships.

To answer these questions, I established a theoretical model that is based on both a privacy calculus and technology acceptance model. More importantly, it incorporates personalization and control over personal information as two important factors on both models. On the one hand, therefore, I aim to examine whether the personalized characteristics of mobile applications would meet users' personal needs more effectively, leading to more positive results (i.e., increased perceived benefit). On the other hand, I intend to demonstrate whether control over personal information can promote users' psychological comfort (i.e., reduced perceived risks) and thus increase their willingness to disclose data, and whether such a solution would also impact on their intention to use mobile applications.

The rest of this paper is organized thus: the next section provide a theoretical foundation and offer hypothesis development for this research. A methodology section is then presented, which describes the data collection process and sample taken, and reports on the testing of my hypotheses. Following a discussion of the main findings and implications, I report its contribution and limitations. Finally, this paper concludes with a brief summary.

4.2 Theoretical Model and Hypothesis Development

4.2.1 Information Privacy and Privacy Concerns

Before moving to the proposed model, it is important to first take a step back and examine what I mean by the term "privacy". The concept of privacy is not new. According to Graeff and Harmon (2002), legal opinion on the right to privacy can be seen to date back to the late nineteenth century. In recent years, the notion of privacy has been widely studied in different disciplines, from psychology and sociology to law and information systems. However, due to its multidimensional nature, it is difficult to find a generally accepted definition across all disciplines. Privacy is usually regarded as an important human right (e.g., Dinev and Hart, 2006b; Goodwin, 1991; Whitley, 2009). Although usually contextually dependent (i.e., Sheng et al., 2008), people place a high value on privacy as an expression of their dignity. Some researchers have treated privacy as a "commodity". From this perspective, privacy is subject to the economic principles of cost-benefit analysis and trade-off (Smith et al., 2011). In the current study, I have adopted the economic perspective of information privacy, and have defined it as "the

interest people have in controlling, or at least significantly influencing, the handling of information about themselves" (Bélanger and Crossler, 2011, p.1018).

Information privacy concerns refer to an individual's subjective concerns within the context of information privacy (Malhotra et al., 2004). Such concerns have often been cited as one of the key reasons for consumers failing to make purchases over the Internet (George, 2004). For example, in a BUSINESS WEEK/Harris poll carried out in early 1998, the majority of the 999 respondents pointed to privacy as the main reason for not using a website – above cost, ease of use, and the morass of unwanted marketing messages (Green et al., 1998). These respondents further expressed a view that such privacy concerns could, in turn, affect their decision to make online purchases. Ackerman (2004) pointed out that it is not only current business practices, but also consumer fears and media pressure, that combine to make consumers seriously concerned about their privacy.

Smith et al. (1996) identified four kinds of information privacy concerns. First, people are concerned about personal information being collected and stored. Second, people are concerned about the risk of unauthorized secondary use. In other words, the information is collected from individuals for one purpose, but it is reused for another purpose – either internally within a single organization or externally with a third party – without authorization from the individuals. Third, people have a general anxiety about improper access. Finally, they are also concerned about errors in their personal data. Hong and Thong (2013) raised two dimensions: control and awareness. People are concerned whether they have adequate control over their personal information, and they are also worried about their awareness of information privacy practices. In a more recent study, Liu et al. (2014) confirmed that these four types of privacy concerns also prevail in the mobile context. In addition, they raised three additional considerations: agreement on information releasing, reputation consideration and legal consideration. While the first two elements are associated more with the organizational perspective, the last one takes a regulation and governmental policy perspective.

According to multidimensional developmental theory (Laufer and Wolfe, 1977), an individual's perception of privacy concerns can be described as a multidimensional concept that results from self-development, environmental impact and interpersonal interactions. Self-development and environmental impact focus more on external impacts that occur over time, such as cultural, social and physical settings. On the other hand, interpersonal interaction, which constitutes the core of privacy perception, focuses on the relationships between an individual and others (Hong and Thong, 2013). In the context of m-commerce, interpersonal interaction can be typically viewed as a dyadic relationship between a mobile phone user and a mobile service provider (e.g., application developer).

It is also important to note that individuals view privacy problems differently. An individual's perception of privacy concerns may be influenced by both external conditions, as described in multidimensional development theory, and internal reasons, such as an individual's personal characteristics and past experiences (Malhotra et al., 2004). For example, Campbell (1997) argued that in markets that are relatively undeveloped in terms of direct marketing, where consumers may have insufficient experience and knowledge of marketing, concerns about information privacy were likely to be lower. Bansal et al. (2010) also documented that some personal traits (e.g., emotional instability) and prior personal negative experiences of personal information disclosure might also significantly increase consumers' information privacy concerns.

Similarly, Ackerman (2004) argued that the differences in consumers' privacy concerns came from two main sources: types of concerns, and degree of concerns among people. Consumers are not one homogenous group; rather, they hold very different opinions on privacy concerns. For example, some people might be indifferent to privacy, while some are extremely uncompromising. Ackerman et al. (1999) labelled these two groups as marginally concerned and privacy fundamentalist; in between the two, he saw a third group known as the pragmatic majority. The pragmatists make up the largest group. Thus, Sheehan (2002) further divided them into two groups, based on the extent of their privacy concerns: circumspect Internet users and wary Internet users. The former have fewer total concerns than the latter. Spiekermann et al. (2001) separated the pragmatic majority identified by Ackerman et al. (1999) into two distinct groups according to the focus of their different privacy concerns. Those in the first group have "identity concerns", focusing on the revelation of identity aspects such as name, address or email. The second group is "profiling averse", and are more concerned with the profiling of their interests, hobbies, health and other personal information. In all these studies, different groups showed significantly different degrees of concern over the potential disclosure of personal data in online situations such as e-commerce.

Privacy concerns might affect behaviors. In a recent study, Bandyopadhyay (2012) identified three possible outcomes of online privacy concerns. Individual information is often asked when consumers are required to register to a website prior to using content. In this situation, consumers who are concerned about their online privacy are more likely to be unwilling to disclose personal information, or provide limited or false personal information to a website (Dinev and Hart, 2007; Nam et al., 2006). Even in cases where consumers do not voluntarily submit any personal information to a website, information may still be exchanged between a consumer's client computer and the website's host server. As a consequence, consumers who are very concerned about protecting their privacy online may reduce their participation in e-commerce transactions. In some extreme cases, they may be unwilling to use the Internet. In other words, users may inhibit their Internet or mobile usage, or develop an aversion to experimenting with new

applications or services (Dinev and Hart, 2007). In the next section, I will consider the cost-benefit trade-off, or privacy calculus, in determining an individual's behavioral reaction.

4.2.2 Privacy Calculus

Prior studies on information privacy have repeatedly found that individuals are willing to disclose personal information in exchange for some economic or social benefit (e.g., Dinev and Hart, 2006a; Keith et al., 2013). This leads to a risk-benefit trade-off analysis, or a privacy calculus; in other words, a determination about whether to disclose information after weighing factors related to how that information will be used (Dinev and Hart, 2007). Keith et al. (2013) argued that it is a "rational theory that seeks to explain the attitudes, beliefs, intentions, and behaviors of IT consumers when the use of the IT includes the cost of a perceived privacy risk" (p.1165).

According to privacy calculus, a user's intention to disclose information depends on two key concepts: perceived risks and perceived benefits. In particular, a user's behavioral intentions and subsequent actions are not only positively affected by expected benefits; they are also negatively affected by the anticipated cost of a potential privacy invasion. This is consistent with expectancy theory, where individuals should behave in ways that maximize positive outcomes (i.e., monetary or non-monetary benefits) and minimize negative outcomes (i.e., risks and its consequences) (Dinev and Hart, 2006a). Culnan and Bies (2003) have described this self-disclosure as a "balancing test", because people disclose their information to gain the benefits of a relationship, and such benefits are somehow balanced against an assessment of the risks of disclosure. Similarly, Culnan and Armstrong (1999) have considered the dyadic relationship between an individual and company as a "social contract"; thus, to curtail an existing relationship with a company involves a switching cost. Consequently, consumers will continue to participate in this social contract as long as the perceived benefits exceed the perceived risks.

The anticipation of benefits is expected to have a positive influence on an individual's intention to disclose personal information. Such benefit may be either monetary or non-monetary. For instance, in their study, Hann et al. (2002) provided evidence that individuals were willing to trade off privacy concerns for economic returns. Phelps et al. (2000) found that direct marketing consumers were willing to exchange personal information for shopping benefits such as future shopping time and effort savings. White (2004) proved that customized marketer benefit offerings are related to a greater willingness to reveal information that is associated with a potential loss of privacy. In the context of e-commerce and m-commerce, empirical results reached a similar conclusion. For example, Nam et al. (2006) found that Internet users tend to feel more secure and safe with websites that they perceive to be more comfortable, convenient and easy to use. In

turn, this positively affects a user's intention to disclose information. Xu et al. (2010) identified two anticipated benefits in using a location-based service (LBS), locatability and personalization, both of which could amplify a user's desire to engage in a LBS transaction.

Expected potential risk, on the other hand, is predicted to be negatively related to the intention to disclose personal information. A number of studies have examined the risk as an antecedent to intentions to conduct transactions (e.g., Dinev and Hart, 2006a, Dinev et al., 2006b; Malhotra et al., 2004). In fact, risks are everywhere. They exist just as much in conventional high street commerce. For example, when a consumer buys a product, a certain amount of risk about the quality of that product is involved. Such a risk may increase if the consumer is not familiar with the product brand. However, the more information technology has come to be used to facilitate transactions, the greater is the risk associated with the disclosure of personal information (Dinev and Hart, 2006a). In the context of the mobile world, where so-called LBS can pinpoint the whereabouts of mobile users, the threat to individual privacy assumes even greater significance. The uniqueness of LBS and its real-time location data nature has led to predictions that it will become the "killer application" of mobile commerce (Junglas and Watson, 2008). However, the use of LBS to continuously collect and utilize users' real-time location data means that privacy risks will persist, with a wide range of threats, from simple annoyance to outright personal danger (Keith et al., 2013).

Some researchers have examined the intentions of users to disclose information from a perceived justice (or fair information practice) perspective (e.g., Culnan and Bies, 2003; Xu et al., 2010). For example, Culnan and Armstrong (1999) argued that companies that establish fair information practice and disclose these practices before collecting personal information from online customers are greatly reducing their perceived risks. Moreover, if an individual's personal information is used in ways that are compatible with their understanding of how it will be used, individual customers will be more willing to continue in a relationship with a company. Xu et al. (2010) drew on justice theory to examine the effects of three privacy-related interventions on the disclosure intentions of mobile users. These interventions include compensation, which represents distributive justice, and industry self-regulation and government regulation, which represent the procedural justice.

The willingness of individuals to provide a company with information may also depend on other factors, such as the type of information requested, personal traits, and trust. For example, Phelps et al. (2000) indicated that direct marketing consumers are more willing to provide marketers with demographic and lifestyle information than with financial, purchase-related, and personal identifier information. In the same vein, Meinert et al. (2006) found that, in an e-commerce context, people are more willing to provide contact

information rather than biographical information, and biographical rather than financial information. Bansal et al. (2010) noted that personality traits have a significant effect on online health information disclosure. Junglas et al., (2008) also drew similar conclusions with regard to the behaviors of LBS users. They assumed that trust plays a crucial role in the reduction of consumers' privacy concerns and in improving relationships between consumers and companies in an e-commerce context (e.g., Tamimi and Sebastianelli, 2007; Wu et al., 2012). Such trust could be built through improved interface design for e-commerce transactions (e.g., Wang and Emurian, 2005), public policy statements (e.g., Meinert, et al., 2006; Miyazaki and Krishnamurthy, 2002), or consumers' perceptions of trustworthiness (B đanger et al., 2002).

Unfortunately, with few exceptions (e.g., Keith et al., 2013; Xu et al., 2010), there is a distinct lack of relevant studies. Thus, it is particularly timely that I seek to gain a better understanding of information disclosure in the context of mobile applications. In the present study, I do not formally hypothesize the privacy calculus-based relationship, as it has been widely tested in previous studies. My emphasis is on the role of personalization and control over personal data, and on individuals' disclosure intentions, whether or not through a change in perceived risks or perceived benefits.

4.2.3 Technology Acceptance Model and M-Commerce

In the same way that a website offers online purchasing, a smartphone can act as a mobile computer; in essence, it is a form of information technology. As a result, individuals' intentions to use products and service via mobiles can be explained in part, if not fully, by the technology acceptance model (Davis 1989; Davis et al., 1989). This model provides sound predictions of usage by linking behaviors to attitudes and beliefs. It asserts that the intention to use and actual use of an information system are primarily dependent on two particular beliefs: perceived usefulness and perceived ease-of-use (see Figure 4.1). Perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p.320) and perceived ease of use refers to "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989, p.320). In addition, TAM theory proposes that the latter positively influences the front construct.

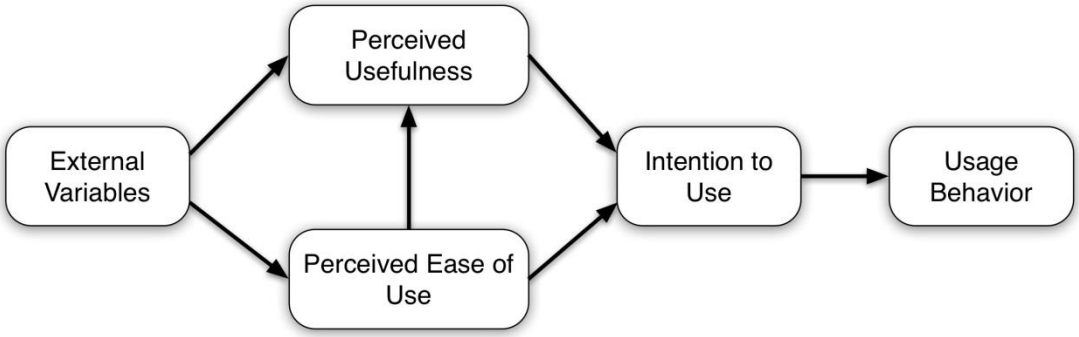


Figure 4.1. Technology acceptance model (TAM, Davis, 1989; Davis et al., 1989)

Since its inception, the TAM has been widely applied to a diverse set of information technologies and users, and a body of empirical research has supported its propositions (e.g., Adams et al., 1992; Gefen et al., 2003; Van der Heijden, 2004; Venkatesh and Davis, 2000). Across these empirical tests, perceived usefulness has consistently been a strong determinant of usage intentions (the regression coefficients are typically around 0.6), with a weaker effect of another important determinant - perceived ease-of-use. However, some recent evidence has shown that, in other contexts, applying the TAM may have the opposite effect (e.g., Ven der Heijden, 2004).

A smartphone, however, is more than just an IT interface. In mobile commerce, typically in a location-based service environment, users are more engaged. They generally get such benefits as LBS resources, discount coupons or monetary awards from a company or service provider by disclosing their location with a certain degree of accuracy (Chorppath and Alpcan, 2013). At the same time, however, disclosing location information brings huge risks for individuals, as a mobile device is more personal than a desktop computer and can possibly be shared with others. Consequently, mobile users have to compromise their privacy in order to bring user experience benefits. Moreover, mobile devices also store additional personal information, such as personal contacts, sent or received messages, emails, photos, and other information. Many mobile applications can automatically access and collect such information, which personally identifies an individual. Consequently, they can use this information for other purposes. Thus, a smartphone is not usually seen as a trustworthy and reliable source of product and service information; indeed, in this respect, it is similar to traditional sources, such as TV and print media.

Furthermore, scholars have extended the original TAM to other areas, such as hedonic information systems (e.g., van der Heijden, 2004), online shopping (e.g., Gefen et al., 2003), a consumer context (e.g., Venkatesh et al., 2012), an e-service context (e.g., Xu et al., 2013), and newly developed mobile applications (e.g., Liu et al., 2014). Among those

extended models, perceived enjoyment (sometimes called hedonic motivation) appears to be an important determinant of behavioral intention and perceived ease of use. Unlike perceived usefulness, which focuses on extrinsic motivation, perceived enjoyment focuses on intrinsic motivation (van der Heijden, 2004). It specifies the degree to which fun can be derived through the use of technology or a particular service (Xu et al., 2013). Given the hedonic aspects of mobile-based applications and services, it is appropriate to capture a hedonic perspective in addition to a utilitarian one (perceived usefulness).

Based on the previous findings, I put forward the idea that, in addition to the original two main predictor variables of the TAM (perceived usefulness and perceived ease-of-use), perceived enjoyment has been playing an increasingly important role in voluntary mobile usage situations. Thus, in this study, I have also included the mobile TAM context. I am now in a position to propose the first set of hypotheses as follows:

> *Hypothesis 1a: The level of perceived usefulness is positively related to mobile user's intention to use.*
>
> *Hypothesis 1b: The level of perceived ease-of-use is positively related to mobile user's intention to use.*
>
> *Hypothesis 1c: The level of perceived enjoyment is positively related to mobile user's intention to use.*
>
> *Hypothesis 1d: The level of perceived ease-of-use is positively related to mobile user's perceived usefulness.*

Although the previous literature has shown that perceived usefulness and perceived ease of use as a primarily determinants in the behavioral usage intention, privacy calculus can also influence, especially for LBS mobile applications where user's contextual information is collected. Some previous studies have documented that user's willingness to disclose personal information could be explained by reference to a trust relationship with the consumers (Anderson and Agarwal, 2011; Dinev and Hart, 2006). A higher level of willingness to provide personal information, therefore, indicates a trustable relationship between users and application provider, or users had already established a relationship. In other words, users who are more willing to provide personal information are more likely to trust the application or they have already used the application. Moreover, research found that consumers indicated a willingness to provide information in exchange for some benefits and interests such as conveniences and time savings (e.g., Phelps et al., 2000; Dinev and Hart, 2006). These findings suggested that mobile users willingly to provide their information because they wanted to enjoy the benefit of certain application, indicating their intentions in continuing to use of the application.

By linking a privacy calculus and the mobile TAM, I am able to propose that users' willingness to disclose data has a strong positive effect on users' intentions to use mobile applications. Thus,

> *Hypothesis 2: The level of a user's willingness to share or disclose data is positively related to mobile user's intention to use.*

4.2.4 The Effect of Personalization

Personalization can be defined as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumer based upon their personal and preference information" (Chellappa and Sin, 2005). Although this definition has its basis in an online setting, a common theme can also be found in the context of the mobile world: personalization is adaptive (Sheng et al., 2008). In particular, it is an interactive process in which a service provider offers relevant customized content based on consumer's individual preferences.

Therefore, personalization is critically dependent on two factors: the ability of firms to acquire and process consumer information, and consumers' willingness to share information and use personalization services (Chellappa and Sin, 2005). From a company's perspective, improvements in personalized services would increase customer satisfaction levels and customers' intentions to repurchase. In turn, this would result in improved company profitability (Kim and Lee, 2009). Today's advancements in networks, applications and devices in the m-commerce environment mean that an enormous amount of information, including real-time data, will become available to service providers. As a consequence, the ability of firms to provide individual care and attention, including personalization, has become a key competitive necessity.

From the customer's point of view, there are two sides to personalization. First, personalization affects information processing and the decision outcomes of customers (Tam and Ho, 2006). With the plethora of choices available in today's business environment, customers are willing to benefit from any tailored information (e.g., advertisement) and services in order to receive potential cost savings (e.g., searching cost). In the m-commerce context, mobile customers disclose their personal information in return for something that has a contextualization value, such as promotional information that is based on their interests, activities, identity, location and the time of the day (Dey and Abowd, 2000; Junglas and Watson, 2006). From a purely monetary perspective, personalized services are offered for "free". Second, personalization is gained only in cases when customers have provided their personal information and location data. Existing social behaviors literature has shown that consumers incur privacy costs when they directly or indirectly provide personal information to a company. There

is no precise value to such a social exchange (Awad and Krishnan, 2006); however, there is a kind of trade-off between personalization and loss of privacy. Some researchers call this dilemma a personalization-privacy paradox (e.g., Sheng et al., 2008; Sutanto, et al., 2013; Xu et al., 2011).

It has been suggested by prior studies that consumers engage in a cost-benefit analysis when they trade the privacy costs associated with sharing information against the values obtained from personalized information and services (e.g., Chellappa and Sin, 2005; Dinev and Hart, 2006a; Hann et al., 2002; Hann et al., 2007; Xu et al., 2011). Personalization has been found to be positively associated with perceived benefit. Consequently, it can lead to a higher level of intention to use personalized services, and can influence actual future behaviors. For example, based on a survey of 387 online bookstore users, Liang et al. (2012) reported that personalized customer services can generate higher perceived usefulness compared with non-personalized ones. From a mobile location-awareness marketing perspective, Xu et al. (2011) found that personalization approaches can influence the way individuals calculate the utility gained by disclosing personal information; in other words, personalization can somehow override privacy concerns. Focusing on mobile advertising, a recent study conducted by Sutanto et al. (2013) concluded that personalized and privacy-safe applications engaged in higher levels of application usage behavior. Awad and Krishnan (2006) distinguished between two personalization outcome contexts: personalized services and personalized advertising. They argued that consumers are more likely to assign a greater benefit value to online services and would be more willing to partake in online personalization in this case. In the current study, I focus on personalized services where the benefits are more apparent to consumers.

Although most of these studies have addressed personalization and privacy issues in the online setting, several of their conclusions could be extended to the mobile arena. Therefore, I have chosen to examine the presence of personalized factors in the usage of mobile services (i.e., perceived benefit and hence willingness to provide information), as well as their direct (i.e., intention to use) and indirect effects (i.e., perceived ease-of-use and perceived usefulness) on a mobile user's decision to use these services.

Hypothesis 3a: The level of personalized service is positively related to mobile user's perceived benefit.

Hypothesis 3b: The level of personalized service is positively related to mobile user's perceived risk.

Hypothesis 3c: The level of personalized service is positively related to mobile user's perceived ease-of-use of a mobile application.

Hypothesis 3d: The level of personalized service is positively related to mobile user's perceived usefulness of a mobile application.

Hypothesis 3e: The level of personalized service is positively related to mobile user's perceived enjoyment of a mobile application.

Hypothesis 3f: The level of personalized service is positively related to mobile user's intention to use a mobile application.

4.2.5 The Effect of Control over Personal Data

When a consumer chooses to enter into a relationship with a company, he or she must first be convinced that it is in their best interest to do so (Chen and Rea, Jr. 2004). At the point when a consumer's personal information (e.g., mailing list) is sold to a third party, the relationship between that consumer's original interests and the company's interest changes. In particular, it may become more tenuous. In this case, the consumer may not be interested in the relationship with the third party because they may not share any of the profit from that transaction (Varian, 1996). Nevertheless, from an economic perspective, such costs could be somehow mitigated if the individual has "a voice" in the transaction (Varian, 1996). In other words, if the consumer is able to choose whether or not to sell his or her information to the third party (e.g., the consumer may be interested in selling information to a third party which could then send him/her useful information), they may be less likely to worry about information privacy.

The case mentioned above relates to the avoidance of unwanted persons or contact during an interaction. Goodwin (1991) defined this type of control as "control over unwanted presence in the environment" (p.151). In a consumer context, when individuals provide personal information to a company, people should have the right to know why the information is collected, its expected uses, and any means of reuse elsewhere. However, the unwanted presence of others is not so easy to control. Xu (2010) drew upon a study by Yamaguchi (2001), proposing that consumers be able to exercise personal control or proxy control over their personal information via technology, industry self-regulation and government regulation in a location-based service context. In reality, however, most companies lack privacy policy creation and implementation (Chen and Rea, Jr. 2004). As a result, consumers must rely on personal controls. In addition to privacy-enhancing technology, as suggested by Xu (2010), consumers may develop mechanisms to protect their information privacy by directly controlling the flow of their personal information to others. This can take place in three ways (Chen and Rea, Jr. 2004): (1) falsification of a user's personal information; (2) passive reaction, by which a user ignores or employs a simple mechanism to block another person's presence; and (3) identity modification, whereby a user alters his or her identifications. It should be noted, however, that all three

control techniques would hamper the development of online business. In the present study, I have assumed that users rely on technology solutions, meaning that users have the ability to determine what information to share, with whom they will share it, and how to control its dissemination.

More generally, research has shown that the ability of consumers to take control of their personal data to some extent offsets the risk of possible negative consequences (Dinev & Hart, 2004; Stewart and Segars, 2002). Internet customers tend to think that information disclosure is less invasive, and less likely to lead to negative consequences when they can control when and how their information is disclosed and used in the future (Bandyopadhyay, 2012; Dinev and Hart, 2004; Malhotra et al., 2004). Such a belief could easily extend to customers' attitudes to mobile applications. In fact, privacy concerns become particularly salient in the mobile context because a mobile phone is rather personal, and could potentially be associated with a consumer's lifestyle habits, behaviors, and movement (King et al., 2010; Xu, 2010). Researches in this domain have also reported similar findings (e.g., Christin et al., 2013; Xu, 2010). As a consequence, mobile users' perceived risks are likely to be reduced in cases when they believe they have ability to take control of their disclosed personal data. This leads them to disclose more personal information. Therefore I propose the following:

Hypothesis 4a: The level of control ability over mobile user's personal information is negatively related to his/her perceived risk.

