Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

Privacy-Friendly Business Models for Location-Based Mobile Services

Zhan Liu[1], Riccardo Bonazzi[2], Boris Fritscher[3] and Yves Pigneur[4]

University of Lausanne, Faculty of Business and Economics
[1] zhan.liu@unil.ch, [2] riccardo.bonazzi@unil.ch, [3] boris.fritscher@unil.ch, [4] yves.pigneur@unil.ch

Received 13 January 2011; received in revised form 15 April 2011; accepted 18 May 2011

Abstract

This paper presents a theoretical model to analyze the privacy issues involved in business models for location-based mobile services. We report the results of an exploratory field experiment in Switzerland that assessed the factors driving the net payoff to users of mobile businesses. We 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 user 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 user payoff. The results suggest that privacy protection could be the main value proposition in the B2C mobile market. From our theoretical model, we derive a set of guidelines to design a privacy-friendly business model pattern for third-party services. We 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

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

1 Introduction

New regulatory requirements, such as the guidelines given by the Organisation for Economic Co-operation and Development [33], 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 [19]. On the other hand, the collection of data about consumers is constrained by their privacy right, which we refer to 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 [21]). 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., [14], [28]). In this sense, user privacy concerns are found to be one major predictor of the willingness to provide personal information. We 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 we consider 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" [41] if user's payoff is not assured, data security is in peril [2].

In the rest of the paper, we focus on location-based services offered in the Business to Consumer (B2C) market, such as navigation, information, advertising, tracking, and billing [18]. We exclude emergency services from our analysis because users of those services deal differently with privacy concerns [40]. Location-based applications open new opportunities for business models in the mobile sector. Hence, we primarily address an audience mainly composed of stakeholders in mobile services who seek guidelines to develop privacy-friendly business models. We 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 [6]. Our 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. In the next section, we review some of the related work in privacy and location-based services that addresses our research question, and we define a set of research sub-questions to fill the remaining gaps. The third section presents the methodology we use to address these sub-questions. The fourth section introduces our theoretical model and presents empirical evidence to support it. In the fifth section, we implement our theoretical model to derive a set of guidelines to obtain privacy-friendly business models. Section 6 presents a set of possible instantiations of our guidelines using real companies as potential candidates. In the final section, we discuss the implications of our analysis, draw some conclusions, and propose further possible research.

2 Literature Review

In this section we briefly highlight a set of well-known works that help us in answering our research question. For a more complete literature review of privacy management technologies, we suggest reading [11]. After outlining the remaining gaps in the literature, we derive a set of research sub-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 [1]. 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 [35]. We 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) [30].

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 [25], [27]. 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 [25]. 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 [27].

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

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. We therefore derive the following research sub-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 [10]). 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 [28], [41].

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 [36]. Issues of information control are essential in increasing the likelihood of consumers contributing information to online firms [42].

Another important issue is the value of personalization. According to [8], 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, our second research sub-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 [27] four different clusters of users: well-intended, negotiator, unconcerned, and reticent. These analyses suggest that when considering the approach to e-commerce, we should also respect the different groups of Internet users. Such results appear to not have strong statistical relevance. Hence, our third sub-question is:

R3: How should the differences in payoff among privacy risk–neutral and privacy risk–averse mobile users be addressed?

In the following section, we illustrate how we intend to address our research sub-questions to answer our initial research question.

3 Methodology

Based on the relevant literatures, we create an artifact in the form of a model [29] to express the relationship between user payoff and the extent of personal data disclosed.

We adopt a design science research methodology, and we refer to existing guidelines for design theories [20]. 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" [20]. Therefore, we advance in three steps, as illustrated in Figure 1.

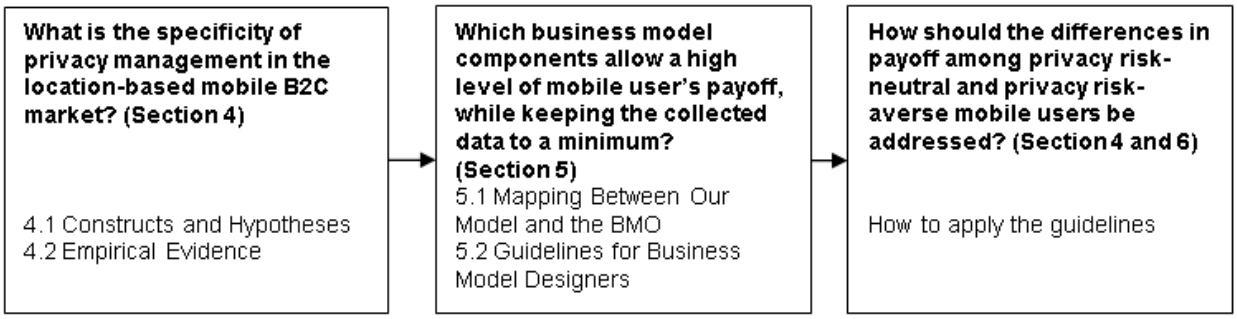

Figure 1: Model of user's payoff

An information system design theory (ISDT) should define its purpose and scope, that is, the boundaries of a theory. In our case, our theory concerns data management for privacy risk reduction of location-based services. The second

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

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, in section 4 we introduce a model composed of four constructs and derive hypotheses concerning the interaction among constructs. In doing so, we ground our claims on existing theories of control [12], as well as perceived justice and equity theory (used in [41]).

