Business Model Considerations for Privacy Protection in a Mobile Location Based Context

Riccardo Bonazzi
Faculty of Business and Economics
University of Lausanne
1015 Lausanne Switzerland
Email: riccardo.bonazzi@unil.ch

Boris Fritscher
Faculty of Business and Economics
University of Lausanne
1015 Lausanne Switzerland
Email: boris.fritscher@unil.ch

Yves Pigneur
Faculty of Business and Economics
University of Lausanne
1015 Lausanne Switzerland
Email: yves.pigneur@unil.ch

***Abstract*—In this paper we discuss the main privacy issues around mobile business models and we envision new solutions having privacy protection as a main value proposition. We construct a framework to help analyze the situation and assume that a third party is necessary to warrant transactions between mobile users and m-commerce providers. We then use the business model canvas to describe a generic business model pattern for privacy third party services. This pattern is then illustrated in two different variations of a privacy business model, which we call privacy broker and privacy management software. We conclude by giving examples for each business model and by suggesting further directions of investigation.**

I. Introduction

In this paper we refer to the right of privacy as *the right to be left alone; right of a person to be free from unwarranted publicity; and right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned. There are four general categories of tort actions related to invasion of privacy: (a) appropriation, (b) intrusion, (c) public disclosure of private facts, and (d) false light privacy* (Black's Law dictionary in [1]). Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

Situation dependency in e-commerce can be conceived to comprise three dimensions: identity (the identity of the user), spatiality/ubiquity (the place of use), and temporality (the time of use) [2]. Ubiquity refers to the ability to access information from any location at any time. Ubiquity can be beneficial in cases where timely information is important. Localization provides customized information based on physical location [3], thereby being more relevant. The possibilities of ubiquitous access to timely and relevant information have become a reality with today's devices. Mobiles have evolved beyond their previous limitations: screens sizes are bigger, can display high resolution color content. Storage capacity, data transfer rates and device processing power, have also greatly improved. Some limitation due to lack of keypad have been alleviated through multi-touch input on the whole surface of the screen. Location has become more precise through the broad availability of GPS and AGPS integrated into the devices. The major remaining limitations, but which are not hindering the emergence of location based services, are battery capacity and the heterogeneity of the multiple platforms available.

In the rest of the paper we focus on localization-based services offered in the Business to Consumer (B2C) market. Glaglis et al. [4] provides a taxonomy of the mobile services, among which we select those offering navigation, information, advertising, tracking and billing. We exclude from our analysis the emergency services because it has been previously shown by Sheng et al [5] that users do not fear for their privacy in an emergency context.

New regulatory requirements, such as the guidelines given by the Organisation for Economic Co-operation and Development [6], and consumer concerns are driving companies to consider more privacy-friendly policies for emergent privacy oriented business models, but such policies often conflict with the desire to leverage customer data. Gaining access to real intentions and close proximity of potential customers has a real value for business, as shows a report published by Juniper Research, which predicts revenues from mobile location-based services to be more than $12.7 billion by 2014 [7].

Our research question is: **which are the required business model components, that allow a high level of customer experience for a mobile location-based service in a B2C market, while keeping the collected data to a minimum?**

In this paper we adopt a design science research methodology proposed by Gregor and Jones [8]. In the next section, we propose a framework based on existing research on privacy and location based services. The third section introduced the underlying knowledge we refer to, to illustrate business models throughout the article. In the fourth part, we describe how to implement a generic business model for privacy, and then we present a set of possible instantiations. Some testable propositions are then presented in th sixth section together with ideas for the evaluation of the proposed models. The last section discuss the implications of our analysis.

978-1-4244-7445-5/10/$26.00

II. Framework to design business models for privacy management

According to Palen and Dourish [9] privacy is a *dynamic and dialectic process of give and take between and among technical and social entities from individuals to groups to institutions in ever-present and natural tension with the simultaneous need for publicity*. Thus, we assume having two actors: a mobile user and a mobile service provider we will call m-commerce provider.

The *user data* the mobile user shares with the provider could be either harmless to user's privacy or it could allow user's full identification. In exchange of the *user data* the m-commerce provider could offer a service, which is either standard or fully customized. In this sense we introduce the concept of service *personalization*, which Chellappa and Sin, (2005) [10] define as dependent on two factors: 1) companies' abilities to acquire and process customers' information; and 2) customers' willingness to share information and use personalized services.