Hypothesis 4b: The level of control ability over mobile user's personal information is positively related to his/her willingness to provide information.

Hypothesis 4c: The level of control ability over mobile user's personal information is positively related to his/her intention to use.

4.2.6 Control Variables

To account for other influences on the core dependent variable, I have included a robust set of controls in the research model.

Despite the rapid growth of smartphone use in our society, some people still choose to avoid them because they feel anxious about using mobile technologies. Mobile technology anxiety is a technology-oriented individual difference that provides insight into the impact of consumers' general concerns about mobile technology on information privacy. Individuals who experience low levels of smartphone anxiety are likely to behave more comfortably around mobile applications. Users' mobile technology anxiety

can directly influence their intention to use mobile applications. Thus, I have included it as a control variable.

Furthermore, previous studies have shown that personal characteristics, such as personal innovation, are likely to affect mobile application usage level (Xu et al., 2011). Personal innovation refers to the degree to which an individual is receptive to new ideas and new technologies (Venkatesh et al., 2012). When a new application is released, mobile users may use it simply for the novelty value. Therefore, personal innovation may positively affect an individual's behavioral intentions. Thus, I have included it in the research model.

In addition, previous studies (e.g., Chen et al., 2013; Kuo et al. 2007; Nosko et al., 2012) have consistently shown that demographic differences such as gender and age have a strong impact on information privacy concerns. Overall, male consumers exhibit fewer privacy concerns than female consumers when using the Internet to purchase products (Graeff and Harmon, 2002; Wills and Zeljkovic, 2011). Young Internet users tend to have positive views on the collection of personal information for marketing purposes (Gervey and Lin, 2000). A related study conducted by Graeff and Harmon (2002) also found that older consumers are less likely to feel that companies should be able to sell customer information. This indicates a relatively low level of willingness to disclose personal data among older consumers. Thus, gender and age have also been included in this model.

4.2.7 Theoretical Model

To summarize, all the constructs and related hypotheses are indicated in Figure 4.2.

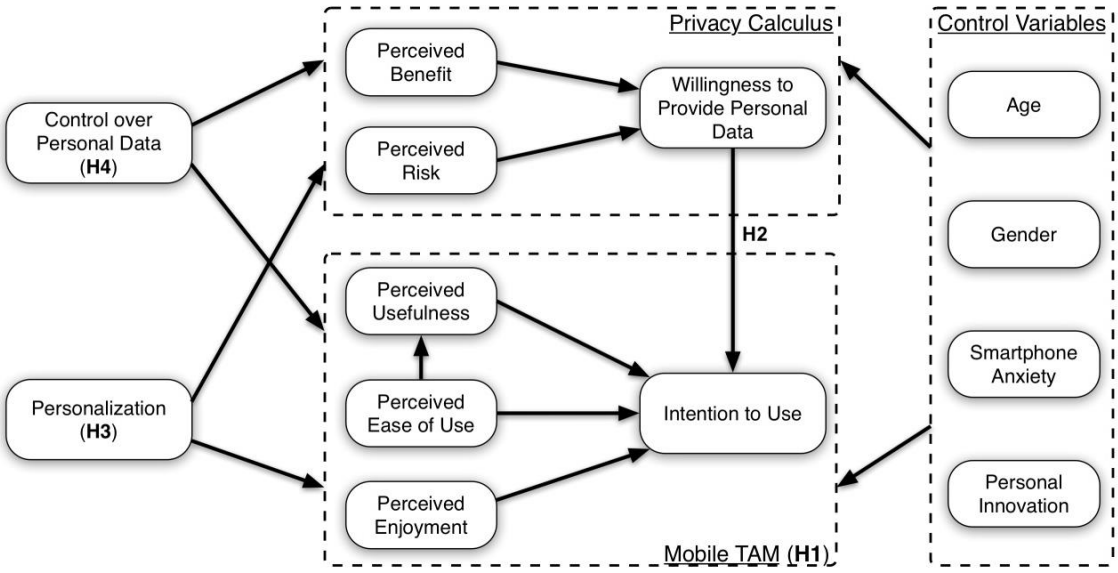


Figure 4.2. Theoretical model

4.3 Methodology

The purpose of this study is to understand the mobile TAM and consumer privacy calculus, taking into consideration control of personal data and personalization. In this thesis, I have sought to identify the factors that have the greatest explanatory power.

4.3.1 Sample

A total of 308 participants volunteered to participate in the study. As an incentive to participate, volunteers were given an opportunity to enter a lottery to win a Samsung Galaxy S4. In total, 308 people took part in the study: 204 of these were males and 104 were females. All subjects ranged in age between 18 and 58 years, with an average age of 30.8 years. Among the participants, 77.3% indicated that they were familiar with smartphones (score above 4), and 58.5% indicated that they were familiar with LBS mobile applications (score above 4). Table 4.1 gives a summary of the demographic characteristics of the respondents.

Table 4.1. Respondents' demographics (n=308)

	Number	Percentage
Gender		
Male	204	66.2%
Female	104	33.8%
Age		
under 20	32	10.4%
21-25	85	27.6%
26-30	37	12.0%
31-35	50	16.2%
36-40	43	14.0%
41-49	47	15.3%
50 and over	14	4.5%
	Mean	Std.
Familiar with Smartphone	5.5	1.59
Familiar with LBS application	4.5	1.72

Bélanger and Crossler (2011) based their work on a review of 500 papers that examine information privacy research in Information Systems. They argued that studies that rely heavily on student-based samples may result in findings of limited generalizability. The

sample of participants does not only focus on students; rather, it also includes diverse profiles of potential users from various occupational fields. Thus, I consider the results of this study to have adequate generalizability.

4.3.2 Procedure

The initial questionnaire was reviewed by two experts: one male from an information system background and one female from a marketing background. It was then distributed to 10 mobile users who were familiar with smartphone and social applications. These two pilot studies have two objectives: first, to clarify the scenarios described and the questions included in the survey; and second, to ensure that the experiment is well planned and effectively executed. An analysis of their feedback revealed that the respondents found some descriptions in the scenarios were unnecessary; these were removed, and several revisions to items on the questionnaire were made.

Each participant was asked to answer the questionnaire with LimeSurvey online. All percipients were told that there were no right or wrong answers. The response time was recorded. It took an average of 15-20 minutes to complete, including reading the survey instructions, the scenarios, and completion of the questions.

The final survey comprised three parts: (1) socio-demographic characteristics, to measure age, gender, and country of the origin; (2) a general question, to measure subjects' privacy concerns, technology anxiety and innovation, and their knowledge of smartphone and location-based mobile applications; and (3) a description of a scenario and questions based on the scenario, which formed the main body of this study and were designed to measure key variables in the model.

With a few exceptions (which will be discussed in section 4.3.3), respondents were asked to use a seven-point scale, from 1 (strongly disagree) to 7 (strongly agree) to describe their perceptions regarding a statement of the relevant variable. In order to minimize possible ordering effects of questions to subjects, some questions were reverse scored and questions in scenarios were randomly ordered.

Experimental manipulations were checked in two stages. First, I discounted data from participants who spent less than 10 seconds on reading the scenario descriptions. Second, at the end of the questionnaire, respondents were asked to state the name of the mobile application for manipulation check purposes. Of the 340 total questionnaires, 32 were removed from the final sample, as they failed to answer this question. These manipulation checks resulted in a final sample of 308 usable and valid responses.

4.3.3 Measurement

This study primarily used a scenario-based survey to address the perceptions of mobile users of privacy calculus and their attitude to mobile technology acceptance. One mobile social application called "Check Me In" was described in the scenarios:

> *Assume that you have installed a new application called "Check Me In" on your mobile phone. It is a geographical location based social network that allows you to post your location at a restaurant or a bar ("checking in") and connect with your friends.*
>
> *You can now see where your friends check in, explore restaurants you haven't yet visited and monitor popular destinations. Moreover, points and badges are awarded for checking in at various restaurants. For example, if you have checked in a certain restaurant for the first time, you will earn a "newbie" badge. If you have checked in a certain amount of times in a given period at a certain restaurant, you will be honored as "VIP". Special deals (e.g., a free drink or 10% discount of the meal) from that restaurant will be offered to you.*

The main independent variables in this study are personalization and control over personal data. Thus, I designed 2X2 scenarios: (A) a situation that has both a low level of personalization and control over personal data; (B) a situation that has a high level of personalization but a low level of control over personal data; (C) a situation that has a low level of personalization but a high level of control over personal data; and (D) a situation that has both a high level of personalization and a high level of control over personal data.

The measures used in this study were mainly adapted from relevant prior studies (Davis, 1989; Venkatesh, 2000; Xu et al., 2010; Xu et al., 2011). Willingness to disclose data was assessed by a single question adapted from Culnan and Armstrong (1999): how likely would you be to provide your personal information (including your location) when using "Check Me In"? Otherwise, multi-item measures were established for the following variables:

> *Both Perceived benefits* (BENEFIT, 4 items) and *Perceived risks* (RISK, 3 items) were measured using questions adapted from Xu et al. (2010). Thus I adopted the definition of perceived risks as: "the expectation of losses associated with the release of personal information to the service provider" (p.149)
>
> *Perceived ease-of-use* (EASE): was assessed on the basis of four items taken from Venkatesh (2000).

Perceived enjoyment (ENJOYMENT): was measured using a basis of three items adapted from Venkatesh et al (2012).

Perceived usefulness (USEFULNESS): I did not adopt the original TAM scales for perceived usefulness as in this case "improved job performance", for instance, might be an inappropriate outcome of using the social mobile application. For this reason, I developed new items that preserve the utilitarian nature of the scale.

Intention to use (INTENTION): was measured by 4 items, of which 2 items were taken and adapted from Venkatesh (2000). The other 2 new items were developed specially for this study.

Personal innovation (INNOVATION): was assessed using three items taken from Xu et al. (2011).

Smartphone anxiety (ANXIETY): was based on six items taken from a study by Venkatesh (2000). The original measure was computer anxiety. To meet the required thresholds, we had to delete "it would not bother me to take smartphone courses", a factor loading analysis that was revealed during this study.

The items for all the measures are listed in the Appendix of this chapter.

4.4 Results

The reliability of each multi-item measure was assessed by calculating Cronbach's coefficient alpha. Cronbach's alpha and descriptive statistics for the key constructs used in the research model are presented in Table 4.2 and Table 4.3, which contain information on the correlation coefficients between all constructs. Table 4.3 indicated that the variable perceived benefits and perceived usefulness are highly correlated (0.840, $p<0.01$). The reason is probably because both variables describe values to users. However, there exist differences between the two constructs. Perceived benefits refer to direct or indirect advantages that mobile users can enjoy by using a specific mobile application. For example, users can benefit from a wider range of monitory benefits (e.g., discount), increased sociality and so forth. Perceived usefulness, on the other hand, discusses about the functions and utilitarian of a mobile application. Moreover, in my framework these two variables are in two separated models where there are no direct relationships between them. Therefore I believe it would not affect the validity of my results.

Table 4.2. Descriptive statistics for the constructs (n=308)

Variables	Number of Items	Reliability (Cronbach's alpha)	Mean (Value range 1-7)	Std.
Perceived benefits (BENEFIT)	4	0.854	4.806	1.186
Perceived risks (RISK)	3	0.863	4.487	1.472
Perceived ease-of-use (EASE)	4	0.801	4.868	1.029
Perceived usefulness (USEFULNESS)	3	0.841	4.618	1.349
Perceived enjoyment (ENJOYMENT)	3	0.866	4.568	1.217
Intention to use (INTENTION)	4	0.917	4.677	1.367
Personal innovation (INNOVATION)	3	0.910	4.568	1.546
Smartphone anxiety (ANXIETY)	5	0.879	2.363	1.152

After establishing the validity of the measures, I tested my hypotheses by examining the sign and significance of the path coefficient. Each hypothesis was tested based on the sign and the statistical significance for its corresponding path in the structural model.

Table 4.3. Pearson correlations between constructs (n=308)

	Variables	01	02	03	04	05	06	07	08	09
01	Personalization (PERS)	1								
02	Control over personal data (CONTROL)	0.006	1							
03	Perceived benefits (BENEFIT)	0.193**	0.023	1						
04	Perceived risks (RISK)	0.113*	-0.394***	0.063	1					
05	Willingess to disclose data (WILLINGNESS)	0.108	0.266***	0.516***	-0.372***	1				
06	Perceived ease-of-use (EASE)	0.147***	0.035	0.617***	0.118**	0.356***	1			
07	Perceived usefulness (USEFULNESS)	0.215***	0.025	0.840***	0.018	0.574***	0.631***	1		
08	Perceived enjoyment (ENJOYMENT)	0.110	0.087	0.538***	-0.115**	0.442***	0.393***	0.570***	1	
09	Intention to use (INTENTION)	0.146**	0.200***	0.648***	-0.272***	0.614***	0.539***	0.749***	0.693***	1

4.4.1 Privacy Calculus in Mobile Context

To verify privacy calculus in a mobile context, I first conducted a simple regression analysis with the continuous variable – willingness to disclose data (WILLINGNESS) as the dependent variable and perceived benefit (BENEFIT) and perceived risks (RISK) as the independent variables. I then introduced the two manipulated variables, personalization (PERS) and control over disclosed data (CONTROL), in the model. These two variables were coded as dichotomous variables with 1 being with condition and 0 being without condition. In step 3, my analysis also included control variables: AGE, GENDER, personal innovation (INNOVATION) and smartphone anxiety (ANXIETY). The results are given in Table 4.4.

Table 4.4. Regression results of privacy calculus

Depedent variable: WILLINGNESS			
Predictor variable	STEP1	STEP2	STEP3
Intercept	1.386***	0.971**	1.280*
BENEFIT	0.887***	0.864***	0.801***
RISK	-0.535***	-0.484***	-0.474***
PERS		0.182	0.158
CONTROL		0.420**	0.362*
AGE			0.008
GENDER			0.115
INNOVATION			0.008
ANXIETY			-0.198**
F-value	169.68	90.94	50.22
R^2	0.31	0.443	0.454

As seen in Table 4.4, all three regression models were statistically significant at the $p<0.01$ level. In step 1, the overall regression model with the two predictor variables was found to be statistically significant: F (2, 305) = 169.68, with R^2 = 0.431. Both predictor variables were found to significantly affect users' willingness to disclose personal data. This result is consistent with previous findings on privacy calculus (e.g., Dinev and Hart, 2006a). In step 2, the overall regression model with the two predictor variables was found to be statistically significant: F (4, 303) = 90.94, with R^2 = 0.443. Interestingly, users' control over personal data was found to have a significantly positive effect on users' willingness to disclose data (standardized coefficient estimate = 0.420, $p<0.01$), whereas personalization has no significant influence on users' willingness to disclose data. Thus, H4b was supported. Step 3 concluded other control variables and the intercept coefficient

in this model was found to be less significant because some of the effects were explained by users' background information (e.g., anxiety).

I conducted a further analysis to address the effect of personalization (PERS) and control over disclosed data (CONTROL) on predictor variables in the framework of the privacy calculus. Here, perceived benefit (BENEFIT) and perceived risk (RISK) were treated as dependent variables. I also included control variables in my analysis. Both regression models came out to be statistically significant at the $p<0.01$ level, $F(6, 301) = 8.15$ and $F(6, 301) = 14.43$. The R^2 obtained were 0.174 and 0.193 respectively. Personalization was positively related to the perceived benefit (standardized coefficient estimate = 0.419, $p<0.01$) and perceived risk (standardized coefficient estimate = 0.362, $p<0.05$). Therefore both H3a and H3b were both supported. Control over disclosed data, on the other hand, had a strong negative impact on perceived risk (standardized coefficient estimate = -1.071, $p<0.01$), but had no significant effect on perceived benefit (standardized coefficient estimate = -0.050, n.s.). Hence, I found support for H4a. The results are given in Table 4.5.

Table 4.5. Regression results predicting BENEFIT and RISK

	Regression model 1	Regression model 2
Dependent variables:	BENEFIT	RISK
Intercept	4.159***	3.478***
PERS	0.419***	0.362**
CONTROL	-0.050	-1.071***
AGE	0.002	0.013
GENDER	0.426***	0.242
INNOVATION	0.113***	0.083
ANXIETY	-0.274***	0.130*
F-value	8.15	14.43
R^2	0.174	0.193

4.4.2 TAM in Mobile Context

A structural equation modeling was used to test the mobile TAM. Figure 4.3 and Figure 4.4 depict the results of set 1 of the proposed hypotheses and of a final, adjusted mobile TAM. In the hypothesis, perceived ease-of-use had a direct effect on users' intentions to use mobile applications, whilst perceived enjoyment only had a direct impact on users' intentions to use mobile applications. In the final model, however, perceived ease-of-use

served as a mediator for the influence of perceived usefulness and perceived enjoyment on users' intentions to use mobile applications. Thus, against my expectations, H1b was not supported. This finding is of particular interest because perceived ease-of-use has served as a key element since the integration of the TAM theory. This has been proved by many prior studies (e.g., Venkatesh, 2000; Venkatesh and Davis, 2000). Furthermore, perceived enjoyment not only had a direct impact (standardized coefficient estimate = 0.464, $p<0.01$), but also had an indirect impact (via perceived usefulness, standardized coefficient estimate = 0.401, $p<0.01$) on users' intentions to use mobile applications. Obviously, perceived enjoyment has replaced the role of perceived ease-of-use, and has become an important predictor in mobile users' intentions to use mobile applications. Among all predictor variables, perceived usefulness still had the strongest effect on users' intentions to use mobile applications (standardized coefficient estimate = 0.671, $p<0.01$). Therefore, H1a, H1c and H1d were all supported.

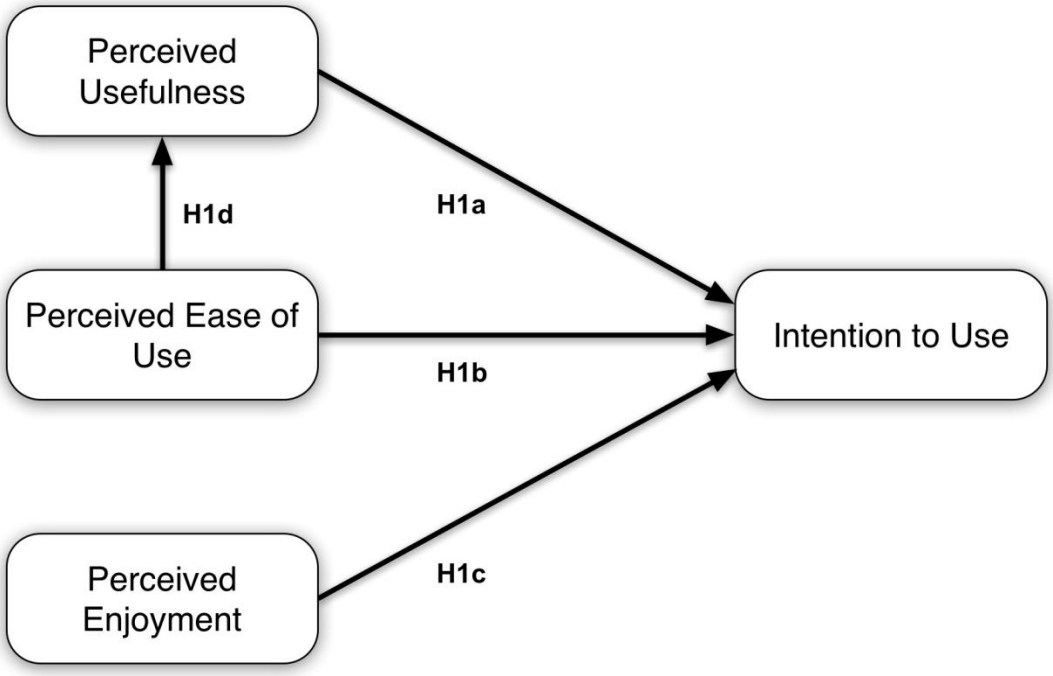


Figure 4.3. Proposed mobile TAM (Hypothesis set 1)

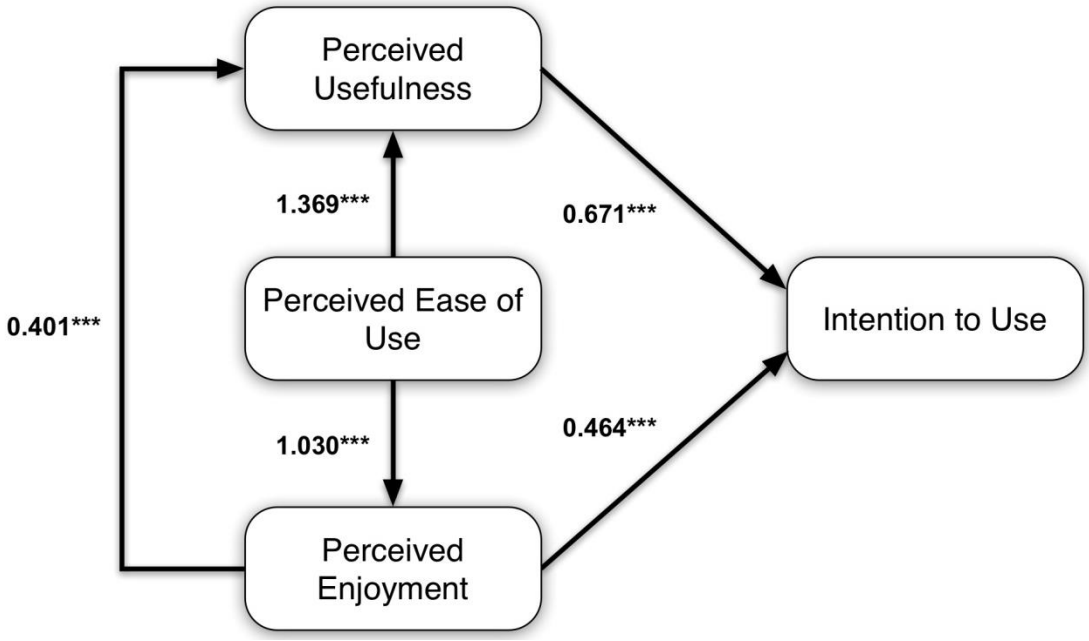


Figure 4.4. Final mobile TAM

To test H2, I added a privacy calculus in the final mobile TAM and found that users' willingness to disclose data was positively related to users' intentions to use mobile applications (standardized coefficient estimate = 0.011, $p<0.01$). Hence, H2 was also supported.

Next, I conducted a regression analysis in three steps to examine the effect of personalization and control over disclosed data. Here, users' intentions to use mobile applications (INTENTION) were the dependent variable. Again, the first step contained three main predictor variables: perceived usefulness (USEFUL), perceived ease-of-use (EASE) and perceived enjoyment (ENJOYMENT); the second step added personalization characteristics (PERS) and users' control over personal data (CONTROL). The third step included all four control variables. Table 4.6 shows the regression results.

Table 4.6. Regression results of TAM

Depedent variable: INTENTION			
Predictor variable	STEP1	STEP2	STEP3
Intercept	-0.101	-0.245	0.247
USEFUL	0.477***	0.488***	0.485***
EASE	0.119*	0.114*	0.099
ENJOYMENT	0.437***	0.418***	0.418***
PERS		-0.032	-0.023
CONTROL		0.418***	0.391***
AGE			-0.009*
GENDER			0.007
INNOVATION			-0.011
ANXIETY			-0.033
F-value	182.61	151.51	91.26
R^2	0.67	0.694	0.699

All three regression models were found to be statistically significant. In the absence of other variables (step1), F (2, 305) = 182.61, with R^2 = 0.670. Here, perceived ease-of-use had a marginally significant effect on users' intentions to use mobile applications (standardized coefficient estimate = 0.119, p<0.1). In step 2, F (4, 303) = 151.51, with R^2 = 0.694. CONTROL was found to be positively related to users' intentions to use mobile applications (standardized coefficient estimate = 0.418, p<0.01). Thus, I found support for H4c.The results for the effect of PERS on users' intentions to use mobile applications were surprising. I found no relationship between them (standardized coefficient estimate = -0.032, n.s.); thus, I failed to provide evidence for H3f. In Step 3, where all control variables were included, F (6, 301) = 91.26, and R^2 value increased to 0.699. I obtained similar results for PERS and CONTROL, but perceived ease-of-use no longer had a strong effect on users' intentions to use mobile applications (standardized coefficient estimate = 0.099, n.s.).