The evaluation strategy of testable propositions uses surveys as an ex post artificial type of evaluation [37]. 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 5 starts by mapping our constructs with the constructs of the Business Model Ontology (BMO) [34], a tool often used by startups and multinational companies to represent their business models. Because our model has only four constructs and the BMO is composed of nine elements, we 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 our third sub-question, we need to test the feasibility of the proposed guidelines. Hence, section 6 presents a set of instantiations of our 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, we illustrate four examples of application for our guidelines by naming four existing companies as possible candidates.

4 Model

In this section, we present our theoretical model, following the guidelines to describe a theory [43]. We start by presenting the constructs and by augmenting our hypotheses using the references we introduced in the literature review. Then we show the correlations among components, which we derive from our test results.

4.1 Constructs and Hypotheses

Our model is composed of four constructs, the definitions of which are derived from previous research summarized in Table 1.

Table 1: Definitions of each construct of our model

Construct	Definition	Source
Personal data disclosed	Degree to which a mobile user perceives personal data being disclosed by the mobile service companies	[41]
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 providing personal information	Ibid.
Personalization available	Degree of fairness that a mobile user perceives from mobile service company treatment of information privacy	Ibid.
Control over user personal data	Degree to which a mobile user perceives whether 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, we focus on the effects among antecedents. We refer to [41] 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 our model) is found to be one major predictor for *personal data disclosed,* which we define as the degree to which a mobile user perceives whether personal data is disclosed by the mobile service company. Therefore, we propose a model of user payoff as indicated in Figure 2.

H1: The personal data disclosed has a negative effect on user payoff.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

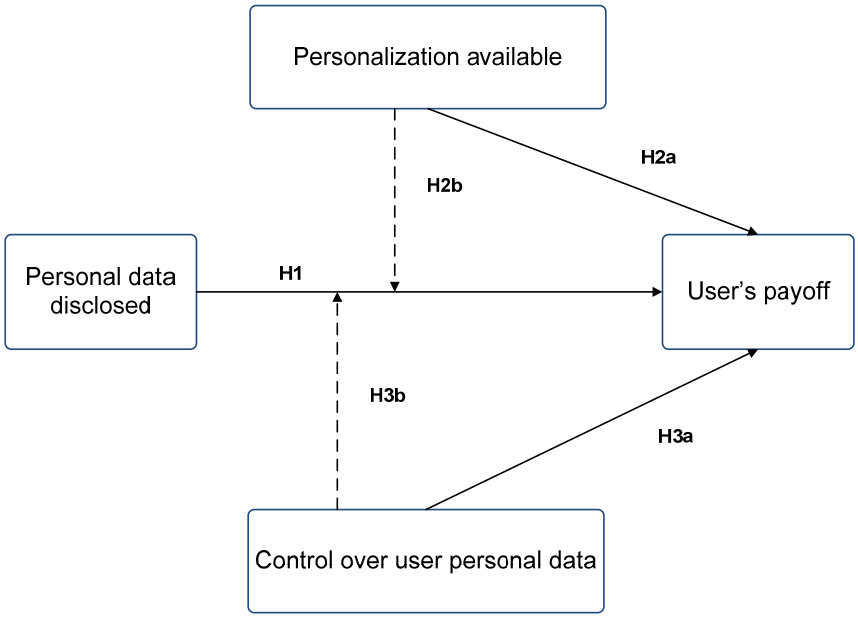

Figure 2: Model of user payoff

In exchange for user data, the m-commerce provider could offer a service, which is either standard or fully customized. We introduce the concept of service personalization, which we define as the degree of fairness that a mobile user perceives relative to mobile service company's treatment of information privacy. As we previously mentioned in the literature review, service personalization depends on customer willingness to share information and use personalized services [8]. 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 and (b) a moderating effect on user 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 [22] are a useful tool to decrease user concern for privacy risks. Lack of such controls decreases mobile user trust in the provider [12] and lowers the perceived payoff. Hence, we propose that:

H3: The amount of control over user personal data has (a) a direct and positive effect and (b) a moderating effect on user payoff.

4.2 Test Design

In our study, we want to test the effect of the data disclosure, service personalization, and data control over user payoff. We test the effect of such constructs in two steps.