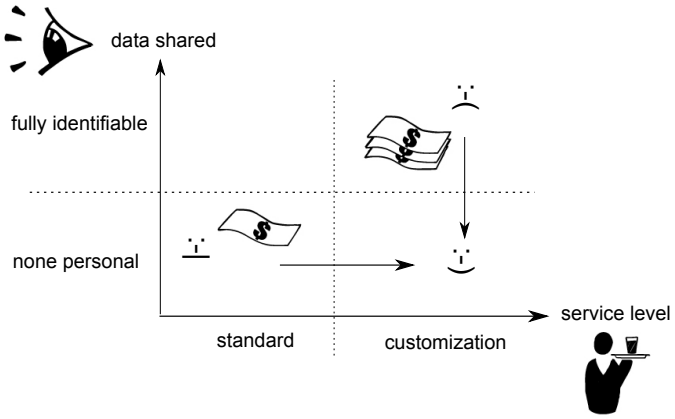

Fig. 1. Our proposed framework to assess business models for privacy management

A. The framework

Figure 1 presents the results of the dialectic process between the mobile user and m-commerce provider. One could model this phenomenon as a game where each player can share his resources hoping that the other player will do the same. Thus the user can decide how much personal data he discloses, while the m-commerce provider can decide what level of personalization it will offer in exchange. In an attempt to model this relationship, one could see the payoff of the mobile user as a direct consequences of the amount of *personalization* allowed with a moderating effect done by the user's exposure to *privacy risk*. On the other hand the payoff of the provider is proportional to the amount of *user data* disclosed with a moderating effect done by the control effort to mitigate the user's exposure to privacy risk. Hence we could express that in the following way:

$$Payoff_{user} = Personalization - PrivacyRisk$$
$$Payoff_{provider} = UserData - (1 - PrivacyRisk)$$

As in many iterative games both players optimize their payoffs as long as they cooperate and that depends on their mutual trust. We refer to Das and Teng [11] to assess that such trust is positively related to the amount of control effort the enterprise assign to lower the *privacy risk*. Such privacy risk depends on the amount of *user data* that is disclosed, and we assume that such dependency is non-linear. Indeed, previous studies have shown that personal information can be derived from those that have been disclosed, making the disclosure of twice the amount leading to a privacy risk that is far greater than double. Thus we express the privacy risk as a quadratic function of the disclosed data with a moderating effect done by the *control effort* of the provider.

$$PrivacyRisk = UserData^2 - Personalization * ControlEffort$$

The payoff for the user and the provider are derived as it follows:

$$\begin{aligned} Payoff_{user} &= Personalization - PrivacyRisk \\ &= -UserData^2 + Personalization \\ &\quad * (1 + ControlEffort) \\ Payoff_{provider} &= UserData - (1 - PrivacyRisk) \\ &= UserData^2 + UserData \\ &\quad - (1 + Personalization * ControlEffort) \end{aligned}$$

This set of formula finds support from previous studies. According to De Vos et al [12] people prefer utilitarian (pragmatic) services and basically just want to share location information with their partners. A study from Nokia Siemens Networks [13] and a research from Bonneau and Preibush [14] identified three types of user: *afraid* protect their data by minimizing the disclosure of information; *selective* are pragmatic and more willing to accept privacy risks in return for added value; *uninvolved* tend to be younger, less likely to own a credit card and lack awareness of privacy issues. This is consistent with our model, where the negative effect of disclosed data can be offset by the services given in return to the user. One can define the control effort as the one perceived by the mobile user, leading to subjective measures depending on the type of user.

Location based services seem for the most part be based around a free model, as shown by a study from KPMG [15], since there seems to be an unwillingness on the part of the user to pay for mobile services. We refer to the concept of asset complementarity described by Teece [16] to note that simply adding context aware features to mobile services does not automatically result in added value to users. *[The] most marketable service do not come as a direct consequence of the [firm's] ability to identify someone's location through a mobile*

device, but rather through combining location identification with additional data to provide added value to the user [4]. This is consistent with our model, where the negative effect of service delivery is compensated by the amount of data collected, rather than by the money paid for the service.

B. A dynamic analysis of the four outcomes

Four possible outcomes can be derived from the combination of the two actors' strategies. The bottom left quadrant concerns value propositions that offer little in exchange of little user data, which is a standard Web 1.0 approach. On the contrary the fully customizable m-commerce service with a fully identifiable user is a typical Web 2.0 approach. In the top left quadrant we feature all business models that collect a large amount of data in exchange of a poor service. Such models have been the subjects of a large number of study. For example Chellappa and Sin [10] have already shown that *non-monetary benefits such as convenience from online personalization can also serve as incentives for consumers to part with their personal and preference information*. An increasing amount of information about a customer can be converted into more profit, either directly by cross-selling or indirectly by selling aggregated data to third parties.