In order to test H3c, H3d and H3e, I conducted three simple regression models. As seen in Table 4.7, the first regression model was found to be statistically significant: F (8, 299) = 68.15, with R^2 = 0.552. Personalized services had a strong impact on perceived usefulness (standardized coefficient estimate = 0.270, p<0.01). Thus, I found evidence to support H3d. The second regression model was also statistically significant: F (6, 301) = 17.50, with R^2 = 0.224. As hypothesized in H3c, perceived ease-of-use was positively related to personalized services (standardized coefficient estimate = 0.315, p<0.01). Similarly, I found partial support for H3e, which hypothesized that perceived enjoyment was positively related to personalized services (standardized coefficient estimate = 0.101, p<0.1), although the R^2 was a bit lower (0.172) in regression model 3.

Table 4.7. Regression results predicting USEFUL, EASE and ENJOYMENT

	Regression model 1	Regression model 2	Regression model 3
Dependent variables:	USEFUL	EASE	ENJOYMENT
Intercept	-0.411	3.556***	2.491***
EASE	0.561***	-	0.471***
ENJOYMENT	0.408***	-	-
PERS	0.270**	0.315***	0.101*
CONTROL	-0.095	0.027	0.150
AGE	0.005	-0.001	-0.001
GENDER	0.328***	0.395***	0.095
INNOVATION	0.008	0.225***	0.071
ANXIETY	-0.114**	-0.147**	-0.052
F-value	68.15	17.50	2.59
R^2	0.552	0.224	0.172

4.5 Discussion

4.5.1 Discussion of the Findings

The overall goal of this study is to examine the relationships between beliefs about information privacy (privacy calculus) and mobile application usage intentions (e.g., TAM). A further goal is to shed light on the effects of personalization and the ability of users to maintain control over their personal data in a mobile context. I integrated privacy calculus theory into the mobile TAM framework to form the theoretical foundation for this study. In this way, this study was able to conceptualize and empirically test the effect of personalized services and the ability of users to maintain control over their personal data in terms of privacy concerns relating to mobile applications.

In general, the results of both the hierarchical regression analysis and structural equation analysis provide strong support for the proposed research model. The detailed results of the tests of my hypotheses are summarized in Table 4.8.

Table 4.8. Summary of results of the tests of hypotheses

	Hypotheses	Result
H1a	USEFUL → + INTENTION	Supported
H1b	EASE → + INTENTION	Not supported
H1c	ENJOYMENT → + INTENTION	Supported
H1d	EASE → + USEFUL	Supported
H2	WILLINENESS → + INTENTION	Supported
H3a	PERS → + BENEFIT	Supported
H3b	PERS → + RISK	Supported
H3c	PERS → + EASE	Supported
H3d	PERS → + USEFUL	Supported
H3e	PERS → + ENJOYMENT	Supported
H3f	PERS → + INTENTION	Not supported
H4a	CONTROL → - RISK	Supported
H4b	CONTROL → + WILLINGNGESS	Supported
H4c	CONTROL → + INTENTION	Supported

As presented in the results, the most striking finding was that perceived enjoyment had replaced the role of perceived ease-of-use in a traditional technology acceptance situation. This had a strong effect on users' intentions to use mobile applications, indicating that a hedonic element is a key component in a mobile context. The structural equation analysis also suggested that the link between perceived usefulness and users' intentions to use mobile applications is stronger than for other direct and indirect effects. This result confirmed prior TAM research which showed that perceived usefulness was a more important predictor of intended system usage than others (Davis, 1989). Perceived usefulness also mediated the relationship between perceived ease-of-use and perceived enjoyment in a mobile context. In terms of the TAM framework, however, I did not find that perceived ease-of-use of mobile applications had a direct impact. One possible reason is that, in a mobile context, such an effect is offset, to some extent, by enjoyment and usefulness.

Another surprising outcome of this study is that my results failed to support the hypothesis that personalized services directly affect users' intentions to use mobile applications (H3f). While offering a personalized service had a strong impact on both perceived enjoyment and perceived usefulness, it had no direct impact on whether or not users would like to use a specific application. This might imply that mobile users are more aware of the existence of potential benefits, such as enjoyment and usefulness. In addition, we have proved that personalized services would increase user's perceived risk, which had a negative effect on their willingness to provide personal data. It hence in turn

decreased mobile user's intention to use mobile application. To some extent, this negative effect might offset some of the positive effects that come from increased enjoyment and usefulness, resulting in the impact of personalized services on usage intention unclear.

Unlike previous findings on gender difference in privacy issues, I found that females were more likely to value a higher level of perceived benefit, perceived usefulness and perceived ease-of-use compared with male mobile users. In all likelihood, female mobile users are more interested in using social mobile applications and are more likely to enjoy the potential discounts offered by "Check Me In".

4.5.2 Contribution and Implications

This study is a rich source of theoretical implications. First, while prior studies have examined privacy calculus and TAM separately, this paper studies both theoretical models at the same time. I found that users' willingness to disclose data was positively related to users' intentions to use mobile applications. Future research should apply this framework in order to investigate the relationship between users' beliefs and rights, and disclosure behavior regarding privacy issues in general.

Second, this study provides preliminary theoretical insights and empirical evidence into the structural relationships of antecedents that affect mobile users' intention to use applications. Thus, it has extended the understanding of a mobile TAM. My findings have also proved that the conventional TAM proposed by Davis (1989) no longer fits well in the mobile context. As discussed earlier, perceived ease-of-use did not have a significant impact on users' intention to use mobile applications. Instead, perceived usefulness served fully as a mediator for the influence of perceived ease-of-use on users' intention to use mobile applications. On the other hand, as a new characteristic, perceived enjoyment played an important role (path coefficient is 0.464). In this respect, it can be seen to be similar to perceived usefulness (path coefficient is 0.671). This has important implications for theoretical development. This study serves as a starting point for future research into a mobile TAM, identifying considerable opportunities and opening up new avenues for exploring predictors using a mobile TAM theory.

Third, this study serves as an initial examination of issues relating to privacy by investigating whether or not personalized services and users' ability to control their information can influence personal information disclosure and use intention. Using a privacy calculus lens, I argued that personalized services and control over disclosed data play an important role in the way that individuals weigh up the utility gained by disclosing personal information against the disutility of adverse effects resulting from such an action. The results also suggest that personalized services can somehow increase users' perceived risks (the path coefficient is 0.362). However, the way that mobile users'

value personalization (e.g., its effects on a perceived benefit) was more influential than their concern for potential risks (path coefficient 0.419 versus 0.362). Moreover, this research also builds on previous studies that have sought to understand the effects of users' ability to control information. It provides empirical evidence that control over personal data is an important driver of mobile users' perceived risks, which in turn influences users' willingness to disclose personal information

Another theoretical implication is that whilst the bulk of previous research has examined individuals' willingness to share information and consumer disclosure behavior in either an offline or online setting, this paper contributes empirical results from a mobile context. My findings support the premise that personal information disclosure involves a cost-benefit trade-off analysis in a mobile privacy calculus. It reveals that perceived benefit was a much stronger predictor than the negative effect of perceived risk. This indicates that when the level of benefit is high, users may not worry too much about any potential risks. Thus, they may be more willing to disclose their personal data in order to use mobile applications.

From the perspective of practice, my findings also provide several important implications for various players. First, the results indicate that mobile users are concerned about their private personal information and are less willing to disclose personal information in m-commerce. These negative consequences could be alleviated by increasing the level of control that users have over disclosed information. Thus, marketers in an m-commerce setting will need to ensure that users are able to control information (e.g., by issuing a privacy statement). Giving users greater control over disclosed personal data can reduce users' perceived risk of using mobile applications, which, in turn, can increase their intention to use these applications.

For application designers, this study provides practical guidance as to how to design and develop mobile applications. A simple and enjoyable application will probably encourage more mobile users to download and use that application. In addition, my findings suggest that every new personalization is likely to increase users' anxieties about the risks with providing personal data. Application designers should, therefore, pay careful attention to the relationship between the potential benefits of personalized services to users, and the related privacy problems they may cause.

4.5.3 Limitations

I acknowledge that, like other studies, this paper has its limitations. First, this study has focused on a single mobile application: a geographical location-based social network. If consumers are not interested in connecting with friends through mobile technology, or getting discounts from restaurants and bars, then this application is not going to be of

interest to them. Thus, the findings obtained from this study might not be generalizable to other mobile applications (e.g., games).

Second, I admit that an experimental method was used for data collection. Thus, the participants did not use the mobile application in a real-world setting. If they had used a mobile application in the real world, (e.g., which may affect networking quality), this may have had an effect on users' intentions.

Finally, despite the care I took in designing the experiment, some common method bias was not avoidable. Although the final sample consisted of people from diverse occupational backgrounds and different age groups, I have to admit that they were mainly from only two countries: China and Switzerland. This may also negatively affect the generalizability of the results. Future research is needed to address the potential moderate effects of cultures.

4.6 Conclusion

Building upon the privacy concern literature juxtaposed with the technology acceptance model, this study has developed a theoretical framework that combines the role of personalized services and users' control over personal data in the mobile application context. An interesting finding of this study is that perceived enjoyment has replaced perceived ease-of-use as a main predictor of perceived behavioral intentions in m-commerce. Perceived usefulness still has the strongest impact. At the same time, the results also reveal that users' control over personal data and personalized services has a strong effect on both a privacy calculus and mobile TAM. Marketers and application designers need to understand these influences and address them appropriately to encourage mobile users to disclose personal information and use mobile applications.

4.7 References

Ackerman, M. S. 2004. "Privacy in Pervasive Environment: Next Generation Labeling Protocols," *Personal and Ubiquitous Computing* (8), pp.430-439.

Ackerman, M. S., Cranor, L., Reagle, J. 1999. "Privacy in e-Commerce: Examining User Scenarios and Privacy Preference," In Proceeding of ACM conference on electronic commerce, Denver, Colorado, pp.1-8.

Adams, D. A., Nelson, R. R., and Todd, P. A. 1992. "Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication," *Management Information Systems Quarterly* (16), pp.227-247.

Anderson, C. L., and Agarwal, R. 2011. "The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information," *Information Systems Research* (22:3), pp. 469-490.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *Management Information Systems Quarterly* (30:1), pp.13-28.

Bandyopadhyay, S. 2012. "Consumers' Online Privacy Concerns: Causes and Effects," *Innovative Marketing* (8:3), pp.32-39.

Bansal, G. Zahedi, F. M., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support System* (49:2), pp.138-150.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information System," *Management Information Systems Quarterly* (35: 4), pp.1017-1041.

Bélanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Strategic Information Systems* (11), pp.245-270.

Campbell, A. J. 1997. "Relationship Marketing in Consumer Markets: A Comparison of managerial and Consumer Attitudes about Information Privacy," *Journal of Direct Marketing* (11:3), pp.44-57.

Chellappa, R. K., and Sin, R. G. 2005. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6), pp.181-202.

Chen, X., Ma, J., Jin, J., and Fosh, P. 2013. "Information Privacy, Gender Differences, and Intrinsic Motivation in the Workplace," *International Journal of Information Management* (33), pp.917-926.

Chen, K., Rea, Jr., A. I. 2004. "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques," *Journal of Computer Information System* (44:4), pp.85-92.

Chorppath, A. K., and Alpcan, T. 2013. "Trading Privacy with Incentives in Mobile Commerce: A Game Theoretic Approach," *Pervasive and Mobile Computing* (9), pp.598-612.

Christin, D., Lopey, P. S., Reinhardt, A., Hollick, M., and Kauer, M. 2013."Share with Strangers: Privacy Bubbles as User-Centered Privacy Control for Mobile Content Sharing Applications," *Information Security Technical Report* (17), pp.105-116.

Clarke, R., 1999. "Internet Privacy Concerns Confirm the Case for Intervenion," *Communication of the ACM*, (42:2), pp.28-31.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp.323-342.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*," Management Information Systems Quarterly* (13:3), pp.319-340.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp.982-1003.

Dey, A. K., and Abowd, G. D. 2000. "Towards a Better Understanding of Context and Context-Awareness," In Proceedings of the CHI 2000 Workshop on The What, Who, Where, When, and How of Context-Awareness, The Hague, Netherlands, April.

Dhar, S., and Varshney, U. 2011. "Challenges and Business Models for Mobile Location-based Services and Advertising," *Communication of the ACM* (54:5), pp.121-129.

Dinev, T., and Hart, P. 2004. "Internet Privacy Concerns and Their Antecedents – Measurement Validity and A Regression Model," *Behavior & Information Technology* (23:6), pp.413-422.

Dinev, T., and Hart, P. 2006a. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information System Research* (17:1), pp.61-80.

Dinev, T., and Hart, P. 2006b. "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," *International Journal of Electronic Commerce* (10:2), pp.7-29.

Dinev, T., and Hart, P. 2007. "Privacy Concerns and Levels if Information Exchange: An Empirical Investigation of Intended e-Service use," *e-Service Journal* (4:3), pp.25-61.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in Online Shopping: An Integrated Model," *Management Information Systems Quarterly* (27:1), pp.51-90.

George, J. F. 2004. "The Theory of Planned Behavior and Internet Purchasing," *Internet Research* (14:3), pp.198-212.

Gervey, B., and Lin, J. 2000. "Obstacles on the Internet: A New Advertising Age Survey Finds Privacy and Security Concerns Are Blocking the Growth of E-commerce," *Advertising Age* (71:16), pp.13-22.

Goodwin, C. 1991. "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing* (10:1), pp.149-166.

Graeff, T. R., Harmon, S. 2002. "Collecting and Using Personal Data: Consumers' Awareness and Concerns," *Journal of Consumer Marketing* (19:4), pp.302-318.

Green, H., Yang, C. Judge, P. C. 1998. "A Little Net Privacy, Please", *Business Week*.

Hann, I.-H., Hui, K.-L., Lee. T. S., and Png, I. P. L. 2002. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off," in Proceeding of 23rd International Conference on Information System, pp.1-10.

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

Hong, W., and Thong, J. Y. L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *Management Information Systems Quarterly* (37:1), pp.275-298.

Junglas, I. A., Johnson, N. A., and Spitzmuller, C. (2008). "Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-Based Services", *European Journal of Information Systems* (17: 4), pp. 387-402.

Junglas, I. A., and Watson, R. T. 2006. "The U-Constructs: Four Information Drives," *Communication of AIS* (17), pp.569-592.

Junglas, I. A., and Watson, R. T. 2008. "Location-based Services: Evaluating user perceptions of location-tracking and location-awareness services," *Communication of the ACM* (51:3), pp.65-69.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior," *International Journal of Human Computer Studies* (71), pp.1163-1173.

Kim, E., and Lee, B. 2009. "E-service Quality Competition through Personalization under Consumer Privacy Concerns," *Electronic Commerce Research and Applications* (8), pp.182-190.

King, N. J., and Jessen, P. W. 2010. "Profiling the Mobile Consumer – Privacy Concerns When Behevioural Advertisers Terget Mobile Phones – Part I," *Computer Law and Security Review* (26), pp.455-478.

Kuo, F.-Y., Lin, C. S., and Hsu, M.-H. 2007. "Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices," *Journal of Business Ethics* (73), pp.145-460.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Development Theory," *Journal of Social Issues* (33:3), pp.22-42.

Liang, T.-P., Chen, H.-Y., Du, T., Turban, E. and Li, Y. 2012. "Effect of Personalization on the Perceived Usefulness of Online Customer Services: A dual-Core Theory," *Journal of Electronic Commerce Research* (13:4), pp.275-288.

Liu, Z., Shan, J., Bonazzi, R., Pigneur, Y. 2014. "Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications," In Proceeding of the 47st Hawaii International Conference in System Sciences, Waikoloa, Hawaii, USA, pp. 1063-1072.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp.336-355.

Meinert, D. B., Peterson, D. K., Criswekk, J. R., and Crossland, M. D. 2006. "Privacy Policy Statements and Consumer Willingness to Provide Personal Information," *Journal of Electronic Commerce in Organization* (4:1), pp.1-17.

Miyazaki, A. D., and Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *The Journal of Consumer Affairs* (36:1), pp.28-49.

Nam, C., Song, C., Lee, E., and Park, C. I. 2006. "Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online," *Advances in Consumer Research* (33), pp.212-217.

Nosko, A., Wood E., Kenney, M., Archer, K., De Pasquale, D., Molema, S., and Zivcakova, L. 2012. "Examining Priming and Gender as a Means to Reduce Risk in a Social Networking Context: Can Stories Change Disclosure and Privacy Setting Use when Personal Profiles are Constructed?" *Computers in Human Behavior* (28), pp. 2067-2074.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1), pp.27-41.

Sheehan, K. B. 2002. "Toward a Typology of Internet Users and Online Privacy Concerns," *The Information Society* (18:1), pp.21-32.

Sheng, H., Nah, F.F.-H., and Siau, K. 2008. "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems* (9:6), pp. 344–376.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *Management Information Systems Quarterly* (35:4), pp.989-1015.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. Information Privacy: Measuring Individual's Concerns About Organizational Practices, *Management Information Systems Quarterly* (20:2), pp.167-196.

Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior", In Proceedings of ACM conference in electronic commerce, Tampa, Florida, US, pp.38-46.

Stewart, K. A., and Segars, A. H. 2002. "An empirical examination of the concern for information privacy instrument," *Information Systems Research* (13:1), pp. 36-49.

Sutanto, J., Palme, E., Tan, C-H., and Phang, C.W. 2013. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *Management Information Systems Quarterly* (37:4), pp.1141-1164.

Tam, K. Y., and Ho, S. Y. 2006. "Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes," *Management Information Systems Quarterly* (30:4), pp.865-890.

Tamimi, N., and Sebastianelli, R. 2007. "Understanding eTrust," *Journal of Information Privacy and Security* (3:2), pp.3-17.

Van der Heijden, H. 2004. "User Acceptence of Hedonic Information System," *Management Information Systems Quarterly* (28:4), pp.695-704.

Varian, H. R. 1996. "Economic Aspects of Personal Privacy," Technical report, University of California, Berkeley, US.

Venkatesh, V. 2000. "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information System Research* (11:4), pp.342-365.

Venkatesh, V.; Davis, F. D. 2000. "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management Science* (46:2), pp. 186–204.

Venkatesh, V., Thong, J. Y. L., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *Management Information Systems Quarterly* (36:1), pp.157-178.

Wang, Y. D., and Emurian, H. H. 2005. "An Overview of Online Trust: Concepts, Elements, and Implications," *Computers in Human Behavior* (21), pp.105-125.

White, T. B. 2004. "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology* (14:1&2), pp.41-51.

Whitley, E. A. 2009. "Informational Privacy, Consent and the 'Control' of Personal Data," *Information Security Technical Report* (14), pp.154-159.

Wills, C. E., and Zeljkovic, M. 2011. "A Personalized Approach to Web Privacy: Awareness, Attitudes, and Actions," *Information Management and Computer Security* (19:1), pp.53-73.

Wu, K.-W., Huang, S. Y., Yen, D. C., and Popova, I. 2012. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust," *Computer in Human Behavior* (28), pp.889-897.

Xu, J. D., Benbasat, I, and Cenfetelli, R. T. 2013. "Integrating Service Quality with System and Information Quality: An Empirical Test in the E-Service Context," *Management Information Systems Quarterly* (37:3), pp.777-794.

Xu, H. 2010. "Locus of Control and Location Privacy: An Empirical Study in Singapore," *Journal of Global Information Technology Management* (13:3), pp.63-87.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2010. "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.

Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. 2011. "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing," *Decision Support Systems* (51), pp.42-52.

4.8 Appendix: Measure Items

Smartphone Anxiety (ANXIETY)

Concerning smartphone …

…it does not scare me at all.

…working with it makes me nervous.

…it makes me feel uneasy.

…it makes me feel uncomfortable.

…I get a sinking feeling when I think of trying to use it.

Personal innovation (INNOVATION)

Concerning new information technology …

…once I heard about it, I would look for ways to experiment with it.

…among my peers, I am usually the first to try out new information technologies.

… I like to experiment with new information technologies.

Perceived benefits (BENEFIT)

Overall, I fell that using "Check Me In" is beneficial.

"Check Me In" allows me to see where my friends like to go.

Using "Check Me In" would give me special deals in a restaurant or a bar.

"Check Me In" allows me to record and share my adventures.

Perceived risks (RISK)

There would be high potential for loss in disclosing my personal information to "Check Me In".

It would be risky to disclose my personal information to "Check Me In".

Providing "Check Me In" with my personal information would involve many unexpected problems.

Perceived ease-of-use (EASE)

Learning to operate "Check Me In" would be easy for me.

I find it easy to get "Check Me In" to do what I want it to do.

I find "Check Me In" to be easy to use.

My interaction with "Check Me In" is clear and understandable.

Perceived enjoyment (ENJOYMENT)

Using “Check Me In” would be fun.

Using “Check Me In” would be enjoyable.

Using “Check Me In” would be very entertaining.

Perceived usefulness (USEFULNESS)

I find “Check Me In” to be useful in my daily life.

Using "Check Me In" would always give me good suggestions for a nice restaurant.

Using "Check Me In" would help me to connect with my friends.

Intention to use (INTENTION)

If "Check Me In" is available on Mobile App Store, I predict that I will download and use it.

Assuming I have access to "Check Me In", I intend to use it.

I intend to increase the use of "Check Me In" in the future.

I would appreciate using "Check Me In".

Willingness to disclose data (WILLINGNESS)

How likely would you provide your personal information (including your location) used in "Check Me In"? (From 0 to 100, where 0 = not at all; 100 = extremely likely)

Chapter 5

Conclusions

This thesis described a context-aware based adaptive privacy management system for mobile devices. It addressed three important privacy-related problems in mobile context by three inter-related essays. The research process is followed by firstly design and test an idea, then implement and evaluate an artifact based on this idea, and finally develop the new theory of privacy concerns in mobile world. Since each essay has its own conclusion, this section highlights the contributions of my thesis, and briefly describes the limitations and some areas that merit future research.

5.1 Summary of Contributions

I believe this thesis will improve literature on both of the theoretical aspects and the practical aspects in privacy risk management for mobile devices. To answer the first research question, I presented a theoretical model for an adaptive single sign-on (ASSO) solution regarding privacy risk management associated with context-aware technologies. By using mobile users' location and time, I proved that ASSO solution could be used to increase mobile user's perceived ease of use of the system, and service provider's authentication security of application. This study represented the first to offer empirical evidence that user's context information can be used to protect their private information against theft therefore provided various implications for both scientific community as well as practitioners. Based on this result, I proposed a new instantiation of the business model pattern with privacy at the core of its value proposition. To validate this idea, I then designed and developed an artifact in the form of the mobile application. The new findings of this study addressed the second research question. The third essay focused on new privacy related theory development. This theory combined the privacy calculus model and mobile TAM together, to answer the third research question concerns mobile users perceive about information privacy. Moreover, the analysis of how the role of personalized service available and user's control ability interact with privacy calculus and

mobile TAM provides a blueprint to guide future research and creation concerning the organizational performance impacts of information technology.

One story of Apple's invention news that happened quite recently seems to corroborate the feasibility and superiority of the proposed ASSO solution. On July 17 2014, the US Patent & Trademark Office published a patent application from Apple – named as "Generating notifications based on user behavior" – that describes a method by which an iPhone can set off an alert notification or automatically lock the device based on detected changes in user behavior. This system would employ behavior recognition techniques, such as location, motion sensor data, and input gesture patterns, to determine whether the current user is the device owner. When usage patterns don't match those of the owner, an alert, notification or system action is triggered. Such idea is very similar to the adaptive single sign on solution proposed in my thesis, which utilizes mobile users' behavioral information (i.e., location, time, etc.) to secure users' private information.

5.2 Limitations and Future Research

As with all research, this doctoral thesis is subject to several limitations. First, the proposed ASSO solution should offer an approach to secure user's private information for people who have a relatively regular life. I admitted that such a solution might not be applicable for people whose life is rather flexible. For them, other user recognition techniques other than conjoining location and time information, such as motion sensor data, face recognition technology, should be employed.

Secondly, I considered scenario based questionnaire, instead of asking questions to real users in chapter 4. However, the views between respondents that have used and those have not may diverge. I choose to accept this research limitation because seeking answers from respondents that have used this application with such a large scale, as attempted initially, would severely increase the time and cost.

Finally, this thesis' interests lie in the context-aware based adaptive privacy management system in mobile context. To better capture the level of "adaptive", semantic technology may serve as a good solution. Unlike traditional web technologies, which are based on a syntactical markup of information, semantic web technology provides semantic search and additional features like knowledge-based, location based, or context aware information. Such technology is believed to offer high value added services without sacrificing its safety feature. However, so far little work has been done to explicitly account for aspects of mobile privacy in semantic service frameworks. Future research could extend to build a semantic context awareness privacy management system in this direction.