Because we are dealing mostly with perceptions, we test the effect of our model using scenario-based surveys. This form of assessment has been successfully implemented in previous studies on information system security [5].

As illustrated in Table 2, we designed 2^n different scenarios, where n is the number of constructs in our model that we 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.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

In step 2, we 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 2: Our 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 3 indicates, each variation of the scenario operationalizes one construct of our model and is derived from previous works.

Table 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	[25]
Personalization available	Low: None High: "You have the possibility to customize your personal preferences to get the discount information you desire."	[4]
Control over user personal data	Low: None High: "You still can see which data are sold to the discount providers and set a limited amount of options regarding such disclosure."	[28]

To measure the user's payoff, we derive three items from previous studies. A set of control variables is included as well, as shown in Table 4.

Table 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 in obtaining this discount service makes me suppress my privacy concerns	[14]
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) I believe that regulations in my country require personal data to be properly protected	[27]
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 tasks related to work or private life	[27]
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 pseudonym E3) Concerning my personal data, I always give false information E4) Concerning my personal data, I do not answer personal questions if they are not mandatory	[27]

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

4.3 Results

We 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 5. Our 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 [26].

From previous research, we derived two items to test for cultural effect. We can compare to the English sample of [27] that had the same sample distribution.

Table 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 6 presents information on the correlation coefficients between all the constructs. We 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. We did not otherwise observe any significant proof of multicollinearity among our variables.

Table 6: Correlation among variables

		1	2	3	4	5	6	7	8	9	10	11
		gender	**fsp**	**fmsl**	**gp**	**mss**	**apdd**	**payoff1**	**payoff2**	**data**	**pers**	**control**
1	**gender**	1.000	-	-	-	-	-	-	-	-	-	-
2	**fsp**	-0.234	1.000	-	-	-	-	-	-	-	-	-
3	**fmsl**	-0.294	0.585	1.000	-	-	-	-	-	-	-	-
4	**gp**	-0.049	0.135	0.217	1.000	-	-	-	-	-	-	-
5	**mss**	-0.106	0.184	0.185	0.656	1.000	-	-	-	-	-	-
6	**apdd**	-0.078	0.119	0.017	-0.006	0.158	1.000	-	-	-	-	-
7	**payoff1**	-0.119	-0.061	0.009	-0.021	0.031	0.126	1.000	-	-	-	-
8	**payoff2**	-0.179	0.077	0.212	0.084	0.148	0.108	0.488	1.000	-	-	-
9	**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.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

To test the relationships between variables, we 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 $R^2 = -0.0057$. Therefore, we include this control group in our final model. Accordingly, the sample size doubles in the regression equations. Table 7 presents the outcomes of our four steps; in each step, we tested a different regression. In all regression models, the dependent variable is user payoff.

In the first step, we simply focus on the impact of data disclosed. We introduce control variables such as gender, familiarity with smart phones, and user's familiarity with location-based services and authenticity of disclosed data.

In the second step, we add personalization available as another main independent variable. We also consider the potential interaction effect between the new variable and data disclosed, which we 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.

For each step, we measured the adjusted *R*-squared. Table 7 indicates whether the inclusion of additional variables increased the overall explanatory power of the model.

Table 7: Regression models

Dependent variable: user's payoff				
	Step 1	**Step 2**	**Step 3**	**Step 4**
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;
control: control over personal data;
*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;
fsp: familiarity with smart phone;
fmsl: familiarity with mobile services using location;
authenticity: authenticity of personal data;
*data*pers*control*: interaction of personal data disclosed, personalization available and control over personal data;
_cons: constant.

As Table 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 [41], which found a value at 0.60 as well. Interestingly, we 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*.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

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). We 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 [27], we confirm that gender was an effect on user's payoff. We 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, we divide our sample into two clusters accordingly. We adopt the median cluster method based on two variables: subjects' global concerns for privacy and concerns in the mobile service sector. We exclude sample observations that are equal to the value of the median. We conduct regression analysis for both clusters, and the results are indicated in Table 9.

We 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 [7]. 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 essential indicators. In the last column of Table 8, we 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 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	-1.364*	-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;
control: control over personal data;
*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;
fsp: familiarity with smart phone;
fmsl: familiarity with mobile services using location;
authenticity: authenticity of personal data;
*data*pers*control*: interaction of personal data disclosed, personalization available and control over 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.* We also observe from Table 8 that the adjusted *R*-squared is 0.449 for risk-neutral mobile users, indicating that the overall

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

explanatory power of the model is increased within this group, as opposed to the one that includes all observations (Table 7).