Appendix A

A Dynamic Privacy Manager for Compliance in Pervasive Computing

Published in the book of Privacy Protection Measures and Technologies in Business Organization: Aspects and Standards
Edited by G.O.M. Yee, December 2011, page 285-307
Publisher: IGI Global
ISBN: 978-1-61350-501-4

Abstract In this paper I propose a decision support system, for privacy management of context-aware technologies, which requires the alignment of four dimensions: business, regulation, technology, and user behavior. I have developed a middleware model able to achieve compliance with privacy policies within a dynamic and context-aware risk management situation. I illustrate the model in more details by means of a small prototype that I developed and I present the current outcomes of its implementation to derive some pointers for the direction of future investigation.

Keywords: Privacy management, Context-aware technologies, User's behavioral intention, Design science, Infomediary, Middleware

6.1 Introduction

Privacy is generally referred as “a state in which one is not observed or disturbed by others” (Oxford Dictionary, 2010), and privacy management for pervasive technologies can be treated as an information security issue. Security experts have been advocating that information security should result from the alignment of the technical, business, and regulatory dimensions (Anderson, 2001), suggesting an information risk management approach to let the user achieve the best security level according to the environmental threats (Blakley et al. 2001). Therefore one should also look at how to manage the risk that privacy is not assured, before looking at how to achieve privacy from a technical point of view.

Contingency theory is a class of behavioral theory that claims that the optimal course of action is contingent upon both the internal and external situations. Such theory postulates that impacts of environmental factors are systemic, rather than entirely situational. That fits the case of mobile payment services that differ between markets, in ways linked to their particular systems, for instance there are differences in payment technology infrastructure, regulation, laws, or habits. Therefore contingency theory can be used as a reference framework to assess the literature on mobile payment published in information system, electronic commerce, and mobile commerce journals, and conference proceedings (Dahlberg et al. 2007). It appears that a contingency factor (Changes in Technological Environment) has been intensively studied, two contingency factors (Changes in Commerce Environment and Changes in Legal, Regulatory, and Standardization Environment) have been addressed by not more than twenty articles, whereas one contingency factor (Changes in Social/Cultural Environment) was not treated in any article.

Literature on privacy risk management can be assessed using three contingency factors suggested by Anderson (2001): technology, business, and legal. To address the gap underlined by Dahlberg et al. (2007) I add a fourth dimension: the user’s perception of its environment.

6.1.1 Awareness of Changes in the Technology Environment

Technology awareness concerns the understanding of the technological options for privacy management that are offered in a particular moment in time to the user. The link between pervasive computing and user’s privacy risk has been addressed by many researchers, mostly in the field of location privacy. In his literature review of computational location privacy Krumm (2009) claims that “location data can be used to infer much about a person, even without a name attached to the data.”(p. 4). Most

applications focus on controlling access and use of user's data, or they propose security algorithms to protect/obfuscate the communication of data between two users. Krumm (2009) lists a set of solutions for location computational privacy. For example "blurring" is a security algorithm, which ensures a certain degree of location privacy by using inaccurate or at least not so accurate location information, in order to obfuscate the communication of users. Another algorithm is "Access control", which ensures that the sensitive data is only accessed by authorized people, in order to protect user's information privacy.

Middleware development has been adapting to evolving technology, and in this sense a solution is mentioned that deals with conflicting privacy policies (Capra et al., 2003) and another solution that uses an extended version of a privacy policy language that takes into consideration the time dimension (Hong et al., 2005).

This paper presents the design of software for decision support regarding privacy risk management for pervasive technologies, with a particular interest in context-aware applications, as described by Schilit et al. (1994) and Chen and Kotz (2000). Thus this study aims at increasing the user's acceptance of the privacy management system. The theoretical foundation can be found in the technology adoption model proposed by Davis (1989), which assess that user's behavioral intention to adopt a system depends on the perception of usefulness and ease of use. Thus a context-aware privacy management system should protect the user's data and it should reduce the number of actions requested to the user.

6.1.2 Awareness of Changes in the Commerce Environment

A stream of research called economics of security, which Anderson and Blakely's research belongs to, has contributed in adopting economic concepts like "game theory with incomplete information" and "behavioral economics" into IS risk management (e.g. Acquisti, 2003). Recognizing the importance of privacy management as a business process, and a business support process, the use of a context-awareness application casts privacy management into a business perspective with benefits and costs to either party in a process. This is especially relevant for communications operators as brokers, and for communication channels between content owners (individuals, businesses) and enterprise applications.

Privacy risk management is a situation where actors with diverging goals have a temporary interest in cooperating and sharing information to increase mutual trust (Palen and Dourish, 2003). Nalebuff and Brandenburger (1997) describe this situation of cooperation and competition by means of five elements, which is used here as a general framework to assess the state of the art in academic literatures.

- **Actors involved in the game**: Location privacy can be modeled as a non-cooperative game among peers (Freudiger et al., 2009). In this case the *phone user* and her *peers* are identified as two selfish actors while the *attacker* is a third actor, whose goal is to obtain information about the phone user. The phone user and the peers have an interest in cooperating only once they get close enough to each other and can change pseudonyms in order to confuse the attacker. Extending the work of Hong et al. (2005) a fourth actor emerges, i.e. the *service provider*, for example a weather forecaster of the zone where the phone user is located, who wishes to establish a trusted relationship with his potential users (i.e. he does not want to be considered as an attacker). Yet few authors seem to have recognized the importance of the *privacy system designer*, even if his actions affect other actors and although his goals are not necessarily aligned with any of those previously mentioned. One might recall the statement by Palen and Dourish (2003) that privacy is the result of a set of dynamically evolving regulations between actors as their goals and level of trust change. Thus the way the system is designed might constrain the flexibility required by other actors.

- **Added value of each actor**: Palen and Dourish (2003) clearly identify the need for the *phone user* and her *peers* of a trade-off between the advantages of being visible to the others and the risk of exposure to an *attacker*. In what concerns the *attacker* beside the evident trade-off between the risk of being caught and the advantages of stealing personal data, Anderson (2001) notices how an attacker has fewer resources than the security professionals, but aims at finding only one unknown bug to get an immediate advantage. This issue impacts the *privacy system designer* too, since he might not be the one who pays for the consequences of the theft of private data. This lack of moral hazard could lead to a phenomenon known as "liability dumping". On what concerns the *service provider*, one could expect him to look for the greatest number of potential phone users to reach with the least effort, and this could also be a case where the quest for network externalities (i.e. the search for more users to attract even more users) might be to the detriment of the security of private data. Again there is the possibility that the service provider could decide to act as an infomediary, i.e. an information intermediary (Hagel 3rd and Singer, 1999) that collects data from the *phone users* and the *privacy system designer* and dispatches aggregated data while employing best-practices for privacy management. Such data would be valuable both for the *phone users* and to the *privacy system designer*, and will reduce its value to the *attacker*.

- **Rules of the game**: On the one hand most authors agree on claiming that regulations concerning privacy management for pervasive technologies are still vague and ambiguous. Citing Massey et al. (2010) "specifying legally compliant requirements is challenging because legal texts are complex and ambiguous by nature"

(p.119). This might be due to the hard task that aligning business, technological and legal expertise implies. On the other hand a good example of clear privacy policies that can be understood by humans and machine is the Privacy Preferences Platform as described by Reagle and Cranor (1999) and extended by Hong et al. (2005). On the technological side, many security technological solutions have been proposed and with the increasing computational power of mobile devices the number of offers is expected to grow exponentially. Yet on the business and legal side it is not clear yet how much control should be imposed on the actors involved and how much dynamism should be allowed.

- **Tactics for the players**: Still to the best of my knowledge no author has dealt with the need of an evolution of the privacy system in the phone of the user, as a response of new ways to sense the environment and to enforce privacy policies. Among the security algorithm proposed for privacy protection Freudiger et al. (2009) have taken into account the problem of user's selfishness in their pseudonym change algorithm, but no attempt to combine different tactics and to select dynamically one that fits best a determined state of the environment has been done yet.

- **Scope of the game**: Regarding the scope of the interaction between actors, two dimensions come up to my minds. The temporal dimension suggested by Hong et al. (2005) implies that the privacy system needs to evolve. For the data to be retained, while most authors focused on techniques to retain as little data as possible for as little time as needed, a quick consideration on the possible need in the future of data retention for regulatory compliance underlines the need of a middleware to mediate among different requirements. A second dimension to be considered is the geographical analysis, i.e. the size of physical area to be assessed. For sake of simplicity I shall assume it to be a circle, whose radius is 50 meters for the GPS-enabled mobile device and 100 meters for a Wi-Fi enabled mobile device.

6.1.3 Awareness of Changes in the Regulatory Environment

Regulatory awareness concerns the continuous assessment of laws and standards that apply to a determined environment. From the regulatory point of view laws on data privacy are present in different business sectors and in different countries, leading to a complex multitude of overlapping and sometimes conflicting regulations that change over time, as described by Ponemon (2000). This commonly leads to ambiguity and to address that situation a standard privacy policy language, i.e. P3P (Reagle and Cranor, 1999) has been recommended by the World Wide Web Consortium. Although P3P has been criticized for its difficulty of implementation a stream of research has grown around it. Therefore I cite the recent work of Manasdeep et al. (2010), who propose a collaborative model for data privacy and its legal enforcement to support a relationship of confidence

between the operating system and the user's data repository. Another approach would be to use the set of metrics derived from privacy regulations, which can be found in Herrmann (2007).

6.1.4 Awareness of Changes in Social Environment

From the social point of view there are two levels of analysis which can be investigated. One could consider users' behavior as an external contingency factor that affects the privacy of a specific user, e.g. different cultures and countries are said to behave differently on what concerns privacy (e.g. Japanese are more likely to share data than Swiss users). Yet at the personal level user awareness is also an internal factor. Researches in human computer interaction have underlined this issue (e.g. Barkhuus, 2004), but little has been done to design a privacy risk management application which takes into consideration those behavioral studies that represent users as opportunistic and rationally bounded.

Most papers on privacy management implicitly assume a rational decision model, with the following characteristics:

- **Sure-thing principle**: This was first introduced by the statistician Leonard Jimmy Savage (1954) and it states that a decision maker can rank all options in order of preference and choose the highest one in the ranking.

- **Independence of tastes and beliefs**: this assumption was proposed by the economists Roy Radner and Jacob Marshak (1954) and it states that the decision maker's tastes concerning the outcome of the different options are independent of the options itself, and that her beliefs about the likelihood about the different outcomes are independent of the corresponding outcomes itself. In other words the decision maker is going to assess the outcomes and the likelihood of each option without any bias.

- **Logical and adequate capacity for computing**: from the first two assumptions a third implicit assumption can be derived, i.e. that the agent should be logical and have potentially unlimited capacity of formulation.

Simon (1959) revised the rational decision model and relaxed the third assumption in his bounded rationality model. Indeed the logical approach to decision maker risk aversion does not imply risk neutrality. A rational user can be either risk neutral or risk averse. In the latter case the risk-averse user looks at the worst probable outcome (thereinafter indicated as "wpo") for each option and then chooses the option with the greatest "wpo" among the list. Therefore let us assume that someone has to make a bet on one of two options. Option A can let him win €100 or lose €50, whereas option 2 lets him win €75 or

lose €25. If he wants to avoid risk he will rationally bet on the option B, since it has the greater wpo (-€25 is greater than -€50).

Simon (1959) also relaxed the assumption concerning the potentially unlimited capacity of formulation. Facing high uncertainty humans can not deal with high degree of complexity and look for simplified models to assist them in making choices. Simon et al. (1987) have combined the concepts of bounded rationality and computational costs to introduce sub-optimal solutions that are called "satisfying". According to this model a decision maker starts creating options and ranks them sequentially. Once a satisfactory result is found the decision maker stops searching for other options. This is a dynamic decision rule strategy that drops the other options, even if they might perform better, because the cost of search is greater than the gain in performance.

Radner (2000) has proposed a “truly bounded rationality model” that acknowledges the cost involved in decision making (observation, computation, memory, and communication) and addresses the challenges in ordering the options (inconsistency, ambiguity, and vagueness of the options, unawareness of other options that might rise in the future) using a Bayesian model. But even such a model fails to determine the long-term outcomes of each option, making it hard to rank them properly.

On what concerns security management, Straub and Welke (1998) used the bounded rationality model to explain why managers take apparently irrational risk management decisions to minimize their perceived risk exposure. On what concerns perception Tversky and Kahneman (1974) have shown that people tend to seek for opportunity and avoid risk in an unbalanced way. Therefore users might have the tendency to underestimate their exposures to privacy risks, which are hard to be perceived in the physical world. Therefore a privacy management application should support the user by decreasing the cost of decision making and by reducing the challenges in ordering the options. Otherwise the risk perceptions will be biased and the user is likely to be exposed involuntarily to risk.

From the literature review it seems that the user dimension has received little attention from the information system community. Hence I investigate the implications of user awareness for privacy management system design in more detail. In doing so I assume that privacy risk management is a set of actions that the user expects his devices to perform dynamically in response to his perceived environment at a determined moment in time. My research question arises accordingly: *what are the design characteristics of a privacy management system for an opportunistic and rationally bounded user using a context-aware mobile device?*

In this study I follow a research design approach using the guidelines of Peffers et al. (2007). Thus the remainder of the paper is structured as follows: I start by briefly

summarizing the methodology used in this study. Then I describe the design of the solution and how I came to develop it. After that I present a prototype, which I constructed according to my design and in conclusion we describe and illustrate a first evaluating session I performed with experts in the field.

6.2 Methodology

Based on the relevant literatures, I create an artifact in the form of a model (March and Smith, 1995) to express the relationship between user benefit and the amount of personal data disclosed.

I adopt a design science research methodology and I refer to existing guidelines for design theories (Gregor and Jones, 2007). The theories for design and action "give explicit prescriptions on how to design and develop an artifact, whether it is a technological product or a managerial intervention" (Gregor and Jones 2007, p.233). Therefore I advance in three steps as illustrated in the Table 6.1.

Table 6.1. From the theoretical model to the practical application of the design guidelines

What are the characteristics of privacy management software that increase the user's intention to adopt the system?	**What are the design characteristics of a privacy management system that can be derived from the previous model?**	**How can these design characteristics be converted into design guidelines?**
Our **theoretical framework** has three dimensions (technology – context- regulation), which influence a fourth dimension (user's decision)	Our **solution** decomposes the user's decision dimension into a five-step information flow. It combines the other three dimensions I obtain eight scenarios to assess existing privacy management applications for mobile devices	The **implementation** of the solution shows how to combine the technology-context-regulations dimensions into a five-step information flow.

6.3 Theoretical Framework

From the literature review we derive a set of constructs presented in the Figure 6.1.

The first construct is technology awareness, which is defined as the possibility for the mobile user to receive updates about the security solutions available on the phone currently used. This construct could be measured by using the number of technological updates sent to the user's mobile device.

The second constructs concerns context awareness, which is defined as the possibility for the mobile user to receive updates about the privacy risk of the zone where she is currently located. This construct could be measured by using the number of sensor updates sent to the user's mobile device.

The third construct is the regulatory awareness, which is defined as the possibility for the mobile user to receive updates about the best combination "security solution"-"privacy risk" according to security frameworks and laws. This construct could be measured by using the number of rule updates sent to the user's mobile device.

The fourth construct concerns the user's behavioral intention to adopt the system and it is based on the theory of reasoned action of Fishbein and Ajzen (1975), whose explanatory power has been proved in the past by means of two metanalyses conducted by Sheppard et al. (1988).

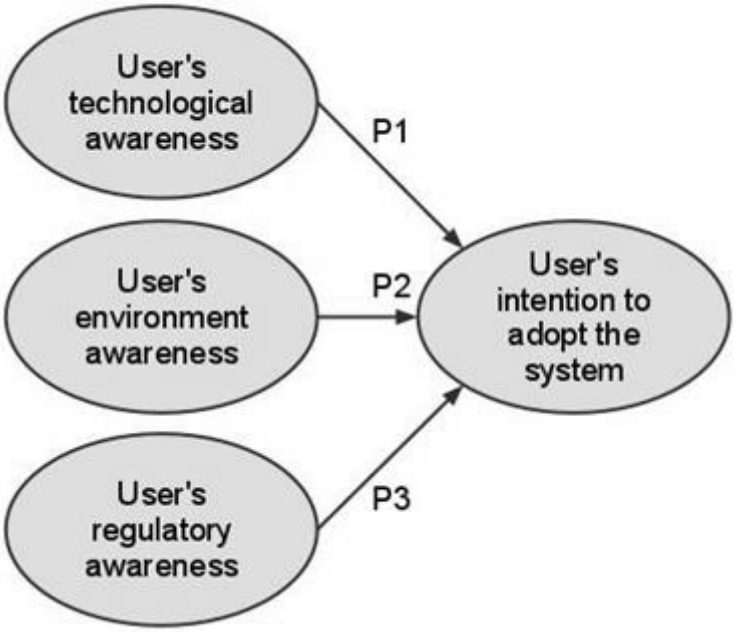


Figure 6.1. Theoretical model

The technology adoption model of Davis (1989) and its later extension called Unified Theory of Acceptance and Use of Technology of Venkatesh (2003) stated that a user's perceived usefulness increases the user's intention to use the system. User's awareness of the security technologies available supports the realization of user's identity protection. Therefore, this study claims that a user's behavioral intention to adopt the system follows the user's technological awareness in a linear way, as illustrated by the Figure 6.2. My first proposition can be expressed by the following formula:

*(P1) User's behavioral intention to adopt the system = a1 + b1*Technological_Updates + n1*

Where "a1" is constant that represents the fact that the user would adopt the system even if it does not offer any technological awareness. "a2" is a positive coefficient representing the relationship between the two constructs. "n1" is usually used in linear regression models to represent the difference between the estimated values and the actual values that are measured in reality. This difference is a consequence of variables that are missing in the equation.

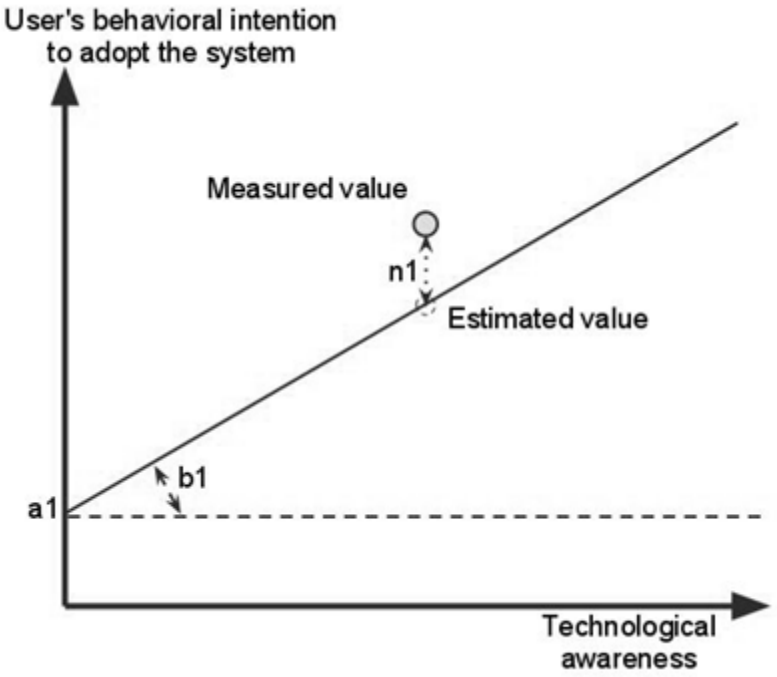


Figure 6.2. User's behavioral intention to adopt the system follows the user's technological awareness in a linear way

The technology adoption model of Davis (1989) and its later extension called Unified Theory of Acceptance and Use of Technology of Venkatesh (2003) also assess that a user's perceived efficiency increases the user's intention to use the system. User's

awareness of the surrounding environment allows him/her to clearly decide what security technology to use and how to reduce waste of energy. I base this claim on the previous analysis of a user's bounded rationality and the consequent need of simplification. Therefore, this study claims that a user's behavioral intention to adopt the system follows the user's context awareness in a linear way.

Our second proposition can be expressed by the following formula:

*(P2) User's behavioral intention to adopt the system = a2 + b2*Environment_Updates + n2*

Where "a2" is another constant, "b2" is a positive coefficient and "n2" takes into account the estimated noise effect created by the variables missing inthe equation.

The theory of trust, control and risk of Das and Teng (2001), which has been applied to information systems by Gallivan and Depledge (2003), describes how controls in place reduce the perceived risk and how that indirectly increases the user's trust in the system. The perceived risk can be decomposed into two parts: (1) the risk that someone steals the user's data, and (2) the risk that the system does not protect the data. The controls can be split into output controls (e.g. a log of all activities done on the mobile to identify intrusions), behavioral controls (e.g. the assessment of how a security algorithm works to protect the user data) or social controls (e.g. observing how surrounding people are behaving and are following the same norm).

User's trust can be towards other people's good intentions or towards the system capacity to protect the user's data. According to this theory a user's awareness of the regulatory environment allows this person to understand the system's controls to reduce the environmental risk, and that increases the user's trust in the system and her intention to adopt it. This study grounds this claim on the previous analysis of user's co-opting relationship with the surrounding mobile users and the consequent need for mutual trust. Therefore, this study claims that a user's behavioral intention to adopt the system follows the user's regulatory awareness in a linear way.

Our third proposition can be expressed by the following formula:

*(P3) User's behavioral intention to adopt the system = a3 + b3*Regulatory_Updates + n3*

Where "a3" is another constant, "b3" is a positive coefficient and "n3" takes into account the noise effect created by the variables missing inthe equation.

6.4 Solutions and Recommendations

Before passing to the technical implementations details of the framework, its business implications are worthwhile investigating.

6.4.1 Business Implications of the Model

Previous works regarding middleware for privacy management (Capra et al., 2003; Hong et al., 2005) have positioned their middleware on the server of the service provider. From the business perspective, this approach allows the service provider to obtain compliance in respect to privacy regulations.

To give more data control ownership to users can lead to new value propositions, which in turn can differentiate a firm from its competitor. A practical example of a firm that is currently gaining money from allowing the users to fine-tune their privacy preferences is the case Allow Ltd described by Angwin and Steel (2011). This London-based company negotiates with marketers on the behalf of users and obtains good deal for the users' data. The business opportunity arises from a proper context-regulation-technology model: in UK (context) the UK's Data Protection Act (regulation) allows user to remove their data from marketers' databases, by means of system (technology) that detects if the data was collected without user's permission.

In addition that I suggest shifting the control of the privacy towards the mobile users, and that enables two additional value propositions:

- Greater performance for the privacy management system: in accordance to proposition 1 and 2 of the model the intention to adopt the system of the user is expected to be greater. Therefore one could expect the mobile user to be willing to pay more for this kind of software.
- Greater trust in the service provider: in accordance to proposition 3 of the model the trust in the system, and indirectly in the service provider is expected to be greater. Therefore one could expect the service provider to gain from the trusted relationship with the mobile user.

These types of business model considerations for mobile platforms have been already addressed in specific workshops, such as the business models for mobile platform (BMMP) workshop. In this sense Bonazzi et al. (2010) have presented a set of business models that allows different key players in the mobile business sector to gain money from privacy management. But that article misses to explain in details how to technically implement each business model. Therefore I wish to extend their business models by

adding a set of design guidelines to the framework.

6.4.2 Framework

Figure 6.3 shows the information flows among the four constructs of the framework illustrated in Figure 6.1.

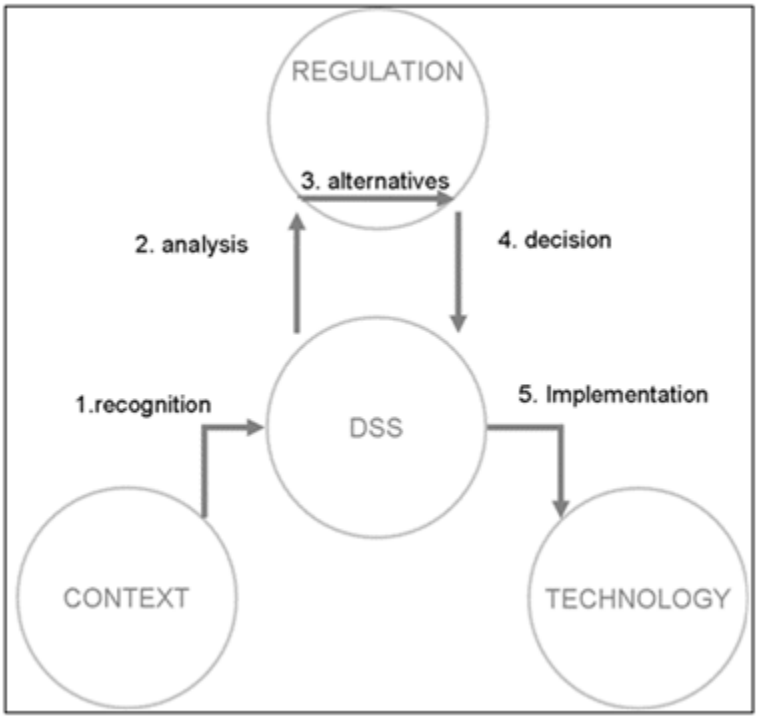


Figure 6.3. Information flow to support risk management decisions

I refer to the literature in decision making and use the process proposed by Straub and Welke (1998) to list the five steps of a security risk plan implemented by my system.

The first step is the recognition of security problem, defined by Straub and Welke (1998:450) as "the identification and formulation of problems with respect to the risk of IS security breaches or computer disaster". In my case, the system gets awareness of the context by collecting data from its sensors (e.g. Wi-Fi, GPS, and Bluetooth).

The second step is risk analysis (defined by Straub and Welke, 1998), "the analysis of the security risk inherent in these identified problem areas; threat identification and prioritization of risks". The system gathers the sensor data and assesses them using the updated roles database to assess the context data.

The third step is the alternatives generation (defined by Straub and Welke, 1998), "the

generation of solutions to meet organizational needs specified during risk analysis". A set of regulations might match the context. The profile that has the highest fit is automatically selected.

The fourth step concerns the decisions (defined by Straub and Welke, 1998), "matching threats with appropriate solutions; selection and prioritization of security projects". For a given threat, the profile suggests a set of actions to be enforced.

The fifth step is the implementation (defined by Straub and Welke, 1998), "realizing the plans by incorporating the solutions into the on-going security of the organization". The set of actions is enforced by the information infrastructure and the tuple time-sensor data-risk profile-actions enforced is recorded in a log by the system, for further compliance analyses.

6.4.3 A Set of Scenarios Illustrating Privacy Risk Management on the Client-side

An information risk management approach in the context awareness lets the user achieve the best security level according to environmental threats she currently faces. The design solution envisaged makes use of state of the art technologies and constantly adapts to the environment to take a proactive stance against privacy risk.

Table 6.2. Operationalization of variables for the scenarios

Construct	**Variable**
Context awareness	**Low**: No information about your location **High**: Information about the privacy risks of your current location is constantly updated
Technological awareness	**Low**: No information about the available technological options available is given from the central system **High**: Information about the available optimal technological configuration to protect your privacy are constantly updated from the central system
Regulatory awareness	**Low**: No information about the option is given to you to configure the system **High**: A set of predefined profiles is constantly updated and displayed to help you choose your privacy option. A log of your previous risk exposure levels can be seen to let you enable or disable the privacy functionalities

I operationalize the construct of the model, as illustrated in Table 6.2. I obtain 2^n different scenarios (Table 6.3), where n is the number of constructs in the model, and 2 is the value that each construct can get (0=Low or 1=High). For the sake of clarity, I briefly describe each scenario, and I link it to existing applications for the Android OS.

Table 6.3. Eight scenarios obtained by combining the three dimensions of theoretical model

	Context awareness	**Technology awareness**	**Regulatory awareness**
Scenario 1	0 (Low)	0 (Low)	0 (Low)
Scenario 2	0 (Low)	0 (Low)	1 (High)
Scenario 3	0 (Low)	1 (High)	0 (Low)
Scenario 4	0 (Low)	1 (High)	1 (High)
Scenario 5	1 (High)	0 (Low)	0 (Low)
Scenario 6	1 (High)	0 (Low)	1 (High)
Scenario 7	1 (High)	1 (High)	0 (Low)
Scenario 8	1 (High)	1 (High)	1 (High)

As the scenario number one does not concern any construct, I start with the second scenario. The second scenario describes the software that contains a set of profiles that have to be manually changed. Predefined rules are constantly updated from a central system. A log of user's previous risk exposure can be seen to let the user enable/ disable the privacy functionalities. For this scenario, two applications for Android already exist: "Privacy Guard" and "The eye". The third scenario describes the software that contains the information about the available optimal technological configuration to protect user's privacy which is constantly updated from the central system. For this scenario, I have found the following applications for Android: "Mobile Security™", "Lookout Mobile Security", "Antivirus Free", "Norton mobile" and "AVG antivirus Pro". The fourth scenario describes the software that combines the information of technological solution and regulation: information about the available optimal technological configuration to protect the user's privacy is constantly updated from the central system. A set of profiles has to be manually changed. Predefined rules are constantly updated from a central system. A log of the user's previous risk exposure can be seen to let you enable /disable

the privacy functionalities. For this scenario, I have found the following application for Android: "MyAndroid protection 2.0". The fifth scenario describes the software that contains the information about the privacy risks of the user's current location and where this information is constantly being updated. For this scenario, I have found the following application for Android: "Glympse". The sixth scenario describes the software that combines the information of context and regulation. For this scenario, I have found the following applications for Android: "Locale", "Setting profiles full" and "Toggle settings". The seventh scenario describes the software that combines the information of context and technological solution. For this scenario, I have found no application for android but web services exists: "General crime", "Homicides" and "Victims". The last scenario includes all of the above three constructs. However, I could not find a corresponding application. Therefore in the rest of the paper I wish to explore the last scenario more in details. I start by illustrating two examples to distinguish the eighth scenario from the other seven, as illustrated by Figure 6.4.

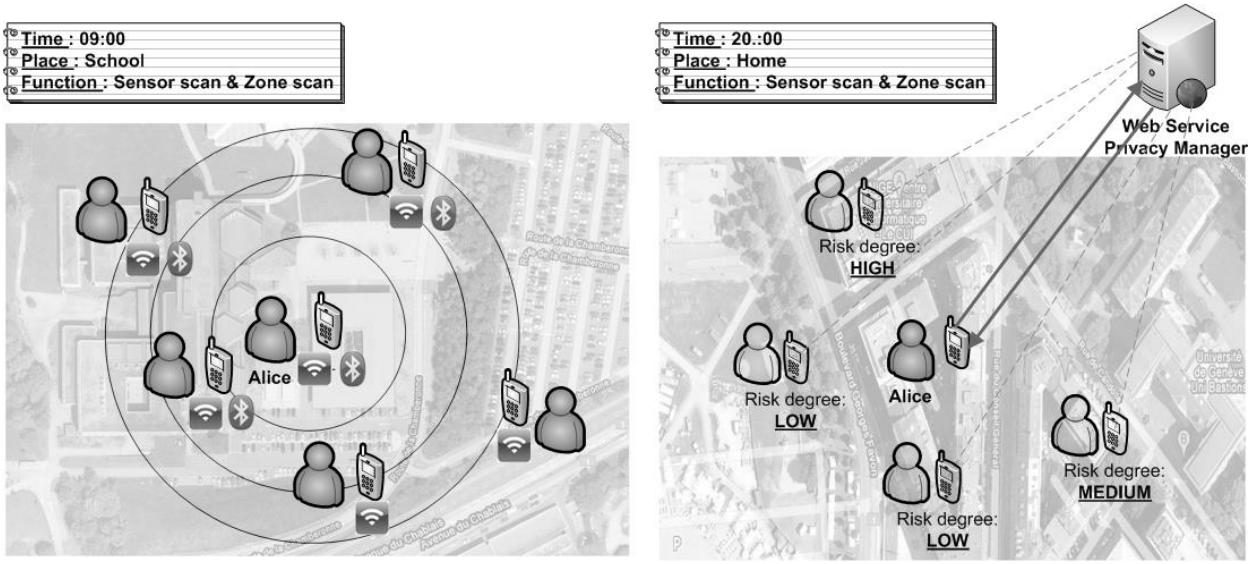


Figure 6.4. Scenario examples

Example 1: Sensors Analysis for Unknown Environments

Alice is a student at the University of Lausanne. She often uses her mobile phone to buy things online. In order to protect her privacy information from the privacy attacks in her surrounding environment, she installed the software "Privacy Manager" on her mobile phone. This software allows Alice to define and configure her privacy preferences, such as degrees of risk, types of potential attacks and corresponding solutions to protect her private information. After the configuration, the software automatically detects the connection information of mobile devices around her via sensor technologies on the phone. Once it identifies any unknown connections during her purchasing procedure, it

responds by taking avoiding action to protect her privacy. For example, one day Alice buys a book when she is in the university. “Privacy Manager” detects that there are many unknown connections around her current position. “Privacy Manager” reports it and adopts two technological solutions (blurring and access control) to protect her online purchasing. After lunch, Alice goes for a walk near the Leman Lake. She wants to book a train ticket with her mobile phone. Again, “Privacy Manager” detects that there is 1 unknown connection. Here reporting a fake location (blurring) is not useful and it should be not implemented to save computational effort and battery energy. Thus “Privacy Manager” implements only “access control” to protect her information.

Example 2: Aggregated Historical Data for Known Environments

After class, Alice goes back home. “Privacy Manager” realizes it is a safe place according to Alice's earlier set configuration and does not implement any protection actions. Now Alice is going to buy a CD online with her mobile phone. “Privacy Manager” allows her phone to connect to the web server and it gets historical data in this zone. This connection has been protected by the security firewall. By combining police database information and private users’ devices configuration details, the privacy manager web service can send information to Alice’s mobile device about the privacy risk of the zone where she is located. Therefore “Privacy Manager” suggests to Alice to increase her privacy protection level since many mobile users have claimed to have had their mobile phones stolen in that neighborhood. Finally, Alice takes Privacy manager’s suggestion and adjusts the risk profile to the “Medium” accordingly.

Table 6.4. The five steps of risk management decision making in two examples

	Example 1 – Part 1	**Example 1 – Part 2**	**Example 2 – Part 1**	**Example 2 – Part 2**
Step 1. recognition	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data. Zone information from infomediary
Step 2. analysis	Many connections	Few connections	Many connections	Many connections. Risky zone.
Step 3. alternatives	“Medium” profile is ranked as first, “Low” profile is ranked as second	“Low” profile is ranked as first, “Medium” profile is ranked as second	“Medium” profile is ranked as first, “Low” profile is ranked as second	“Medium” profile is ranked as first, “Low” profile is ranked as second

Step 4. decision	“Medium” profile is automatically chosen. “Blurring” and “access control” algorithms are chosen to obfuscate the user’s position and to protect user’s data	“Low” profile is automatically chosen. “Access control” algorithm is chosen.	None profile is imposed by the user. No security algorithm is chosen.	“Medium” profile is automatically chosen. “Blurring” and “access control” algorithms are chosen to obfuscate the user’s position and to protect user’s data
Step 5. implementation	“Blurring” and “Access control” are executed	“Access control” is executed	No security algorithm is executed	“Blurring” and “Access control” are executed

Table 6.4 links the two examples to the data flow for decision support presented in Figure 6.3. As previously said the security algorithms have already been implemented with success in mobile applications. Therefore I shall present a prototype that illustrates how to enforce a set of security profile according to contextual privacy risk, which is assessed by means of data sensors collection and zone risk updates sent by a trusted third party.

6.5 Implementation

I implement a prototype of PRIVACY MANAGER according to the design guidelines discussed earlier. The overall goal in designing PRIVACY MANAGER is to examine the feasibility of the approach and to understand the privacy issues possibly involved. I describe the prototype's system architecture, the frameworks used, as well as the graphical user Interface. In doing so, I give implementation details for Symbian platform (Nokia), even though a prototype for Android platform has been developed as well.

6.5.1 System Architecture

Figure 6.5 shows the local privacy manager's interaction with the components of the privacy architecture and the web service.

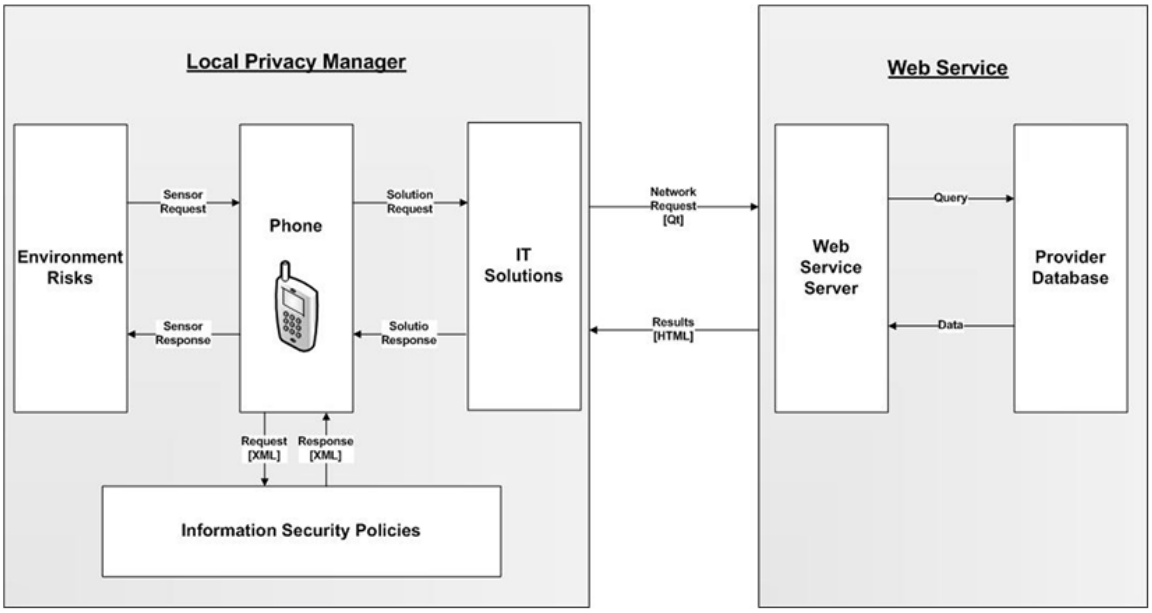


Figure 6.5. System architecture

For the configuration of a user's located privacy policies, I use a XML file to store user's preferences on the phone. It allows the user to edit, create and delete their privacy policies at any time. Detecting the risk of environment is done by using the python socket architecture (Python Software Foundation, 2009); it provides the service of interactive communications between the different sensors of technologies. The local IT privacy solutions can be accessed directly via the information requests of users.

The web service server receives and processes requests vis-à-vis the provider database, before requested data is sent back to the user via QtWeb Network Requests. The resultant information is finally transmitted by the web service to a user-friendly GUI using HTML.

6.5.2 Implementation Details

The application PRIVACY MANAGER for Symbian platform is mostly written in C++, with the toolkit Nokia Qt, which is a cross-platform application and UI framework. It includes a cross-platform class library, integrated development tools and a cross-platform IDE. Using this toolkit, the web-enabled application can be written and deployed across embedded operating systems.

The XML file stores all service provider information, including the risk criteria given by present data, the context of current situation, as well as the corresponding proposed privacy policies.

For the online Web service, I utilized the PHP and a MySQL based framework, which facilitates the development of dynamic Web applications and allows for the exchange of information with web services.

On the client side, the Qt Network Request and Access Manager offers dynamic HTML with integration of Google Maps technologies, which provides localization and auto-update functions, as well as high performance risk degree parsing.

6.5.3 Graphical User Interface

The designed application aims at a clear layout and a high degree of user friendliness. For a complete review of the graphical user interfaces, in the following, I focus on the design of the activity, information and interaction. For the user who is a first time user of this application, a welcome page is proposed and used for the configuration of privacy policies, which explains the purpose and the content of the local risk degree, and its proposed privacy policies on related risk. From this starting page (at the top left corner of Figure 6.6), the user has the option to define the degree of attack for each phone's technology, for example the Bluetooth, Wi-Fi, GPRS and so on. Privacy policies are represented by a list that contains a large related security application which could be selected by the user to enforce the rule that fits the current risk degree. All the information about the status change is stored in a file for future use of compliance checking against privacy policies. If a technology or related security application is not listed in the privacy policies list, users can create a new one at any time. Once the local privacy policies are configured by the user, then the 3 main functions of application of the privacy manager are available for use.

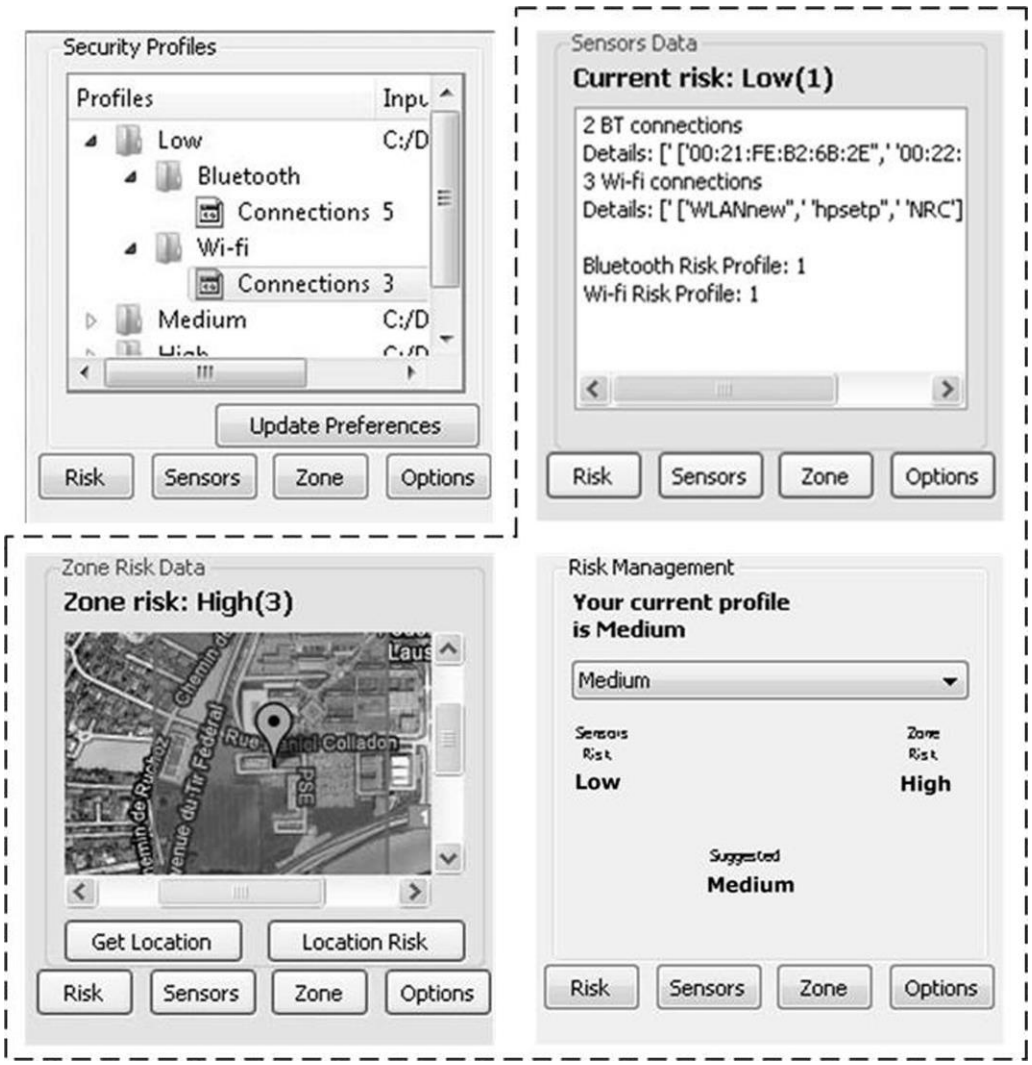


Figure 6.6. Graphic user interfaces: Configuration interfaces (top left corner); Sensor analysis interfaces (top right corner); Zone risk analysis interfaces (bottom left corner); Risk management interface (bottom right corner)

Recalling Table 6.4, I illustrate how to implement the five steps of the decision support for privacy risk management. The first function offers a physical sensor that continuously collects diverse information from the environment (at the top right corner of Figure 6.6). It keeps detecting context information of the technologies of different devices around the user, in order to get an updated context degree of risk in real time, including the technology's name, its MAC address and the specific identification, as well as the number of connections for each technology. In addition, each technology's risk profile is calculated automatically to conform to the user's risk degree configuration. The information of ranking, which represents the average of current risk between all of the technologies detected— is presented at the bottom of the screen.

The second function shows the information about zone risk (at the bottom left corner of Figure 6.6), which includes 2 tasks: displaying the user's current position and obtaining this position's historical risk.

When clicking the button “Get location”, the phone component GPS (Global Positioning System) will be activated and get the user's current position, including the address information of that latitude and longitude. These position values finally are sent to a Web Service Server by PRIVACY MANAGER.

Reverse Geocoding (Google Inc., 2010) is a service of Google Maps available through the Web Server, which can be used to translate latitude and longitude information into an address. This feature is very important for interactions with the user, since positioning technologies provide coordinate information (i.e. “Latitude = 46.5222, Longitude = 6.583555”) which is not meaningful to the end user, and users provide location information in the form of an address (i.e. “UNIL Dorigny, 1015 Chavannes-près-Renens, Switzerland”) which is not useful to software and positioning technologies. Reverse Geocoding bridges the gap between the end user and the positioning technology and enables user interaction with applications, as well as enabling the other types of services by supplying location information to the software in a usable format. For the sake of simplicity, I did not implement a secure connection between the mobile device and the web server even though I adware of its importance.

In considering the usability aspects and by involving the users, the map user interface service is added in the Web server. This is the ability to display location information in the form of a map, including landmarks and routes, on the mobile phone screen. This service has various levels of control, I can add or remove certain related features on a map, such as add a polygon or showing a significant marker on the map. Users will also be able to select different map views such as regular, satellite, and hybrid that are integrated on phone screen.

Focusing on a zone's risk data sharing, the second button named “location risk” which is set up to allow the phone to contact the online web service to send the information regarding the user's current located risk data to the Web Service Server This web server provides interface to users who authorize to access the application. A database is used to store all information about user's risk. Then the web server will return to the users a risk level which is calculated by the average in a similar area in real time (i.e. each 10 minutes). And here the similar area is defined as a specified area, which is a circumference of a circle with its radius of 500 meters. Finally, the web service will deliver in return the average of the risk degree reported by others users in the same geographic area in an earlier period of time. In order to distinguish the degree of risk in a specific area, an alarm system is integrated, and by using different colors on the map to

signify the degree of risk, for example, blue signifies low risk in this area and red signifies high risk.

The last function lists the average degree of risk obtained previously (at the bottom right corner of Figure 6.6), including the sensors risk (risk value from Wi-Fi and Bluetooth) and the zone risk (risk value from current location). PRIVACY MANAGER calculates the average of sensor risk and zone risk, and provides the final risk value to help user make the decision, which will be used to execute the related security applications in order to deal with the current risk.

6.6 Discussions

A first evaluation has been done within experts in Nokia, to whom the prototype has been presented. Although the idea has been accepted as innovative most of the feedback I received regarding future improvements concerned the user interface and the need to include in the prototype an example of a security enforcing policy.

A second evaluation of the prototype has been done within a small sample of mobile users to assess the software usability and the users' intention to use it. I have conducted a pre-test of my prototype using ten volunteers in a controlled environment. Since I cannot perform a benchmark with existing solutions, I opted for a scenario-based test as suggested by Rosson and Carroll (2002). The volunteers were asked to read the two parts of the scenario 8 presented in the previous section. Then they were asked to perform it using an Android mobile phone, on which the Privacy Manager prototype was installed. Since I did not fully implement the security algorithm simulated that part. At the end of the experience the volunteers were asked to answer questions concerning technology acceptance taken from Vankestesh et al. (2003). The answers I obtained from the volunteers came as partially unexpected. Most users declared they liked the application and they found it useful but that they did not want to use it in their everyday life. It turned out that most users did not feel their privacy menaced and they did not want to be constrained by this kind of application. Yet the same users agreed they might have been exposed to privacy risks and they declared that if the application informs the user of the consequences of each privacy risk, then they would find it useful. Although the sample size does not allow any statistical interpretation, I am currently investigating more in details the underlying causes behind the test results. If they are due to an effect of adverse selection, as suggested by Anderson (2001), then this impacts the requirements for software development, since the application should protect and inform the user in the proper way. Moreover it could be that for high maintenance information system for security this statement is not always correct. This point is worth a further analysis, since it would have a significant impact on design requirements.

6.7 Future Research Directions

In the close future I am going to improve the prototype using the outcome of our preliminary test before testing it on a larger scale using the guidelines illustrated in Table 6.5. Yet it is believed that by now the proposed design makes a contribution since it is a first attempt at empowering the user with a system that allows him to manage the dynamically privacy risk according to his own preference and perceptions. Future research directions envisage from the work are the following ones:

- **Extending the model, e.g. adding more contingency factors**: in this article I did not take into account other seminal researches, like the five-force model of Porter (1998).
- **Adding more business models for competitive users**, e.g. for a distributed infomediary: as previously mentioned the informediary does not have to be a centralized entity. In the extreme case where all the computation is done among mobile users in a distributed fashion the infomediary business model might not work as described here.
- **Technical improvements for the prototype**: a greater amount of effort could be spent analyzing the ways I could improve the human-computer interaction. Security algorithms have to be translated in a common format to be processed by the application, although this has not be done here for technical limitations of the language used. Each protection algorithm has its own limitations. I cite Krumm (2009) for a good review of their strengths and weakness, and this study suggests reading Shabtai et al. (2010) for a security assessment of Android OS.