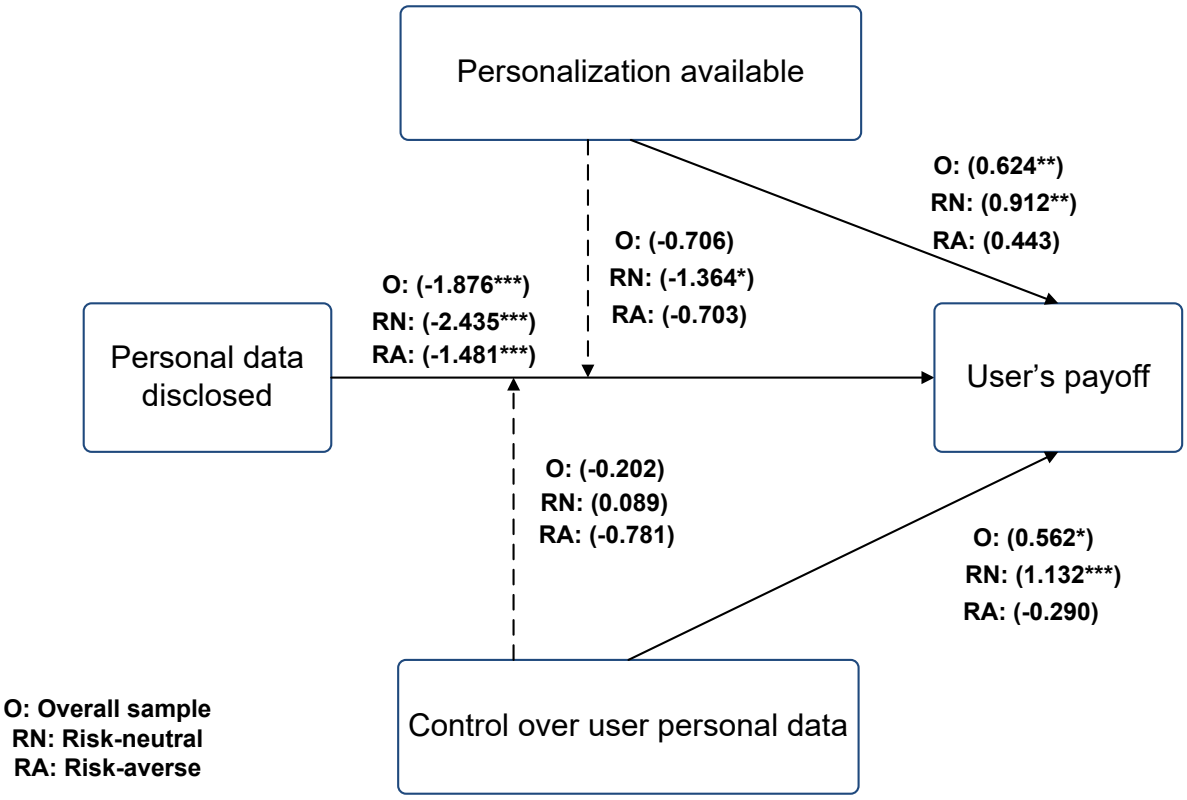

Figure 3: Test model of user payoff

Notes:
**p* < .1; ***p* <.05; ****p* < -01

In Figure 3, we describe how our 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.

5 Implementation of the Theoretical Model: The Trusted Infomediary Pattern

In this section, we derive guidelines to design privacy-friendly business models. We start by mapping the concepts of the theoretical model tested in the previous section onto the nine building blocks of the Business Model Ontology [34]. Then we complete the business model of a third-party agent, which has a value proposition structure around privacy protection, using the description of an infomediary [21].

5.1 Mapping our 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 9.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

Table 9: Regression for risk-neutral and risk-averse users

Business model constructs	**Description of the business model constructs (from [34])**	**→ mapping to our model**
Value proposition (VP)	The bundle that create value for a specific Customer Segment	User payoff
Customer segment (CS)		2 types of user
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 (KR)	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$)	All costs incurred to operate a BM	--
Revenue streams (R$)	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 [9]. 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 our 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 our model define that it applies to Location-Based Services; therefore, the distribution channel can be considered to be a mobile device with location-based services.

Customer Relationship specifies the type of relationship the customer expects and how it should be established and maintained (promotion, support, individual or mass). Our 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 our 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 our model seems to fall into this category.

Figure 4 describes how our model maps with the BMO. The numbers on the arrows refer to the values we obtained in Table 8. According to Figure 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.