Table 6.5. Testing guidelines

Testable Proposition	Testing guideline
P1: User's awareness of the security technologies available supports the achievement of user's identity protection in a linear way.	Measures how the increase of technology updates affects the user's intention to adopt the system
P2: User's awareness of the surrounding environment allows to clearly decide the security technology to use and reduce waste of energy	Measures how the increase of context updates affects the user's intention to adopt the system
P3: user's awareness of the regulatory environment allows to understand the systems controls to reduce the environmental risk, and that increase the user's trust on the system and her intention to adopt it	Measures how the increase of regulatory updates affects the user's intention to adopt the system

6.8 Conclusion

This paper has presented a model for decision support system regarding privacy risk management associated with pervasive technologies, which it is believed is topic with growing importance in these days. The research question focused on context-aware technologies used by a user that I assume as opportunistic and rationally bounded. The theoretical model is the first to take into account the four contingency factors (business, technology, regulation and user behavior) that impacts mobile privacy risk management. I illustrated how the theoretical model allows to benchmark all privacy management applications on the market and to extend such market towards a new type of software. The developed prototype is the first middleware that combines a transparent and reflective approach, as well as a decentralized (sensor analysis) and centralized (zone risk analysis) risk management mechanism. I followed the methodology proposed by Peffers et al. (2007) to structure my design research study, and I used the scenario-based approach of Rosson and Carroll (2002) during the development phase. I presented the results to an audience that was a balanced mix of technology-oriented and management-oriented experts at Nokia and I performed over a set of mobile users to assess their intention to adopt the new system. The guidelines for a new round of tests over a larger sample of users have been illustrated in the previous section.

This study has some limitations. As the development of fully operational prototype is still limited in the results by the application that runs on the phone. However, it is believed that this work is well aligned with those who believe that a risk management approach is required to assure information security, and that privacy management in pervasive computing is a complex and multidimensional issue that should be addressed taking into consideration time and place. The contention is that the model is more flexible than previous ones, since it has been conceived to be updated in time and to mitigate and record threats. Some interesting future researches are envisaged, which might involve privacy risk management in the sector of mobile payment, adding more business models for competitive users, and technical improvements for the prototype.

6.9 References

Acquisti A., Dingledine R., and Syverson P. 2003. “On the economics of anonymity,” in R. N. Wright, editor, *Financial Cryptography*. Springer-Verlag, LNCS 2742.

Anderson, R. 2001. “Why information security is hard-an economic perspective,” in Proceedings 17th Annual Computer Security Applications Conference, 2001, New Orleans, Louisiana: IEEE, pp. 358-365.

Angwin, J., and Steel, E. 2011. “Web's Hot New Commodity: Privacy”, retrieved March 15, 2011, available on: http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html

Barkhuus, L. 2004. “Privacy in Location-Based Services, Concern vs. Coolness,” in Proceedings of Workshop paper in Mobile HCI 2004 workshop: Location System Privacy and Control. Glasgow, UK.

Blakley, B., McDermott, E., and Geer, D. 2001. “Information security is information risk management,” in Proceedings of the 2001 workshop on New security paradigms. Cloudcroft, New Mexico.

Bonazzi R., Fritscher B. and Pigneur Y. 2010. “Business Model Considerations for Privacy Protection in a Mobile Location Based Context,” in Proceedings of the Second International Workshop on Business Models for Mobile Platforms, Berlin, Germany, IEEE.

Capra, L., Emmerich, W., and Mascolo, C. 2003. “CARISMA: Context-aware reflective middleware system for mobile applications,” *IEEE Transactions on software engineering* (29:10), pp. 929-945.

Chen, G., and Kotz, D. 2000. “A survey of context-aware mobile computing research,” Tech. Rep. TR2000-381, Dartmouth, November 2000.

Dahlberg, T., Mallat, N., Ondrus, J., and Zmijewska, A. 2008. “Past, present and future of mobile payments research: A literature review,” *Electronic Commerce Research and Applications* (7:2), pp. 165-181.

Das, T. K., and Teng, B. S. 2000. “A resource-based theory of strategic alliances,” *Journal of management* (26:1), pp.31-61.

Davis, F. D. 1989. “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” *Management Information Systems Quarterly* (13:3), pp. 319-340.

Fishbein, M., and Ajzen, I. 1975. "Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading," Mass.: Addison-Wesley Pub.

Freudiger, J., Manshaei, M., Hubaux, J. P., and Parkes, D. C. 2009. "On Non-Cooperative Location Privacy: A Game-Theoretic Analysis," in Proceedings of ACM Conference on Computer and Communications Security (CCS), Chicago, USA.

Gallivan, M. J., and Depledge, G. 2003. "Trust, control and the role of interorganizational systems in electronic partnerships," *Information Systems Journal* (13:2), pp. 159-190.

Google Inc. 2010. "Google Maps API – Geocoding," retrieved March 15, 2011, available on: http://code.google.com/apis/maps/documentation/services.html#Geocoding

Gregor, S., and Jones, D. 2007. "The Anatomy of a Design Theory," *Journal of the Association for Information Systems* (8:5), pp. 312-325.

Hagel 3rd, J., and Singer, M. 1999. Net Worth, Harvard Business Press.

Herrmann, D. S. 2007. "Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI", Auerbach Publications.

Hong, D., Yuan, M., and Shen, V. Y.(2005. "Dynamic privacy management: a plug-in service for the middleware in pervasive computing," in proceedings of the 7th international conference on Human computer interaction with mobile devices & services. Salzburg, Austria.

Krumm, J. 2009. "A survey of computational location privacy," *Personal and Ubiquitous Computing* (136), pp. 391-399.

March, S. T., and Smith, G. F. 1995. "Design and natural science research on information technology," *Decision Support Systems* (15:4), pp. 251-266.

Manasdeep, A. S., Jolly, D. S., Singh, A. K., Srivastava, M. A., and Singh, M. S. 2010. "A Proposed Model for Data Privacy providing Legal Protection by E-Court," *International Journal of Engineering Science and Technology* (2:4), pp. 649 -657.

Massey, A. K., Otto, P. N., Hayward, L. J., and Antón, A. I. 2009. "Evaluating existing security and privacy requirements for legal compliance," *Requirements Engineering* (15:1), pp. 119-137.

Moore, G. C., and Benbasat, I. 1991. "Development of an instrument to measure the perceptions of adopting an information technology innovation," *Information systems research* (2:3), pp. 192-222.

Nalebuff, B., and Brandenburger, A. 1997. "Co-opetition: Competitive and cooperative business strategies for the digital economy," *Strategy & Leadership* (25:6), pp. 28-35.

Oxford English Dictionary. 2010. "Privacy," retrieved March 15, 2011, available on: http://www.askoxford.com

Palen, L., and Dourish, P. 2003. "Unpacking privacy for a networked world," in Proceedings of the ACM Special Interest Group on Computer-Human Interaction (SIGCHI) conference on Human factors in computing systems, Florida, USA.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45-77.

Ponemon, L. 2000. "Privacy Risk Management," presentation for The National Council of Higher Education Loan Programs. Long Beach, CA, USA.

Porter, M. E. 1998. "Competitive Strategy: Techniques for Analyzing Industries and Competitors," Free Press.

Python Software Foundation. 2010. "Socket — Low-level networking interface — Python v2.6.4 documentation," retrieved March 15, 2011, available on: http://docs.python.org/library/socket.html

Radner, R. 2000. "Costly and bounded rationality in individual and team decision-making," *Industrial and Corporate Change* (9:4), pp. 623-655.

Radner, R., and Marschak, J. 1954. "Note on some proposed decision criteria," in Thrall et al., editors, Decision Processes. John Wiley.

Reagle, J., and Cranor, L. F. 1999. "The platform for privacy preferences," *Communications of the ACM* (42:2), pp. 55.

Rosson, M. B., and Carroll, J. M. 2002. "Usability engineering: scenario-based development of human-computer interaction," Morgan Kaufmann Pub.

Savage, L. J. 1954. "The foundations of statistics," Wiley: New York (2nd edn, 1972, Dover: New York)

Schilit, B., Adams, N., and Want, R. 1994. "Context-aware computing applications," in Proceedings of the workshop on mobile computing systems and application. Santa Cruz, CA, pp. 85-90.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., and Glezer, C. 2010. "Google Android: A Comprehensive Security Assessment," *IEEE Security & Privacy* (8:2), pp. 35-44.

Sheppard, B. H., Hartwick, J., and Warshaw, P. R. 1988. "The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research," *Journal of Consumer Research* (15:3), pp. 325-343.

Shokri, R., Freudiger, J., Jadliwala, M., and Hubaux, J. P. 2009. "A Distortion-Based Metric for Location Privacy," in Proceedings of ACM Workshop on Privacy in the Electronic Society (WPES), Chicago, IL; USA.

Simon, H. A. 1987. "Bounded Rationality," In The New Palgrave, edited by J. Eatwell et al. London: Maemillan.

Simon, H. A.(1959. "Theories of decision-making in economics and behavioral science," *The American Economic Review* (49:3), pp. 253-283.

Straub, D. W., and Welke, R. J. 1998. "Coping with systems risk: Security planning models for management decision-making," *Management Information Systems Quarterly* (22:4), pp. 441-469.

Thompson, J. D. 1967. "Organizations in Action Social Science Bases of Administrative Theory," McGraw-Hill Companies.

Tversky, A. and Kahncman, D. 1974. "Judgment under uncertainty: Heuristics and biases," *Science* (28:5), pp. 1124-1134.

Venkatesh, V., Morris, M., Davis, G., and Davis, F. 2003. "User Acceptance of Information Technology: Toward a Unified View," *Management Information Systems Quarterly* (27:3), pp. 425-478.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *Management Information Systems Quarterly* (26:2), pp. 13-23.

Appendix B

Privacy-Friendly Business Models for Location-Based Mobile Services

Published in the Journal of Theoretical and Applied Electronic Commerce Research,
Volume 6, Issue 2, August 2011, pages 90-107
Publisher: Universidad de Talca
ISSN: 0718-1-1876

Abstract This paper presents a theoretical model to analyze the privacy issues involved in business models for location-based mobile services. I report the results of an exploratory field experiment in Switzerland that assessed the factors driving the net payoff to users of mobile businesses. This study found that (1) the personal data disclosed by users has a negative effect on user payoff; (2) the amount of personalization available has a direct and positive effect, as well as a moderating effect on the relationship between personal data disclosed and user's payoff; and (3) the amount of control over a user's personal data has a direct and positive effect, as well as a moderating effect on the relationship between personal data disclosed and user's payoff. The results suggest that privacy protection could be the main value proposition in the B2C mobile market. From the theoretical model, I derive a set of guidelines to design a privacy-friendly business model pattern for third-party services. I discuss four examples to show how the mobile platform can play a key role in the implementation of these new business models.

Keywords: Privacy, Location-based services, Business model, Design science, Information systems, Personal data disclosed, User's payoff, Personalization available, Control over user personal data

7.1 Introduction

New regulatory requirements, such as the guidelines given by the Organization for Economic Co-operation and Development (2002), and consumer concerns are driving companies to consider more privacy-friendly policies, often conflicting with their desire to leverage customer data.

On one hand, close proximity of potential customers and access to their real intentions regarding purchases of services has a real value for mobile location-based service providers, whose market revenues are expected to reach more than $12.7 billion by 2014 (Gibson and Holden, 2010). On the other hand, the collection of data about consumers is constrained by their privacy right, which I refer as "the right to be left alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned" (Black's Law Dictionary, as cited in Hagel et al., 1999). Improper or non-existent control over disclosure can be the root cause of privacy issues and concerns about the privacy of personally identifiable information. The challenge for companies therefore is to reduce user data collection to the lowest sustainable level possible while providing a profitable service.

Much research to date has focused on understanding the relationship between user privacy concerns and the willingness to disclose personal information to online companies (e.g., Malhotra et al., 2004; Dinev and Hart, 2006). In this sense, user privacy concerns are found to be one major predictor of the willingness to provide personal information. I argue that previous research focuses only on user choice to either withhold or release personal information. This decision is one component of user payoff, which is considered as "the degree to which a mobile user perceives as fair the benefits he or she receives in return for the release of personal information" (Son and Kim, 2008). If user's payoff is not assured, data security is in peril (Anderson, 2001).

In the rest of the paper, I focus on location-based services (LBS) offered in the Business to Consumer (B2C) market, such as navigation, information, advertising, tracking, and billing (Glaglis et al., 2002). I exclude emergency services from the analysis because users of those services deal differently with privacy concerns (Sheng et al., 2008). Location-based applications open new opportunities for business models in the mobile sector. Hence, I primarily address an audience mainly composed of stakeholders in mobile services who seek guidelines to develop privacy-friendly business models. I also wish to raise the interest level of the broader audience of information system researchers and practitioners who are concerned with the impact of business model practices on the design of the IT artifact (Benbasat and Zmud, 2003). My research question is this: *how*

should one design a privacy-friendly business model that can sustainably maximize(s) the payoff to the user of a location-based mobile service user?

The remainder of the paper proceeds as follows. The next section reviews some of the related work in privacy and LBS that addresses my research question, and I define a set of sub-research questions to fill the remaining gaps. The section 7.3 presents the methodology I use to address these sub-questions. The section 7.4 introduces the theoretical model and presents empirical evidence to support it. In the 7.5 section, I implement the theoretical model to derive a set of guidelines to obtain privacy-friendly business models. Section 7.6 presents a set of possible instantiations of the guidelines using real companies as potential candidates. In the final section, I discuss the implications of the analysis, draw some conclusions, and propose further possible research.

7.2 Literature Review

In this section I briefly highlight a set of well-known works that help in answering my research question. For a more complete literature review of privacy management technologies, I suggest reading (Danezis and Gurses, 2000). After outlining the remaining gaps in the literature, I derive a set of sub-research questions that remain to be answered.

The success of the privacy management solution relies on the development of technology and regulations to protect personal information (Anderson, 2009). Privacy is a dynamic and dialectic process of give and take between and among technical and social entities in ever-present and natural tension with the simultaneous need for information to be made public (Palen and Dourish, 2003). I therefore understand the mobile user and the service provider as both competing and cooperating to gain access to a valuable resource (mobile user's data) (Nalebuff and Branderbuger, 1997).

Research aimed at surveying and classifying solutions to managing online privacy was also conducted in order to evaluate the different factors influencing collaboration and their various impacts (Hui et al., 2007; Lancelot Miltgen, 2010). It has been found that different types of privacy assurance have different impacts on people's willingness to disclose personal information; for example, the existence of a privacy statement induces more subjects to disclose personal information, but that of a privacy seal does not (Hui et al., 2007). It has also been proved that monetary incentives had a positive influence on disclosure whereas information request has a negative influence, suggesting that firms do not collect consumer data unless they intend to use them. In addition to that, cross-cultural analyses show that young English people have more concerns about privacy than French people, resulting in greater perceived risks about data disclosure (Lancelot

Miltgen, 2010).

Among prior studies focusing on the online business sector, none has examined the specific domain of mobile business settings. Regardless of the fact that there are some similarities between online and mobile businesses, location-based mobile services have their own unique features that make them different from online businesses. I therefore derive the following sub-research question:

R1: What is the specificity of privacy management in the location-based mobile B2C market?

Much research has been dedicated to understanding the relationship between users' privacy concerns and their response behaviors (e.g., to develop software such as Smokescreen (Malhotra et al., 2004)). This research reveals that Internet users' information privacy concerns are a major antecedent to the willingness to provide personal information to online companies. Previous research shows the influences between perceived justice and procedural justice, as well as perceived justice and distributive justice (Malhotra et al., 2004; Son and Kim, 2008).

Previous research has also suggested that control over personal data is an important component in creating a good relationship with customers. For example, most people want to have more control over the use of personal data to restrict unwanted commercial advertisements (Phelps et al., 2000). Issues of information control are essential in increasing the likelihood of consumers contributing information to online firms (Stewart and Segars, 2002).

Another important issue is the value of personalization. According to (Chellappa and Sin, 2005), service personalization is said to depend on two factors: 1) a company's ability to acquire and process customer information and 2) customers' willingness to share information and use personalized services. They develop a model to predict consumers' usage of online personalization as a result of the trade-off between those consumers' perceived value of personalization of services and their concern for privacy. Those studies do not, however, provide guidelines for the design of a business model for mobile services. Therefore, my second sub-research question is:

R2: Which business model components allow a high level of mobile users' payoff while keeping the collected data to a minimum?

Finally, comprehensive analyses of consumer privacy concerns and Internet-related business have proposed (Lancelot Miltgen, 2010) four different clusters of users: well-intended, negotiator, unconcerned, and reticent. These analyses suggest that when considering the approach to e-commerce, I should also respect the different groups of

Internet users. Such results appear to not have strong statistical relevance. Hence, my third sub-question is:

R3: How should the differences in payoff among privacy risk–neutral and privacy risk–averse mobile users be addressed?

The following section illustrates how I intend to address my sub-research questions to answer the initial research question.

7.3 Methodology

Based on the relevant literatures, I create an artifact in the form of a model (March and Smith, 1995) to express the relationship between user payoff and the extent of personal data disclosed.

I adopt a design science research methodology, and I refer to existing guidelines for design theories (Gregor and Jones, 2007). The theories for design and action "give explicit prescriptions on how to design and develop an artifact, whether it is a technological product or a managerial intervention" (Gregor and Jones, 2007). Therefore, I advance in three steps, as illustrated in the Figure 7.1.

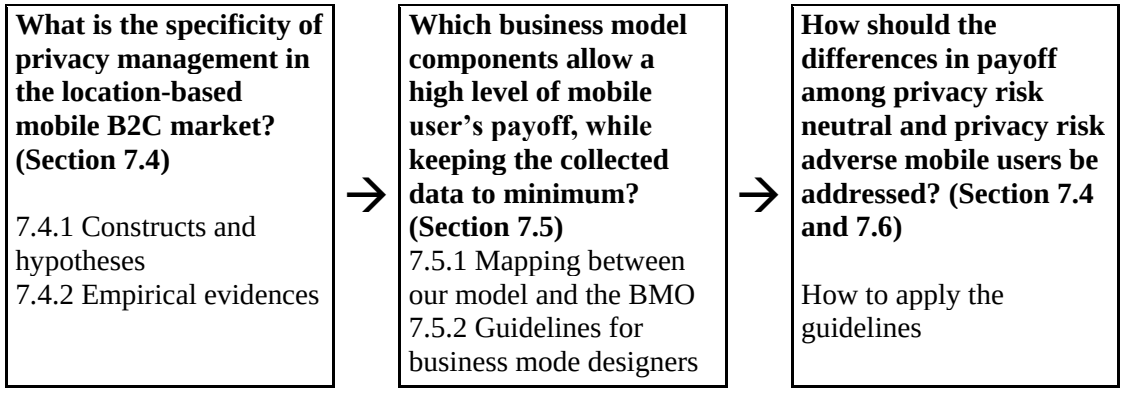


Figure 7.1. Process of methodology

An information system design theory (ISDT) should define its purpose and scope, that is, the boundaries of a theory. In my case, the theory concerns data management for privacy risk reduction of LBS. The second element of an ISDT is the representations of the entities of interest in the theory, that is, constructs. The principles of form and function define the structure, organization, and functioning of the design product or design method. The justificatory knowledge provides an explanation of why an artifact is constructed as it is and why it works.

Accordingly, the section 7.4 introduces a model composed of four constructs and derive hypotheses concerning the interaction among constructs. In doing so, I ground the claims on existing theories of control (Das and Teng, 2001), as well as perceived justice and equity theory (used in Son and Kim, 2008).

The evaluation strategy of testable propositions uses surveys as an ex post artificial type of evaluation (Pries-Heje et al., 2008). The resulting outcomes provide answers to the first sub-question.

Our second sub-question concerns the means by which the design is brought into being—a process involving agents and actions. To address this sub-question, section 7.5 starts by mapping the constructs with the constructs of the Business Model Ontology (BMO) (Osterwalder and Pigneur, 2010), a tool often used by startups and multinational companies to represent their business models. Because the model has only four constructs and the BMO is composed of nine elements, I rely on an existing type of business model (the "infomediary pattern") to fill in the blanks and derive a set of guidelines for business model designers to obtain privacy-friendly business models.

To properly answer my third sub-question, I need to test the feasibility of the proposed guidelines. Hence, section 7.6 presents a set of instantiations of the business model pattern. Whereas a theory is an abstract expression of ideas about phenomena in the physical world, instantiated artifacts are things in the physical world. Thus, I illustrate four examples of application for the guidelines by naming four existing companies as possible candidates.

7.4 Model

In this section, I present the theoretical model, following the guidelines to describe a theory (Sutton and Staw, 1995). I start by presenting the constructs and by augmenting the hypotheses using the references which are introduced in the literature review. Then I show the correlations among components, which I derive from the test results.

7.4.1 Constructs and Hypotheses

Our model is composed of four constructs, the definitions of which are derived from previous research summarized in Table 7.1.

Table 7.1. Definitions of each construct of model

Construct	Definition	Source
Personal data disclosed	Degree to which a mobile user perceives about his or her personal data is disclosed by the mobile service companies.	Son and Kim (2008)
User's payoff	Degree to which a mobile user perceives as fair the benefits he or she receives from mobile service companies in return for the release of personal information.	Ibid.
Personalization available	Degree of fairness that a mobile user perceives about mobile service companies' treatment related to information privacy.	Ibid.
Control effort	Degree to which a mobile user perceives that mobile service companies give him or her procedures for control of information privacy and make him or her aware of the procedures.	Ibid.

Because previous studies have already focused on the effects of antecedents, this study focuses on the effects among antecedents. I refer to (Son and Kim, 2008) and claim that the "Degree to which a mobile user perceives as fair the benefits he or she receives from mobile service companies in return for providing personal information" (i.e., "user payoff" in the model) is found to be one major predictor for "personal data disclosed," which is defined as the degree to which a mobile user perceives whether personal data is disclosed by the mobile service company. Therefore, I propose a model of user payoff as indicated in Figure 7.2.

H1: The personal data disclosed has a negative effect on user payoff.

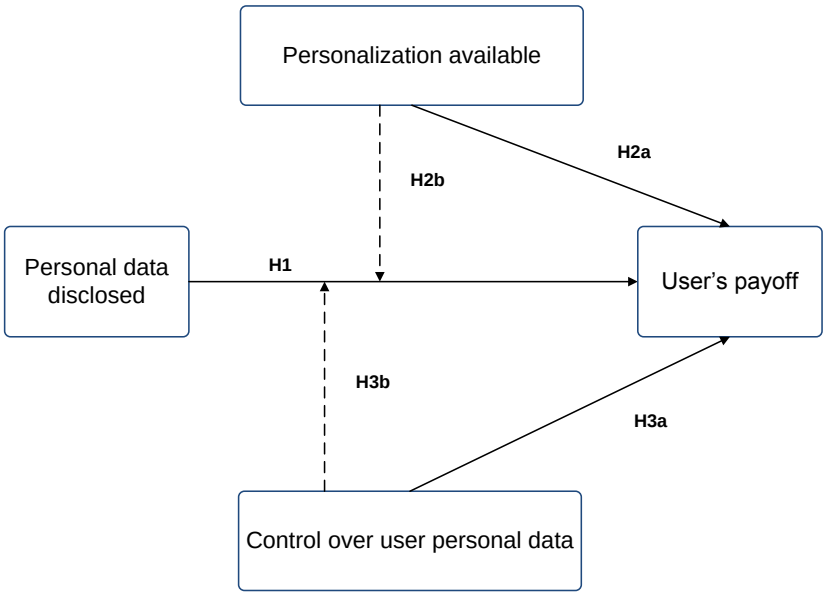


Figure 7.2. Model of user payoff

In exchange for user data, the m-commerce provider could offer a service, which is either standard or fully customized. I introduce the concept of service personalization, which is defined as the degree of fairness that a mobile user perceives relative to mobile service company's treatment of information privacy. As I previously mentioned in the literature review, service personalization depends on customer willingness to share information and use personalized services (Chellappa and Sin, 2005). It is natural to expect a positive relationship between the amount of personalization available and users' benefit.

H2: The amount of personalization available has: (a) a direct and positive effect on user payoff, and (b) a moderating effect on the relationship between personal data disclosed and user's payoff.

Because consumers take relatively high risks by submitting personal data to the mobile service provider, data controls over user personal data using privacy metrics (Herrmann, 2007) are a useful tool to decrease user concern for privacy risks. Lack of such controls decreases mobile user trust in the provider (Das and Teng, 2001) and lowers the perceived payoff. Hence, I propose that:

H3: The amount of control over users' personal data has: (a) a direct and positive effect on user payoff, and (b) a moderating effect on the relationship between personal data disclosed and user's payoff.

7.4.2 Test Design

In this study, I want to test the effect of the data disclosure, service personalization, and data control over user payoff. I test the effect of such constructs in two steps.

Because I am dealing mostly with perceptions, I test the effect of the model using scenario-based surveys. This form of assessment has been successfully implemented in previous studies on information system security (Barrett et al., 2006).