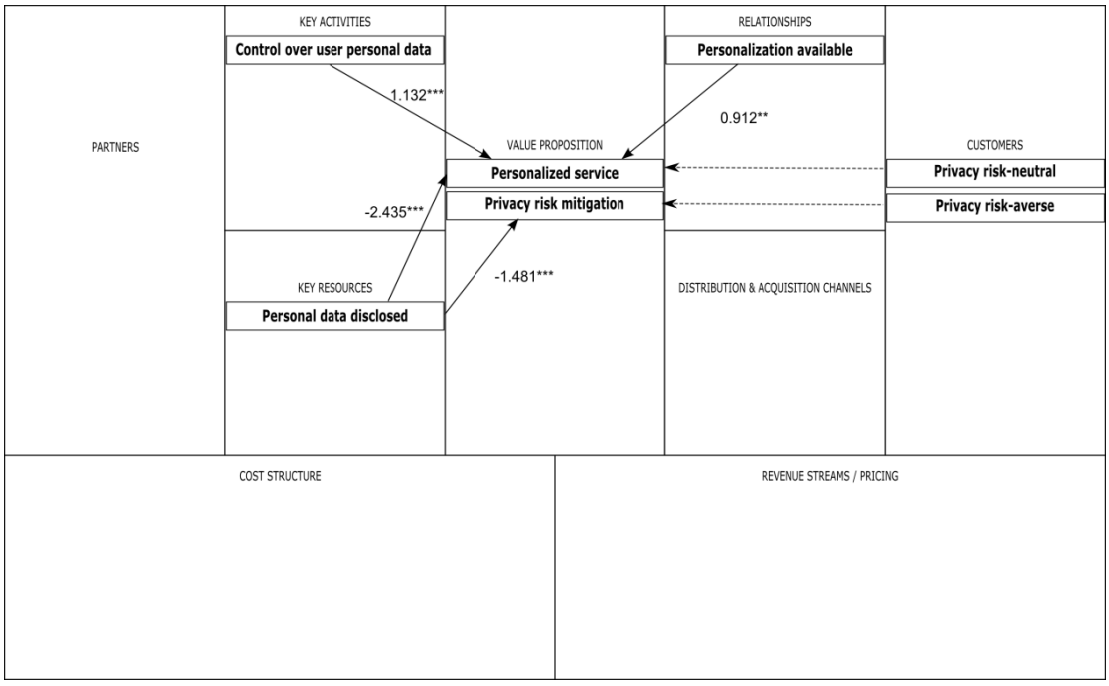

Figure 4: The theoretical model represented using the BMO

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

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 our model. In the next section, we obtain a profitable business model by referring to existing business model patterns.

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 [34]. 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 our purposes, we introduce the pattern of the infomediary as a special case of a multi-sided business model [16]. Infomediary is a term invented by [21]. 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 our 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 5 illustrates the effects of the infomediary pattern introduction on the components of our business model, which we describe here in detail.

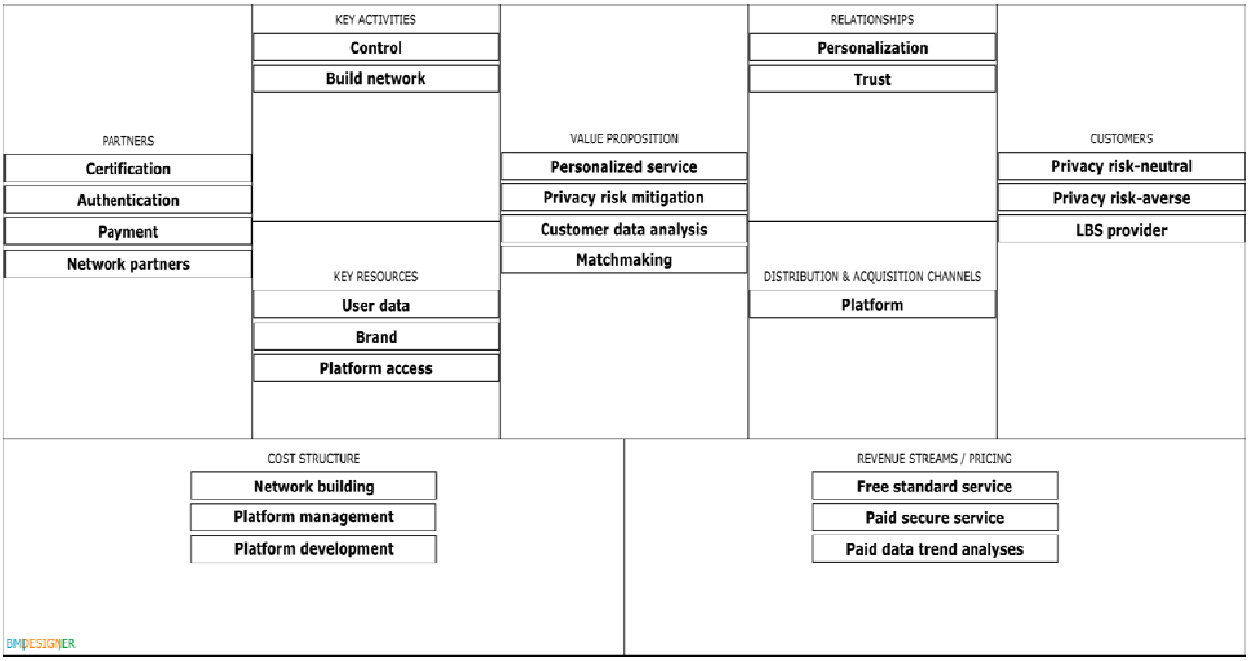

Figure 5: Business model for privacy as value proposition

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, we 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

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

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 Location-Based Services 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 [1]. 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 multi-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 [32].