As illustrated in Table 7.2, I designed 2n different scenarios, where n is the number of constructs in the model that I want to test and 2 is the number of values that each construct can take (0 = Low or 1 = High). All subjects are to receive scenario 0 (step 1), which tests the initial user's payoff:

Your mobile phone operator (e.g., Swisscom) offers you a new service – a discount zone. With this service, you can get exclusive information and access to exclusive personal time and location-limited discounts on a diversity of products and services (e.g., books, pizzas, electronics, cinema, etc.) near your current location. For example, if you are interested in acquiring an iPad, Swisscom will automatically send an SMS to your mobile phone when there is a special and exclusive' discount for iPads near your location.

There are two ways to register for this service: a paid yearly subscription that gives access to the full service, or a free registration. To get free registration, you must provide additional information, including your name, gender, and country of residence. Your data are stored according to privacy laws and sold to discount providers.

In step 2, I split the overall sample into sub-groups. Each sub-group will get a variation of the initial scenario and be asked to express the new user's payoff.

Table 7.2. Scenarios

	Data disclosure	**Service personalization**	**Data control**
Scenario 0	0 (Low)	0 (Low)	0 (Low)
Scenario 1	0 (Low)	0 (Low)	1 (High)
Scenario 2	0 (Low)	1 (High)	0 (Low)
Scenario 3	0 (Low)	1 (High)	1 (High)
Scenario 4	1 (High)	0 (Low)	0 (Low)
Scenario 5	1 (High)	0 (Low)	1 (High)
Scenario 6	1 (High)	1 (High)	0 (Low)
Scenario 7	1 (High)	1 (High)	1 (High)

As Table 7.3 indicates, each variation of the scenario operationalizes one construct of the model and is derived from previous works.

Table 7.3. Operationalization of variables for the scenarios

Construct	**Variable**	**Sources**
Personal data disclosed	Low: Name, gender, country of residence High: Name, gender, country of residence personal phone number, current debt, checking & saving balance and other investment	Hui et al. (2007)
Personalization available	Low: None High: "You have the possibility to customize your personal preferences to get the discount information you desire."	Awad and Krishnan (2006)
Control over user personal	Low: None High: "You still can see which data is sold to the discount providers and set a limited amount of options regarding such disclosure."	Malhotra et al., (2004)

To measure the user's payoff, I derive three items from previous studies. A set of control variables is included as well, as shown in Table 7.4.

Table 7.4. Operationalization of variables for the survey

Construct	Variable	Sources
User's payoff	1) In this case, my need to obtain the discount opportunity provided by this service is greater than my concern about privacy. 2) My interest in the discounts I can obtain from this service overrides my concerns of possible risk or vulnerability that I may have regarding my privacy. 3) My interest to obtain this discount service makes me suppress my privacy concerns.	Dinev and Hart (2006)
User's familiarity with LBS	A) I am familiar with Smartphones. B) I am familiar with mobile services using my location	---
User's perception of country risk	C) Ibelieve that regulations in my country require personal data to be properly protected	Lancelot Miltigen (2010)
User's perception of Internet risk	D1) When I share data with a mobile service I believe that there is enough protection and that privacy risk is low D2) When I share data with a mobile service I believe that there is a safe environment to perform economic transactions D3) When I share data with a mobile service I believe that there is a safe environment to perform taks related to work or private life	Lancelot Miltigen (2010)
User's techniques for privacy protection	E1) Concerning my personal data I always share my real identity E2) Concerning my personal data I always use a pseudonymous E3) Concerning my personal data I always give false information E4) Concerning my personal data I do not answer to personal questions if they are not mendatory	Lancelot Miltigen (2010)

7.4.3 Results

I invited a group of subjects to fill out a survey concerning privacy issues in a location-based mobile service context. The descriptive statistics of the sample are presented in Table 7.5. The sampling frame consisted of 187 bachelor's students at the business faculty of a Swiss university who attended the course in information systems. The sample is representative for the overall population of smart phone mobile users in Europe.

The subjects were between 19 and 24 years of age, and 70 percent of the sample was male. This corresponds well with the recent figures on smart phone users in Europe: 27% between 16 and 24 years of age and 67% male, according to Forrester Research, Inc (Husson, 2010). From previous research, I derived two items to test for cultural effect. I can compare to the English sample of (Lancelot Miltgen, 2010) that had the same sample distribution.

Table 7.5. Descriptive statistics

Subject's background	
Gender	male: 70.06%
Familiarity with smart phone	mean=5.431, SD=1.820
Familiarity with location-based service	mean=4.180, SD=2.067
Global concerns	mean=3.402, SD=1.372
Concerns for mobile sector	mean=3.168, SD=1.185
Main constructs	
User's payoff	mean=3.768, SD=1.559
Personal data disclosed	high: 53.48%
Personalization available	high: 58.29%
Control over personal data	high: 56.68%

Table 7.6 presents information on the correlation coefficients between all the constructs. I observe a relatively high correlation coefficient between global concerns for privacy and concerns in the mobile service sector (0.656). Because both variables deal with attitude to privacy risks, it is natural to expect a positive linkage between them. I did not otherwise observe any significant proof of multicollinearity among the variables.

Table 7.6. Correlation among variables

		01 **gender**	02 **fsp**	03 **fmsl**	04 **gp**	05 **mss**	06 **apdd**	07 **payoff1**	08 **payoff2**	09 **data**	10 **pers**	11 **control**
01	**gender**	1.000										
02	**fsp**	-0.234	1.000									
03	**fmsl**	-0.294	0.585	1.000								
04	**gp**	-0.049	0.135	0.217	1.000							
05	**mss**	-0.106	0.184	0.185	0.656	1.000						
06	**apdd**	-0.078	0.119	0.017	-0.006	0.158	1.000					
07	**payoff1**	-0.119	-0.061	0.009	-0.021	0.031	0.126	1.000				
08	**payoff2**	-0.179	0.077	0.212	0.084	0.148	0.108	0.488	1.000			
09	**data**	0.113	-0.085	-0.163	-0.026	-0.084	0.031	-0.099	-0.673	1.000		
10	**pers**	-0.108	0.089	0.099	-0.036	-0.058	0.036	0.016	0.096	-0.177	1.000	
11	**control**	-0.111	0.116	0.177	0.242	0.221	-0.037	-0.001	0.176	-0.188	-0.229	1.000

Notes

fps: familiarity with smart phone;
fmsl: familiarity with mobile services using my location;
gp: global concerns for privacy;
mss: concerns in mobile service sector;
apdd: authenticity of personal data disclosed;
payoff1: user payoff in scenario 0 (base scenario);
payoff2: user payoff in other scenarios;
data: personal data disclosed;
pers: personalization available;
control: control over personal data.

To test the relationships between variables, I conducted several regression tests using the statistical software STATA 9. The ANOVA test proves that there is no significant effect of scenario 0 over payoff, $F(6,164) = 0.83$, $p = 0.547$, adj $R2 = -0.0057$. Therefore, I include this control group in the final model. Accordingly, the sample size doubles in the regression equations. Table 7.7 presents the outcomes of the four steps; in each step, I tested a different regression. In all regression models, the dependent variable is user payoff.

In the first step, I focus on the impact of data disclosed. I introduce control variables such as gender, familiarity with smart phones, and user's familiarity with LBS and authenticity of disclosed data.

In the second step, I add personalization available as another main independent variable. I also consider the potential interaction effect between the new variable and data disclosed, which is named "data*pers." The third step concerns the control over personal data, and the interaction between data and control (data*control). The final step includes all these three main independent variables and their interactions. The results are shown in Table 7.7.

For each step, I measured the adjusted R-squared. Table 7.7 indicates whether the inclusion of additional variables increased the overall explanatory power of the model.

Table 7.7. Regression models

Dependent Variable: User's Payoff				
	Step 1	**Step2**	**Step3**	**Step4**
data	-2.004***	-1.789***	-2.210***	-1.876***
pers		0.600**		0.624**
control			0.559**	0.562*
data*pers		-0.777**		-0.706
data*control			-0.306	-0.202
pers*control				-0.436
data*pers*control				0.228
gender	-0.404**	-0.396**	-0.378**	-0.373**
fsp	-0.096	-0.091	-0.097	-0.092
fmsl	0.091*	0.086	0.082	-0.084
authenticity	0.227**	0.093**	0.227**	0.231**
_cons	3.566***	3.438***	3.487***	3.343***
Adj. *R*-squared	0.287	0.297	0.296	0.297

Notes
*p < .1; **p < .05; ***p < .01;
data: personal data disclosed; **pers**: personalization available;
data*pers: interaction of personal data disclosed and personalization available;
data*control: interaction of personal data disclosed and control over personal data;
pers*control: interaction of personalization available and control over personal data;
data*pers*control: interaction of personal data disclosed, personalization available and control over personal data; **control:** control over personal data;
fsp: familiarity with smart phone; **fmsl**: familiarity with mobile services using location;
authenticity: authenticity of personal data; **_cons**: constant.

As Table 7.7 indicates, the extent of data disclosed always has a significant effect on user payoff ($p < .01$ in all four steps), which is negative (-2.004 in the first step). In other words, it appears that mobile users sacrifice certain benefit or increase their concerns for risk when the service asks for their personal information. Thus, *H1* is strongly supported.

Service personalization has a significant effect on user payoff ($p < .05$ in steps 2 and 4), which is positive (0.600 in step 2). This fits well with previous results (Son and Kim, 2008), which found a value at 0.60 as well. Interestingly, I find a significant negative interaction effect of personalization available on the relationship between data disclosed and payoff (-0.777 in step 2), though such an effect is not strongly significant ($p > .05$ in steps 2 and 4). Thus, *H2a* is supported but *H2b* is not supported.

Control has a positive (0.599 in step 3) effect on user payoff, although there is not always

a relevant significant effect on user payoff ($p < .05$ in step 3; $p < .01$ in step 4). I found no relevance for the moderating effect of control over user payoff with the whole sample. Therefore, *H3a* is weakly supported and H3b is not supported.

Recalling Lancelot Miltgen (2010), the results confirm that gender was an effect on user's payoff. I also expect that people who show generally low risk aversion have different opinions on their payoffs as opposed to those who are highly risk averse. Thus, I divide the sample into two clusters accordingly. I adopt the median cluster method based on two variables: subjects' global concerns for privacy and concerns in the mobile service sector. I exclude sample observations that are equal to the value of the median. I conduct regression analysis for both clusters, and the results are indicated in Table 7.8.

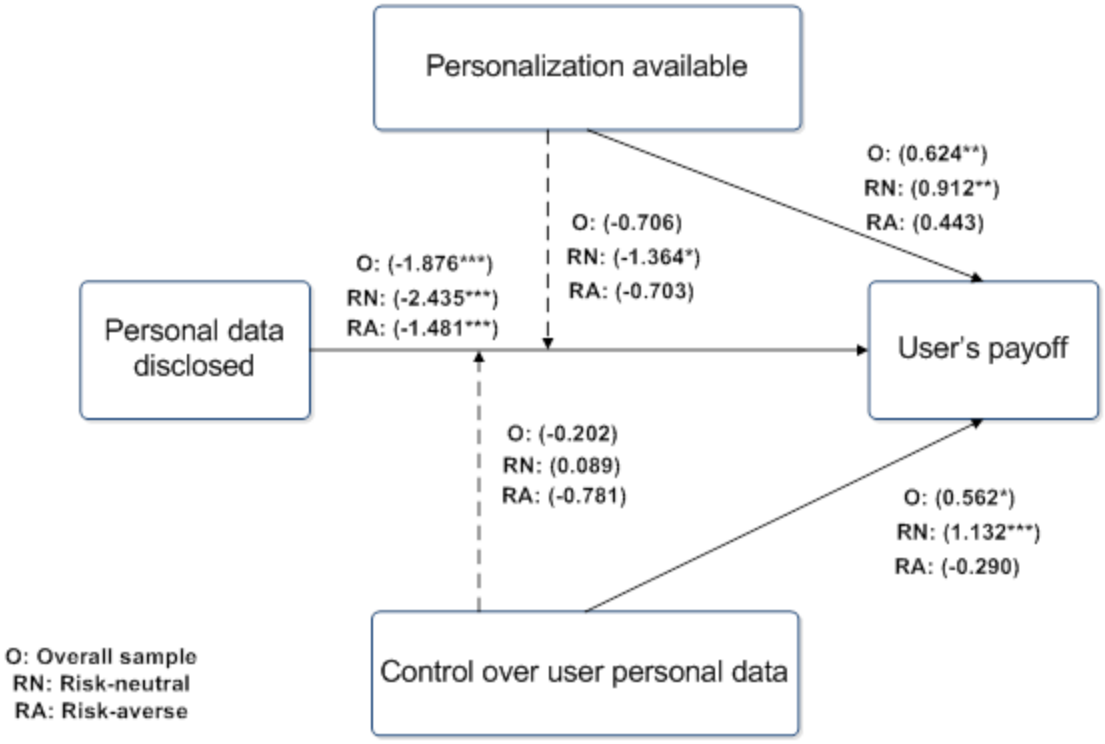
I find that for people who have a relatively high level of concern about privacy when providing personal information (risk-averse users), neither personalization available nor user control over personal data plays an important role in determining payoff, this interpretation extends previous analysis on why privacy policies on website are often not shown in the first page (Bonneau and Preibusch, 2010). For people who have a relatively low level of concern about privacy when providing personal information (risk-neutral users), both variables are demonstrated to be an essential indicators. In the last column of Table 7.8, I observe that the only variable that has a significant impact on payoff is data (-1.481, $p < .01$. *Hence, H2 and H3 are rejected for risk-averse mobile users.* However, there are significant effects of personalization available and user's control for risk-neutral users. In particular, personalization being available has a significant positive direct impact on user payoff (0.912, $p < .05$) and a significant negative moderating effect on the relationship between personal data disclosed and user payoff (-1.364, $p < 0.1$). User's control over personal data has a strong positive impact on user's payoff (1.132, $p < .01$). *Thus, for risk-neutral mobile users, H2 and H3a are supported.*

Table 7.8. Regression for risk-neutral and risk-averse users

Dependent Variable: User's Payoff		
	Risk-neutral users	**Risk-averse users**
data	-2.435***	-1.481***
pers	0.921**	0.443
control	1.132***	-0.290
data*pers	-1.365*	-0.703
data*control	0.089	-0.781
pers*control	-1.226	0.611
data*pers*control	0.993*	0.563
gender	-0.636**	0.001
fsp	-0.259***	0.010
fmsl	0.089	0.120
authenticity	0.386***	-0.021
_cons	3.846***	3.477***
Adj. *R*-squared	0.449	0.216

Notes
*p < .1; **p < .05; ***p < .01;
data: personal data disclosed; **pers**: personalization available;
data*pers: interaction of personal data disclosed and personalization available;
data*control: interaction of personal data disclosed and control over personal data;
pers*control: interaction of personalization available and control over personal data;
data*pers*control: interaction of personal data disclosed, personalization available and control over personal data; **control:** control over personal data;
fsp: familiarity with smart phone; **fmsl**: familiarity with mobile services using location;
authenticity: authenticity of personal data; **_cons**: constant.

There is also a moderating effect of user's control on the relationship between personal data disclosed and user payoff, but such an effect is not significant. Hence, *H3b is not supported for risk-neutral mobile users.* I also observe from Table 7.8 that the adjusted *R*-squared is 0.449 for risk-neutral mobile users, indicating that the overall explanatory power of the model is increased within this group, as opposed to the one that includes all observations (Table 7.7).



Notes:
***p** < .1; ****p** <.05; *****p** < .01

Figure 7.3. Results of the theoretical model

Figure 7.3 describes how the results demonstrate that although there is always a trade-off between user payoff and the extent of personal data disclosed, other factors play different roles in determining user payoff across different groups of customers.

7.5 Implementation of the Theoretical Model: The Trusted Infomediary Pattern

In this section, I derive guidelines to design privacy-friendly business models. I start by mapping the concepts of the theoretical model tested in the previous section onto the nine building blocks of the Business Model Ontology (Osterwalder and Pigneur, 2010). Then I complete the business model of a third-party agent, which has a value proposition structure around privacy protection, using the description of an infomediary (Hagel and Singer, 1999).

7.5.1 Mapping the Model on the Business Model Ontology (BMO)

A business model canvas or ontology (BMO) can be described by looking at a set of nine building blocks. These building blocks were derived from an in-depth literature review of a large number of previous conceptualizations of business models. In this depiction, the business model of a company is a simplified representation of its business logic viewed from a strategic standpoint (i.e., on top of Business Process Modeling), which is explained in detail in the following Table 7.9.

Table 7.9. Business model constructs and descriptions

Business model constructs	Description (from Osterwalder and Pigneur, 2010)	Link to your model
Value proposition (VP)	The bundle of products and services that create	User payoff
Customer segment (CS)	The different groups of people or organizations an enterprise aims to reach and serve	2 types of users
Distribution channel (CH)	How a firm communicates with/reaches its CS to deliver its VP	LBS
Customer relationship (CR)	Types of relationships a firm establishes with a specific CS	Personalization
Key resources (KR)	The most important assets required to make a BM work	Disclosed data
Key activities (KA)	The most important things a firm must do to make its BM work	Control
Partner network (KP)	Suppliers and partners that make the BM work	--
Cost structure (C$)	All costs incurred to operate a BM	--
Revenue stream (R$)	The cash a company generates for each CS	--

At the center is the *Value Proposition*. It describes which customer problems are solved and why the offer is more valuable than similar products from competitors (product, service). Previous studies have already related perceived customer value to privacy risk (Chew and al., 2007). The customers themselves are analyzed in the *Customer Segment*, separated into groups to help identify their needs, desires, and ambitions (e.g., singles, families). In the model, there are two types of mobile users, identified as customer segments: those neutral in respect to privacy risk (52% of the tested sample) and those averse to privacy risk (48% of the tested sample). Thus, the value proposition can be derived by the user's payoff: the risk-neutral users seek personalized service, whereas the risk-averse users seek data control.

Distribution Channel illustrates how the customer wants to be reached and by whom (Internet, store). The boundary conditions of the model define that it applies to LBS; therefore, the distribution channel can be considered to be a mobile device with LBS.

Customer Relationship specifies the type of relationship the customer expects and how it should be established and maintained (promotion, support, individual or mass). The model has a construct concerning service personalization that maps well to this business model component because it allows a personalized relationship between user and

provider. To be able to deliver the value proposition, the business must have *Resources* (staff, machines, secret knowledge), which in the model is the disclosed data of the user. The firm transforms these resources through *Key Activities* into the final product or service (development, production, secret process). The construct concerning data control of the model seems to fall into this category.

Figure 7.4 describes how the model maps with the BMO. The numbers on the arrows refer to the obtained values in Table 7.8. According to Figure 7.4, the segment of privacy risk–neutral users seeks personalized service composed of a personalized customer relationship and a control over personal data. The other segment of mobile users (i.e., the privacy risk–averse) looks for privacy risk mitigation, which can be obtained by a service that collects few personal data.

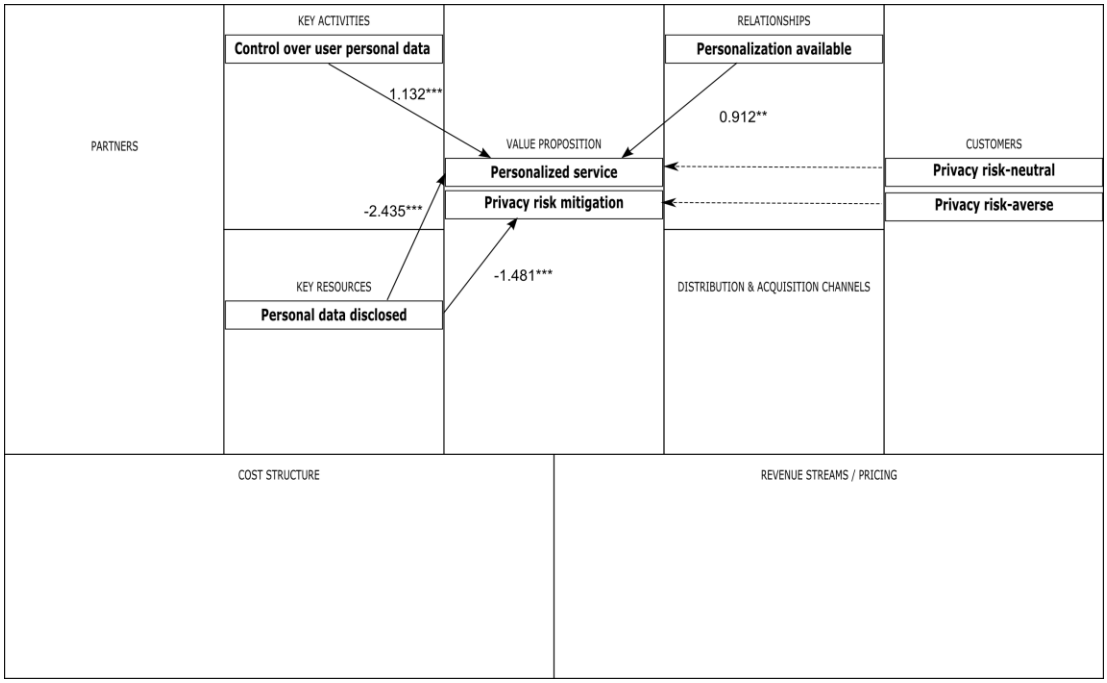


Figure 7.4. The theoretical model represented using the BMO

Most businesses also depend either for resources or for activities on an external *Partner Network* (logistics, financial), which can provide better quality or a lower price for non-essential components. Any business model would be incomplete without financial information. Hence, the last two building blocks focus on cost and revenue: *Cost Structure*, which should be aligned to the core ideas of the business model (key resources, key activities), and *Revenue Streams*, which mirror the value the customers are willing to pay and how they will perform the transaction (one-time fee, subscription).

These elements happen to be missing in the model. In the next section, I obtain a profitable business model by referring to existing business model patterns.

7.5.2 Applying the BMO to Derive a Privacy-Friendly Business Model Pattern

A pattern is commonly referred to as a solution for a problem in a recurring context. Using the business model ontology, one can represent a set of business model patterns (Osterwalder and Pigneur, 2010) Each business model pattern addresses a different goal. It assigns values to components of a business model and specifies relationships to be applied to similar contexts.

For these purposes, I introduce the pattern of the infomediary as a special case of a multi-sided business model (Evans and Schmalensee, 2005). Infomediary is a term invented by Hagel and Singer (1999). It was previously referred to as "boundary spanner" or "information broker" and adapted to the e-business. The infomediary is a trusted third party that helps consumers and vendors connect. The role of the infomediary is to become the custodian, agent, and broker of customer information.

The third party has distinct sets of client segments, which need each other and which cannot get together easily on their own. The infomediary helps them connect through a specific platform. The main cost of a double-sided business is maintaining and developing the platform. As for the revenues, one segment can be subsidies in order to generate enough interest for the platform from the second party, which will then pay for the service.

Figure 7.5 illustrates the effects of the infomediary pattern introduction on the components of the business model, which describes here in detail.

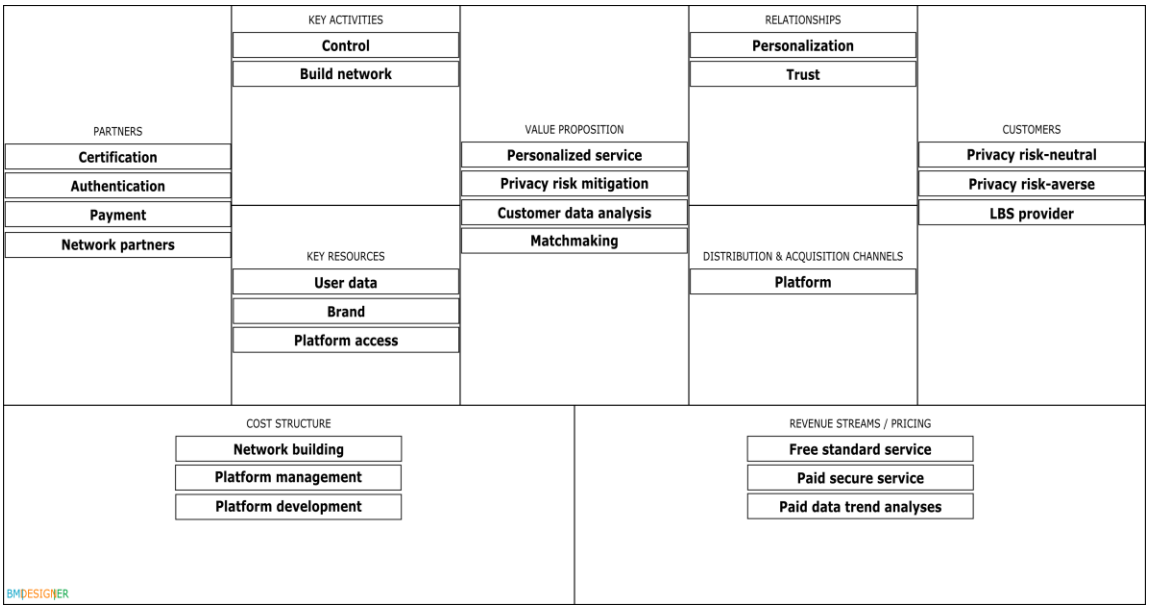


Figure 7.5. Business model for privacy as value proposition

Customer segments: A third customer segment is added to the two existing ones: m-commerce service providers willing to add privacy management to their services to differentiate their offer or tap into the pool of risk-averse users.