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.

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 [39].

The literature review of the last ten years of research in privacy-enabling technologies done by [11] allows assessment of the limits of a trusted third party and supports a claim that it is possible to "crowd source" [24] both identity provision and attribute certification [44]. However this approach does not fully explain how to get rid of a trusted third party. Hence, we consider a combination of centralized and decentralized privacy control solutions. Figure 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

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

mobile device are illustrated. This way, we obtain four possible outcomes in our matrix, which we illustrate by using four possible market players as examples.

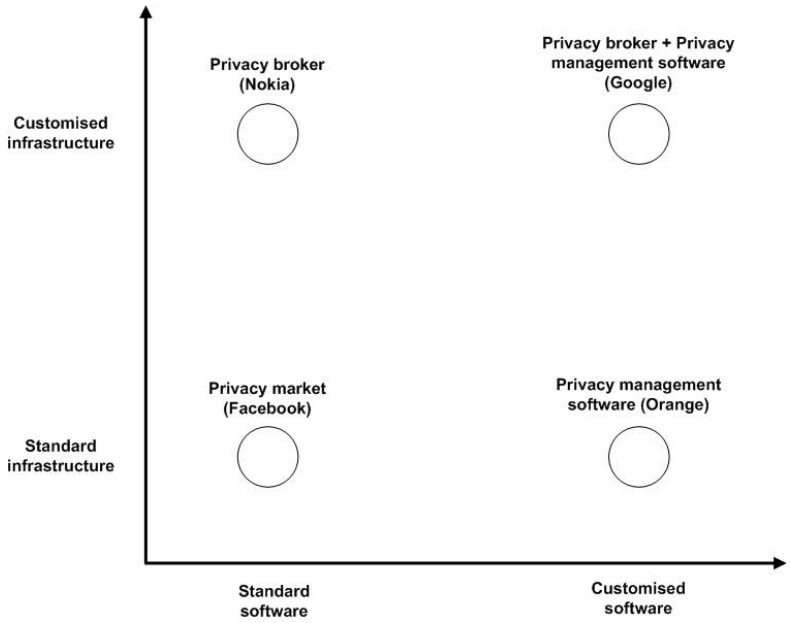

Figure 6: Four instances of a privacy-friendly business model (Infrastructure = centralized; software = decentralized)

Alliances among parties can maximize their payoff by cooperating, even though they have diverging goals [15]. On one hand, a firm that cannot avoid this kind of co-opeting relationship [30] 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.

6.1 Privacy Broker

Table 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, location-based services represent an additional stream of revenue generated from their investments in fixed infrastructure [38].

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 [39].

Over half of users would be happy if their CSP (Communication Service Provider) would fulfill the role of supervising permission policies [32]. 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 10: Adaptations required for the privacy broker

BMO Component	Adaptation Required
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 [23]).
Cost Structure	The cost of developing the platform. Costs relative to the infrastructure and its maintenance, which can be especially high in the case in which it has to scale for enormous demands for real-time transactions.
Revenue Streams	A fee over secure transactions paid by risk-averse users.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

6.2 Privacy Manager Software

Table 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 11: Adaptations required for the privacy manager software

BMO Component	Adaptation Required
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 a predetermined algorithm to assure user location privacy (for an example, the reader can see [17]). 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 solutions on the market, such as the dynamic settings manager for Android called Locale1. 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 because 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.

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 single sign-on user 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.

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 [3]. 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 [31]) 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. We 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 we envisage that in the near future, the firm could pay for its users' data.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 6 / ISSUE 2 / AUGUST 2011 / 90-107

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

7 Discussion and Conclusion

In this paper, we introduced the business model of a trusted third party to protect privacy while enabling location-based services. We ground our claims on a model developed specifically by incorporating existing works. The empirical data we collected extended previous knowledge in privacy management. We referred to business model ontology to derive a set of guidelines for business model designers and identified possible variations to our pattern of the privacy friendly business model inspired by the infomediary business model. We presented some market players who are potential candidates to provide instantiations of such a privacy protection service.