Value proposition: According to the three different customer segments, I identify three main value propositions:

- Service personalization for privacy risk–neutral users: By aggregating customers with the same interest, the infomediary can negotiate better deals. The user receives only advertisements based on a personal opt-in profile. The user can get better recommendations based on that individual's personal protected aggregated profile. The user can opt in to receive certain advertisements, and in some cases even get paid for exposing parts of a personal detailed profile.

- Privacy risk mitigation for privacy risk–averse users: The infomediary acts as a proxy for the transactions and the delivery in order to hide the customer from the business. The LBS provider's data profiling is minimized, and the user's data collection for LBS is reduced. The third party also displays reports for each user profile, as an overview of the collected information, to help the customer choose services.

- Customer data analysis for LBS providers: Trend analyses of privacy risk–neutral users can be exchanged with the LBS provider for money. And to users who opted-in, the infomediary can forward target advertisements on behalf of a business. In return,

the business gets a better return on advertisements because all the recipients theoretically should be in the target segment.

Matchmaking among different customer segments is an additional value proposition that distinguishes the multisided business model pattern.

Customer Relationships: The key to attracting risk-averse users is to promote the importance of privacy protection, as well as to build a very strong trust relationship with the customer. The privacy agent has to show users that it knows the high value a user has for personal data and also must prove it cares a great deal for keeping the data safe. This relationship is very similar to that of a bank and its customers. One way to achieve this is by being transparent. For the risk-neutral users, a personalized service increases user's payoff.

Channels: Service can be personalized either by means of a platform, which could be either an application of the mobile devices or the Internet. For the risk-averse, user's data can be stored in a safe and remote database and retrieved by secure connection.

Revenue Streams: The risk-neutral users get the services for free, to gain from the freemium effect (Anderson, 2009). LBS providers pay risk-neutral users for their data trend analyses, which is the greatest part of the third-party income. Risk-averse users are more likely to pay to get their service, and so they subsidize the controls offered to the risk-neutral users.

Key Activities: The key activity of a mutli-sided business model is to build and promote a network of users of its platform. To ensure compliance with the users' policies, the privacy risk can be mitigated by implementing and maintaining a set of controls according to security frameworks such as CobiT and ISO 270001, together with privacy guidelines (Nokia Siemens Networks, 2009).

Key Resources: The most important element for the third party is user data and control over access to the data sharing platform. An additional resource is represented by the brand value, which allows a trusted relationship with the three customer segments.

Key Partners: The third party must be audited and certified by an external partner. The third party also must have partnerships with mobile device manufacturers or network operators in order to realize and deploy the product (Network Partners). To offer additional services or implement additional privacy protection, the third party might also need to be in relationship with identity and payment providers.

Cost Structure: Network building and Platform Management and Development activities are costly services.

The third party can always be circumvented by mobile users interacting directly with the LBS provider, but these providers implement privacy only by policy. The LBS provider promises not to abuse the data, whereas the third party can implement real privacy by architecture through the platform.

7.6 Business Model Instances of the Trusted Infomediary Pattern

There is a range of possibilities for technical implementation of privacy protection, intended here as algorithms, data storage, and policies. Centralized personalization is seen by some researchers as a major trend in the telecommunications world, whereas others expect most personalization to take place on the end-user terminal for reasons of usability, response time, and privacy (De Reuver and Haaker, 2009).

The literature review of the last ten years of research in privacy-enabling technologies done by (Danezis and Gurses, 2000) allows assessment of the limits of a trusted third party and supports a claim that it is possible to "crowd source" (Howe, 2006) both identity provision and attribute certification (Yu et al., 2008). However this approach does not fully explain how to get rid of a trusted third party. Hence, I consider a combination of centralized and decentralized privacy control solutions. Figure 7.6 shows the centralized and decentralized implementations of privacy protection. Different customization degrees of the (centralized) IT infrastructure of the service provider and of the (decentralized) software on user's mobile device are illustrated. This way, I obtain four possible outcomes in the matrix, which illustrates by using four possible market players as examples.

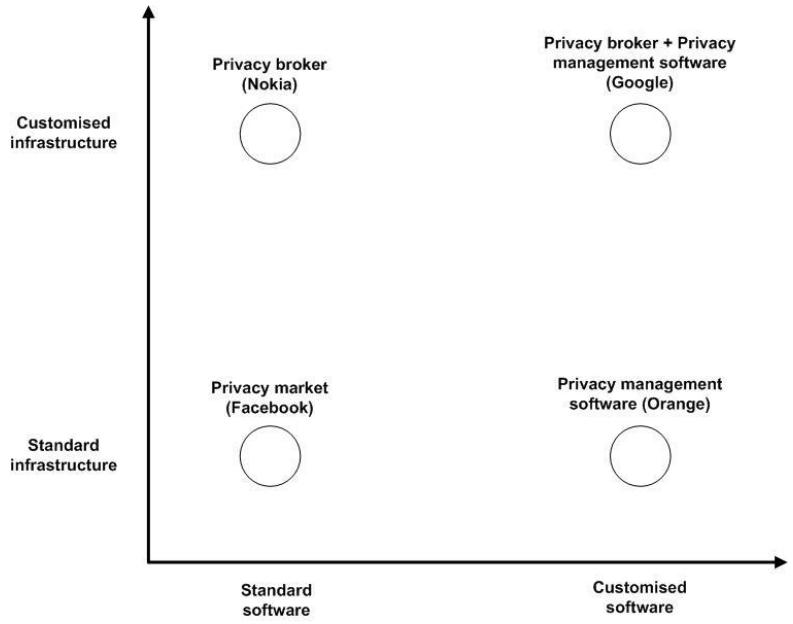


Figure 7.6. Four instances of a privacy-friendly business model (Infrastructure = centralized; software = decentralized)

Alliances among parties can maximize their payoff by cooperating, even though they have diverging goals (Dowling et al., 1996). On one hand, a firm that cannot avoid this kind of co-opeting relationship (Nalebuff and Brandenburger, 1997) in non-core competence areas can best adapt by decentralizing the largest amount of information collected and by letting other firms do most of the key activities. On the other hand, a firm that cannot avoid this kind of relationship in core competence areas can best adapt by centralizing information about the relationship through establishing an inter-organizational structure (the platform) to share information.

7.6.1 Privacy Broker

Table 7.10 illustrates the business model adaptations required for the privacy broker. Mobile network operators such as Nokia are good candidates for deploying a privacy broker because they already possess location information and have direct access to the telecommunication infrastructure. For mobile network operators, LBS represent an additional stream of revenue generated from their investments in fixed infrastructure (Rao and Minakakis, 2003).

For GPS-enabled terminals, the location of the intelligence shifts toward the handset. This may reduce the role of operators and increase the opportunities for service providers, as accurate location-based information becomes available at no cost. Therefore, adding

privacy protection services can become a key differentiator for mobile network operators (De Reuver and Haaker, 2009).

Over half of users would be happy if their CSP (Communication Service Provider) would fulfill the role of supervising permission policies (Nokia Siemens Networks, 2009). Moreover, providing new LBS-like location sensitive billing might be a very attractive aspect of current phone billing possibilities. The biggest difficulty is the creation of relationships with m-commerce providers.

Table 7.10. Adaptations required for the privacy broker

BMO Component	**Required Adaptation**
Key Resources	The platform is composed of a broad range of components between mobile applications, middleware and server based software, depending on the technologies chosen to implement the privacy protection (for an example the reader can see Hong et al., 2005)
Cost Structure	The cost of developing the platform. Costs relative to the infrastructure and its maintenance, which can be especially high in case in which it has to scale for enormous demands for real-time transactions
Revenue Streams	A fee over secure transactions paid by risk adverse users

7.6.2 Privacy Manager Software

Table 7.11 shows the business model adaptations required for the privacy manager software. Operating system providers of mobile devices such as Orange Telecom are in a good position to influence privacy protection on their platforms. They have direct access to the raw sensor of the phone and can define what information is exposed to applications through their Application Programming Interfaces (APIs). Moreover, they have the possibility of integrating the privacy middleware directly into the operating system and thereby targeting the whole market at once.

In addition, they might have an easier job integrating user friendly profile management into the system. Providing a privacy system can further help to expand the dominance of their operating system market share.

Table 7.11. Adaptations required for the privacy manager software

BMO Component	Required Adaptation
Key Resources	The key resource in a decentralized solution is middleware developed for the user's device. Such software is meant to implement a set of policies according to predetermined algorithm to assure user location privacy (for an example the reader can see Freudiger et al., 2009) The user can download the application by phone and let the software manage the phone applications according to the user's privacy policies. This approach relies on existing solution on the market, such as the dynamic settings manager for Android called Locale. One can add a set of so-called security profiles that collect data from phone input sources, use security metrics to assess the context risk, and apply privacy best-practices to enforce security actions depending on the risk profile.
Cost Structure	Development for the device is costly, especially since there are many different platforms, as well as the fact that they evolve rapidly. However, there are no fixed infrastructure costs and once device platforms stabilize, maintenance costs, should also diminish.

7.6.3 Can We Combine Privacy Broker and Privacy Manager Software?

Google appears to be an ideal candidate for becoming a centralized service for managing user privacy profiles. Google already offers SSOuser authentication and has a mobile phone operating system (Android), which includes location applications (Latitude). Consumers use Google to handle private information such as emails (Gmail) and documents (Google Docs). In addition, the company has already implemented some aspects of an infomediary with the Google health offering, as well as a dashboard that gives users an overview of all available services and settings.

Google is in a special position where it can choose to implement either a privacy broker model around the server infrastructure or integrate a privacy manager into the Android operating system. This gives the company the unique opportunity to also choose a mix of both alternatives. The solution could be more independent (phone-based middleware) or deliver real-time centralized server–based privacy mediation.

The caveat is that Google is a private company and its main business model is to sell targeted advertising, which might conflict with privacy protection ideals.

7.6.4 Privacy Market

In a privacy market, the customer can sell his, her, or its personal data. A practical case of a privacy market is Allow Litd (Angwin and Steel, 2011). This London-based firm takes advantage of a recent English regulation that obliges a company to erase all users' data collected without their consent. Once a client signs in with Allow Ltd, the company scans all firms' databases looking for the client's personal data. Once the personal data are found, the firms are requested to remove those data unless they pay a small price, 70% of which goes to the client.

This type of service provider supports the management of the user's sale of the property right over data. For this kind of task, the use of a privacy mirror (as those illustrated by Nguyen, 2002) seems to be appropriate.

Facebook appears to be a good candidate for the privacy market. In the last five years, its privacy policy has increased from 1,000 words to some 5,900 words. I see this effort as an attempt to get consent over user's partial loss of control of property rights over the data (Facebook uses a non-exclusive license of the user's data). As of now, the user loses control over personal data in exchange for some services, but I envisage that in the near future, the firm could pay for its users' data.

7.7 Discussion and Conclusion

In this paper, I introduced the business model of a trusted third party to protect privacy while enabling LBS. I ground the claims on a model developed specifically by incorporating existing works. The empirical data were collected extended previous knowledge in privacy management. I referred to business model ontology to derive a set of guidelines for business model designers and identified possible variations to the pattern of the privacy friendly business model inspired by the infomediary business model. I presented some market players who are potential candidates to provide instantiations of such a privacy protection service.

According to my findings, I answer my research questions by addressing three sub-questions as follows:

R1: What is the specificity of privacy management in the location-based mobile B2C market?

Our empirical evidence in section 7.4 strongly suggests that collected data reduces user payoff, whereas the combination of service personalization and data control increases user payoff. This study confirms previous evidence (Son and Kim, 2008) of a relation

between service personalization and user payoff, and extend it with the notion of control in the B2C market. I also found two clusters that behave slightly differently from what has been seen for Internet privacy (Lancelot Miltgen, 2010). the model is both simple (four constructs) and representative (adj. R^2 between .22 and .45).

R2: Which business model components allow a high level of mobile user payoff, while keeping the collected data to a minimum?

Using the empirical data of the test, I suggest that business model designers should follow the infomediary pattern and then define the degree of software centralization according to how much data should be collected and how much control should be left to the user. According to the type of firm involved, a privacy broker or privacy manager software, or both, is to be preferred.

R3: How should the differences in payoff among privacy risk–neutral and privacy risk–averse mobile users be addressed?

Our test underlines the existence of two types of mobile user with privacy concerns. Although both customer segments care about the personal data they disclose, privacy risk–neutral mobile users seem to be more attentive to a combination of data control and service personalization in exchange for their data.

The privacy risk–averse users obsess about the data, and therefore a pay-per-use SSO service that safely protects their data and acts as a proxy to other services seems more likely to be profitable.

Our proposed model is to be considered as an initial step toward conceive a tool to support strategic decisions, and it has its own limitations. Concerning evaluation of the model, the business model guidelines have been instantiated, but their impact on provider's performance has not been tested empirically. Hence, my proposed models for the service provider must be considered as initial intuitions.

On a more general level, I assume that privacy will become a technological trend. Privacy issues have reached widespread public awareness only in the last few years, and growth of these issues is yet to come. The definition of privacy guidelines within a common framework has just started, and there are no widely adopted solutions integrated by platforms. As long as there is no standard and no real added value or perceived added value to enforcing privacy, there is always the possibility of going directly to a vendor and using raw data from the phone sensors.

I feel that this paper offers some interesting (Davis, 1971) contributions to the field:

- I defend the view of those who believe that privacy should not be seen only as a cost. We propose and show evidence that it could be a value proposition of a business model in the B2C mobile market to complement product customization and risk reduction.

- I suggest that secure service personalization for customers and data access for the company can co-exist sustainably (by means of a third party - to be tested later).

- I present more than one way an enterprise can position itself in relation to its competitors with regard to the trade-off between data control and service personalization. I argue by a set of instantiations that the mobile platform can play a key role at multiple levels (OS, device manufacturer, and operator) in the implementation of these new business models.

Supposing that no third-party actor emerges, some firms might implement some elements from the proposed pattern to add privacy risk mitigation into their value proposition and gain new customers. In the long term, this kind of firm would no longer require a third-party actor.

Accordingly, one could decide to remove the initial assumption regarding the existence of a third-party actor. In that case, the best strategy for a firm is to internalize the third party, if it involves its core competences. This again might raise strategic issues about service integration and business model unbundling.

Further work should address issues such as the possibility of leveraging my proposed privacy business model pattern in other economic contexts, involving incomplete agreements and lack of trust among involved parties.

7.8 References

Anderson, C. 2009. “Free: The Future of a Radical Price,” First Edition, Hyperion.

Anderson, R. 2001. “Why information security is hard—an economic perspective,” in Proceedings 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, USA, IEEE, pp. 358-365.

Angwin, J. and Steel, W. 2011. “Web's hot new commodity: Privacy,” The Wall Street Journal, 2011.

Awad, N. F., and Krishnan, M. S. 2006. “The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization,” *Management Information Systems Quarterly* (30:1), pp. 13-28.

Barrett, M., Garrety, K., and Seberry, J. 2006. “ICT professionals’ perceptions of responsibility for breaches of computer security,” Faculty of Informatics-Papers, pp. 383.

Benbasat, I., and Zmud, R. W. 2003. “The Identity Crisis Within the IS Discipline: Defining and Communicating the Discipline's Core Properties,” *Management Information Systems Quarterly* (27:2), pp. 183-194.

Bonneau, J., and Preibusch, S. 2010 The privacy jungle: On the market for data protection in social networks, *Economics of Information Security and Privacy, Springer*, pp. 121–167.

Chellappa, R. K., and Sin, R. G. 2005. “Personalization versus privacy: An empirical examination of the online consumer’s dilemma,” *Information Technology and Management* (6:2), pp. 181-202.

Chew, K. W., Shingi, P., and Ahmad, M. 226. “TAM Derived Construct of Perceived Customer Value and Online Purchase Behavior: An Empirical Exploration,” *IFIP International Federation for Information Processing* (226), pp. 215-227.

Cox, O. P., A. Dalton, and Marupadi, V. 2007. “Smokescreen: flexible privacy controls for presence-sharing,” in Proceeding of MobiSys, New York, pp. 233–245.

Danezis, G. and Gürses, S. 2000. “A critical review of 10 years of Privacy Technology, in Proceedings of Surveillance Cultures: A Global Surveillance Society?” London, UK. available on:
http://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf

Das, T. K., and Teng, B. S. 2001. “Trust, control, and risk in strategic alliances: An integrated framework,” *Organization Studies* (22:2), pp. 251-283.

Davis, M. S. 1971. “That’s interesting! Towards a phenomenology of sociology and a sociology of phenomenology,” *Philosophy of the Social Sciences* (1:4), pp. 309-344.

De Reuver, M., and Haaker, T. 2009. “Designing viable business models for context-aware mobile services,” *Telematics and Informatics* (26:3), pp. 240-248.

Dinev, T., and Hart, P. 2006. “An extended privacy calculus model for e-commerce transactions,” *Information Systems Research* (17:1), pp. 61-80.

Dowling, M. J., Roering, W. D., Carlin, B. A., and Wisnieski, J. 1996. “Multifaceted relationships under coopetition,” *Journal of Management Inquiry* (5:2), pp. 155-167.

Evans, D. S., and Schmalensee, R. 2005. “The industrial organization of markets with two-sided platforms,” *Competition Policy International* (3:1), pp. 151-179.

Freudiger, J., Manshaei, M., Hubaux, J. P., and Parkes, D. C. 2009. “On Non-Cooperative Location Privacy: A Game-Theoretic Analysis,” available on http://infoscience.epfl.ch/record/140427/files/ccs179-freudiger3.pdf

Giaglis, G., Kourouthanassis, P., and Tsamakos, A. 2002. “Towards a classification framework for mobile location services,” in: Mennecke, B. E. and Strader, T. J., ed. Mobile Commerce: Technology, Theory, and Applications, Idea Group Publishing, pp. 67-85.

Gibson, B., and Holden, W. 2010. “Mobile Location Based Services. Applications, Forecasts & Opportunities 2010 – 2014,” Juniper Research.

Gregor, S., and Jones, D. 2007. “The Anatomy of a Design Theory,” *Journal of the Association for Information Systems* (8:5), pp. 312-335.

Hagel, J., and Singer, M. 1999. “Net Worth: Shaping Markets When Customers Make the Rules,” Harvard Business School Publishing, Boston, MA.

Herrmann, D. S. 2007. “Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance,” Operational Resilience, and ROI (1st ed.). Auerbach Publications, Boca Raton, FL, USA.

Hong, D., Yuan, M., and Shen, V. Y. 2005. “Dynamic privacy management: a plug-in service for the middleware in pervasive computing,” in Proceedings of the 7th international conference on Human computer interaction with mobile devices & services, New York, pp. 1-8.

Howe, J. 2006. “The Rise of Crowdsourcing,” Wired. Available on http://www.wired.com/wired/archive/14.06/crowds.html.

Hui, K., Teo, H. H., and Lee, S. 2007. "The value of privacy assurance: an exploratory field experiment," *Management Information Systems Quarterly* (31:1), pp. 19-33.

Husson, T. 2010. "Profiling Your Best Mobile Customers," Forrester Research, Inc. Available on www.forrester.com

Lancelot Miltgen, C. 2010. "Disclosure of personal data and expected counterparties in e-commerce: a typological and intercultural approach," *Management Information System* (15:4), pp. 1-49.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns(IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355.

March, S. T. and Smith, G. F. 1995. "Design and natural science research on information technology," *Decision Support Systems* (15:4), pp. 251-266.

Nalebuff, B., & Brandenburger, A. 1997. "Co-opetition: Competitive and cooperative business strategies for the digital economy," *Strategy & Leadership* (25:6), pp. 28-35.

Nguyen, D. H. 2002. "Privacy mirrors: Understanding and shaping socio-technical ubiquitous computing," Technical Report.

Nokia Siemens Networks. 2009. "Privacy survey 2009", Nokia Siemens Networks Corporation, available on http://www.nokiasiemensnetworks.com/sites/default/files/document/SDM_PrivacyStudy_Brochure.pdf

Organisation for Economic Co-operation and Development. 2002. "OECD guidelines on the protection of privacy and transborder flows of personal data," OECD Publishing, Paris, France, available on: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Osterwalder, A., & Pigneur, Y. 2009. "Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers," Wiley, Indianapolis.

Palen, L., and Dourish, P. 2003. "Unpacking privacy for a networked world," in Proceedings of the ACM Special Interest Group on Computer-Human Interaction (SIGCHI) conference on Human factors in computing systems, pp. 129-136.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing* (19:1), pp. 27-41.

Pries-Heje, J., Venable, J., and Baskerville, R. 2008. "Strategies for design science research evaluation. In Proceedings of the 16th European Conference on Information Systems (ECIS 2008), Galway, Ireland.

Rao, B., and Minakakis. L. 2003. "Evolution of mobile location-based services," *Communications of the ACM* (46:12), pp. 61-65.

Sheng, H., Nah, F. F., and Siau, K. 2008. "An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns," *Journal of the Association for Information Systems* (9:6), pp. 344-376.

Son, J. Y., and Kim, S. S. 2008. "Internet users' information privacy-protective responses: A taxonomy and a nomological model," *Management Information Systems Quarterly* (32:3), pp. 503-529.

Stewart, K. A., and Segars, A. H. 2002. "An empirical examination of the concern for information privacy instrument," *Information Systems Research* (13:1), pp. 36-49.

Sutton, R. I., and Staw B. M. 1995. "What theory is not," *Administrative Science Quarterly* (40:3), pp. 371-384.

Yu, H., Gibbons, P. B., Kaminsky, M., and Xiao, F. 2008. "Sybillimit: A near-optimal social network defense against sybil attacks," in IEEE Symposium on Security and Privacy DBL, pp. 3-17.

List of Author's Publications

Liu, Z., Shan, J., Bonazzi, R., and Pigneur, Y. 2014. "Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications," Proceedings of the 47st Hawaii International Conference on Systems Science (HICSS-47), Waikoloa, Big Island, Hawaii, USA, IEEE Computer Society, 6-9 January, 2014, pp. 1063-1072.

Liu, Z., Le Calvé, A., Cretton, F., and Glassey, N. 2014. "Using Semantic Web Technologies in Heterogeneous Distributed Database System: A Case Study for Managing Energy Data on Mobile Devices," *International Journal of New Computer Architectures and their Applications* (4:2), pp. 56-69.

Liu, Z., Cretton, F., Le Calvé, A., Glassey, N., Cotting, A., and Chapuis, F. 2014. "MUSYOP: Towards a Query Optimization for Heterogeneous Distributed Database System in Energy Data Management," Proceedings of the International Conference on Computing Technology and Information Management (ICCTIM 2014), Dubai, United Arab Emirates, 9-11 April, 2014, pp. 1-9.

Liu, Z., Le Calvé, A., Cretton, F., Evéquoz, F., and Mugellini, E. 2013. "A Framework for Semantic Business Process Management in E-Government," Proceedings of the IADIS International Conference on WWW/Internet, Fort Worth, Texas, USA, IADIS, 22-25 October 2013, pp. 259-267.

Cretton, F., Liu, Z., and Le Calvé, A. 2013. "A Friendly Localized Platform for Multilingual Semantic Communication," Proceedings of the Actes du 5e Colloque National sur la Recherche en Informatique et ses Applications, Ziguinchor, Sénégal, 25-27 Avril 2013.

Bonazzi, R., Liu, Z., Garnière, S., and Pigneur, Y. 2012. "A Dynamic Privacy Manager for Compliance in Pervasive Computing," Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, *IGI Global*, pp. 285-307.

Grèzes, V., Liu, Z., Crettol, O., and Perruchoud, A. 2012. "From business model design to environmental scanning: the way to a new semantic tool to support SMEs' strategy," Proceedings of the eChallenges e-2012 Conference, Lisbon, Portugal, 17-19 October, 2012.

Liu, Z., Bonazzi, R., Fritscher, B., and Pigneur, Y. 2011. "Privacy-friendly Business Models for Location-Based Mobile Services," *Journal of Theoretical and Applied Electronic Commerce Research* (6:2), pp. 90-107.

Bonazzi, R., Liu, Z., Fritscher, B., and Pigneur, Y. 2011. "From Security for Privacy to Privacy to Security," Proceedings of the 4th International Workshop: Business Model for Mobile Platforms (BMMP 11), Berlin, Germany, pp. 319-324, IEEE, 7 October, 2011.