According to our findings, we answer our 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 4 strongly suggests that collected data reduces user payoff, whereas the combination of service personalization and data control increases user payoff. We confirm previous evidence [41] of a relation between service personalization and user payoff, and extend it with the notion of control in the B2C market. We also found two clusters that behave slightly differently from what has been seen for Internet privacy [27]. Our 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 our test, we 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 Single Sign-On 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, our proposed models for the service provider must be considered as initial intuitions.

On a more general level, we 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.

We feel that this paper offers some interesting [13] contributions to the field:

- We 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.

- We 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).

- We 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. We 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 our 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.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

Accordingly, one could decide to remove our 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 our proposed privacy business model pattern in other economic contexts, involving incomplete agreements and lack of trust among involved parties.

Acknowledgments

The work presented in this paper was supported by the Nokia Research Center (NRC) at Lausanne under the name *Pervacy Project* and by the Swiss National Science Foundation (NSF) under grant number 205121-120534. We thank Jialu Shan and Maria Dobrinas as well as the two anonymous reviewers for their useful advice.

References

[1] C. Anderson, Free: The Future of a Radical Price, New York: Hyperion, 2009.
[2] R. Anderson, Why information security is hard: An economic perspective, in Proceedings 17th Annual Computer Security Applications Conference, USA, 2001, pp. 358-365.
[3] J. Angwin and W. Steel. (2011, February). Web's hot new commodity: Privacy, The Wall Street Journal. [Online]. Available: http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.
[4] N. F. Awad and M. S. Krishnan, The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization, MIS Quarterly, vol. 30, no. 1, pp. 13-28, 2006.
[5] M. Barrett, K. Garrety, and J. Seberry, ICT professionals' perceptions of responsibility for breaches of computer security, in Proceedings of the 20th ANZAM (Australian New Zealand Academy of Management) Conference on Management: Pragmatism, Philosophy, Priorities, Central Queensland University, Rockhampton, 2006.
[6] I. Benbasat and R. W. Zmud, The Identity crisis within the IS discipline: Defining and communicating the discipline's core properties, MIS quarterly, vol. 27, no. 2, pp. 183-194, 2003.
[7] J. Bonneau and S. Preibusch, The privacy jungle: On the market for data protection in social networks, in Economics of Information Security and Privacy, 1st ed., XVI (C. Loannidis, T. Moore and D. Pym, Eds.), Berlin: Springer, 2010, pp. 121-167.
[8] R. K. Chellappa and R. G. Sin, Personalization versus privacy: An empirical examination of the online consumer's dilemma, Information Technology and Management, vol. 6, no. 2, pp. 181-202, 2005.
[9] K. W. Chew, P. Shingi, and M. Ahmad, TAM derived construct of perceived customer value and online purchase behavior: An empirical exploration, in Proceedings Project E-Society: Building Bricks, Boston, 2007, pp. 215–227.
[10] O. P. Cox, A. Dalton, and V. Marupadi, Smokescreen: flexible privacy controls for presence-sharing, New York, 2007, pp. 233-245.
[11] G. Danezis and S. Gürses, A critical review of 10 years of Privacy Technology, in Proceedings of Surveillance Cultures: A Global Surveillance Society?, London, UK, 2000.
[12] T. K. Das and B. S. Teng, Trust, control, and risk in strategic alliances: An integrated framework, Organization Studies, vol. 22, no. 2, pp. 251-283, 2001.
[13] M. S. Davis, That's interesting! Towards a phenomenology of sociology and a sociology of phenomenology, Philosophy of the Social Sciences, vol. 1, no. 4, pp. 309-344, 1971.
[14] T. Dinev and P. Hart, An extended privacy calculus model for e-commerce transactions, Information Systems Research, vol. 17, no. 1, pp. 61-80, 2006.
[15] M. J. Dowling, W. D. Roering, B. A. Carlin, and J. Wisnieski, Multifaceted relationships under coopetition, Journal of Management Inquiry, vol. 5, no. 2, pp. 155-167, 1996.
[16] D. S. Evans and R. Schmalensee, The industrial organization of markets with two-sided platforms, Competition Policy International, vol. 3, no. 1, pp. 151-179, 2005.
[17] J. Freudiger, M. Manshaei, J. P. Hubaux, and D.C. Parkes, On Non-cooperative location privacy: A game-theoretic analysis, in Proceedings of the 16th ACM Conference on Computer and Communications security, NY, USA, 2009. [Online]. Available: http://infoscience.epfl.ch/record/140427/files/ccs179-freudiger3.pdf.
[18] G. Giaglis, P. Kourouthanassis, and A. Tsamakos, Towards a classification framework for mobile location services, Mobile Commerce: Technology, Theory, and Applications (B. E. Mennecke, T. J. Strader), PA: Idea Group Publishing, 2002, pp. 67-85.
[19] B. Gibson and W. Holden. (2010, March) Mobile Location Based Services. Applications, Forecasts & Opportunities 2010 - 2014. Juniper Research. [Online]. Available: http://www.juniperresearch.com/shop/products/whitepaper/pdf/Juniper%20Research%20MLBS10%20White%20Paper.pdf.
[20] S. Gregor and D. Jones, The anatomy of a design theory, Journal of the Association for Information Systems, vol. 8, no. 5, pp. 312-335, 2007.
[21] J. Hagel and M. Singer, Net Worth: Shaping Markets When Customers Make the Rules. Boston: Harvard Business School Publishing, 1999.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762011000200009

[22] D. S. Herrmann, Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI. FL: Auerbach Publications, 2007.
[23] D. Hong, M. Yuan, and V. Y. Shen, 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, 2005, pp. 1-8.
[24] J. Howe. (2006, June) The Rise of Crowdsourcing, Wired. [Online]. Available: http://www.wired.com/wired/archive/14.06/crowds.html.
[25] K. Hui, H. H. Teo, and Lee, S. The value of privacy assurance: an exploratory field experiment, Management Information Systems Quarterly, vol. 31, no. 1, pp. 19-33, 2007.
[26] T. Husson. (2010, July) Profiling Your Best Mobile Customers, Forrester Research. [Online]. Available: http://www.forrester.com/rb/Research/profiling_best_mobile_customers/q/id/56916/t/2.
[27] C. Lancelot Miltgen, Disclosure of personal data and expected counterparties in e-commerce: a typological and intercultural approach, Management Information System, vol. 15, no. 4, pp. 1-49, 2010.
[28] N. K. Malhotra, S. S. Kim, and J. Agarwal, Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model, Information Systems Research, vol. 15, no. 4, pp. 336-355, 2004.
[29] S. T. March and G. F. Smith, Design and natural science research on information technology, Decision Support Systems, vol. 15, no. 4, pp. 251-266, 1995.
[30] B. Nalebuff and A. Brandenburger, Co-opetition: Competitive and cooperative business strategies for the digital economy, Strategy & Leadership, vol. 25, no. 6, pp. 28-35, 1997.
[31] D. H. Nguyen and E. D. Mynatt, Privacy mirrors: Understanding and shaping socio-technical ubiquitous computing systems, Georgia Institute of Technology, Georgia, Atlanta, Technical Report GIT-GVU-02-16, 2002.
[32] Nokia Siemens Networks Corporation. (2009) Privacy survey, Nokia Siemens Networks. [Online]. Available: http://www.nokiasiemensnetworks.com/sites/default/files/document/SDM_PrivacyStudy_Brochure.pdf.
[33] Organisation for Economic Co-operation and Development. (2002) OECD guidelines on the protection of privacy and transborder flows of personal data. OECD Publishing. [Online]. Available: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
[34] A. Osterwalder and Y. Pigneur, Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. Wiley, Indianapolis: OSF, 2010.
[35] L. Palen and P. Dourish, Unpacking privacy for a networked world, in Proceedings of the ACM Special Interest Group on Computer-Human Interaction, Conference on Human factors in computing systems, Florida, USA, pp. 129-136.
[36] J. Phelps, G. Nowak, and E. Ferrell, Privacy concerns and consumer willingness to provide personal information, Journal of Public Policy & Marketing, vol. 19, no. 1, pp. 27-41, 2000.
[37] J. Pries-Heje, J. Venable, and R. Baskerville, Strategies for design science research evaluation, in Proceedings of the 16th European Conference on Information Systems, Galway, Ireland, 2008, pp. 255-266.
[38] B. Rao and L. Minakakis, Evolution of mobile location-based services, Communications of the ACM, vol. 46, no. 12, pp. 61-65, 2003.
[39] M. de Reuver and T. Haaker, Designing viable business models for context-aware mobile services, Telematics and Informatics, vol. 26, no. 3, pp. 240-248, 2009.
[40] H. Sheng, F. F. Nah, and K. Siau, An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns, Journal of the Association for Information Systems, vol. 9, no. 6, pp. 344-376, 2008.
[41] J. Y. Son and S. S. Kim, Internet users' information privacy-protective responses: A taxonomy and a nomological model, MIS Quarterly, vol. 32, no. 3, pp. 503-529, 2008.
[42] K. A. Stewart and A. H. Segars, An empirical examination of the concern for information privacy instrument, Information Systems Research, vol. 13, no. 1, pp. 36-49, 2002.
[43] R. I. Sutton and B. M. Staw. (1995, September). What theory is not, Administrative Science Quarterly. [Online]. vol. 40, no. 3, pp. 371-384. Available: http://www.jstor.org/stable/2393788.
[44] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, Sybillimit: A near-optimal social network defense against sybil attacks, in Proceedings IEEE Symposium on Security and Privacy DBL, Oakland, CA, 2008, pp. 3-17.