Market forces push the provider towards high incomes by selling user's data, whereas regulatory forces defend the request of the user for a good service that does not put privacy in peril. Using our framework one can explore the dynamic evolution of the two conflicting forces. We assume that the regulatory and economic forces do not allow the payoffs of the user and the provider to go below zero.

The bottom right corner represents a major challenge in what concerns profitability, which we believe has been understudied so far and that represents the main focus of the rest of the paper. Indeed, we assume that privacy friendly business models better address current trends of corporate social responsibilities, providing new value for customers without adding high cost for the enterprise. So far the framework has helped us identify the two actors involved in a coopeting relationship where trust is of paramount importance for payoffs long-term maximization. We have shown how control can increase trust, but control implies additional costs for the firm. Hence we state here our central assumption concerning the presence of a third party actor to warrant the transaction between mobile users and m-commerce providers.

III. Underlying knowledge

In this section we introduce two sets of knowledge we referred to while doing our research. First, in order to describe the business model of a third party agent, which has a value proposition structure around privacy protection, we choose to use the Business Model Ontology [17] to describe it. Second, we base the business model of our third party on the business model of an infomediary as defined by [18].

A. Business model canvas

As we illustrate in [19], 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 can be seen in figure III-A.

At the center there is the *Value Proposition*, it describes which customer's problems are solved and why the offer is more valuable than similar products from competitors (product, service). The customer themselves are analyzed in *Customer Segment*, separated into groups to help in identifying their needs, desires and ambitions (singles, families). *Distribution Channel* illustrates how the customer wants to be reached and by whom he is addressed (Internet, store). In addition, *Customer Relationships* specifies what type of relationship the customer expects and how it is establish and maintained with him (promotion, support, individual or mass). To be able to deliverer the value proposition the business has to have *Resources* (staff, machines, secret knowledge). And transform theses resources through *Key Activities* into the final product or service (development, production, secret process). Most of the time a business depends also either for resources or for activities on an external *Partner Network* (logistics, financial), which can provide better quality or a lower price on non essential components. As any business model would not be complete without financial information the last two building blocks focus on cost and revenue: The *Cost Structure* which should be aligned to the core ideas of the business model (key resources, key activities) and *Revenue Streams* which mirrors the value the customers are willing to pay an how they will perform the transaction (one time fee, subscription).

Using their business model canvas Osterwalder and Pigneur [20] have presented a set of business model patterns. A business model pattern describes some components of a business model and their relationships, in manner they can be applied to similar situation. As with patterns in other fields, this allows to identify missing components once a certain situation is recognized (freemium, doublesided, unbundling, long tail).

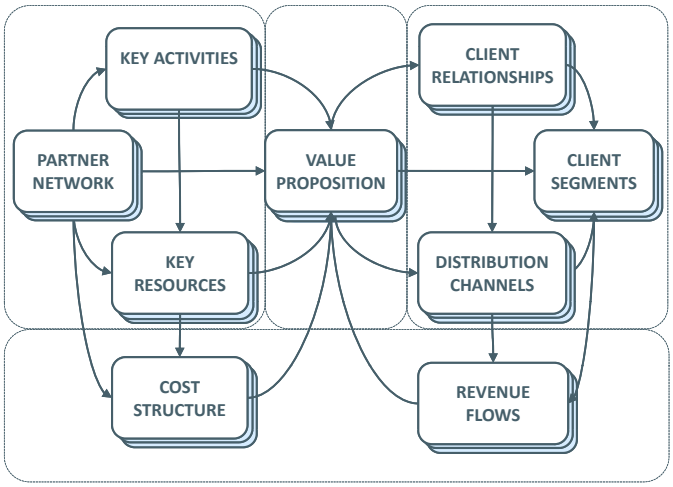

Fig. 2. Business model canvas

B. Infomediary

An infomediary [18], is a trusted third party which helps consumers and vendors connect. The role of the infomediary is to become the custodian, agent and broker of customer's information. At the same time the infomediary protects the consumer's privacy.

By connecting consumers and vendors the business model of an infomediary resembles the business model pattern of a double-sided business [21]. Meaning, that the third party has two distinct set of client segments, consumers and service providers, who need each other, who can't get together easily on their own and he helps them connect through his platform. The main cost of a double-sided business is maintaining and developing the platform. As for the revenues, each customer segments can generate revue or 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.

An infomediary can offer services to its consumer customer segment:

- Power of the number: by aggregating customers with the same interest the infomediary can negotiate better deals.
- Filter service: like a spam filter the user only receives advertisements based on his opt-in profile
- Agent service (search): based on the user's protected aggregated profile he can get better recommendation.
- Marketing service (subscribe): the user can opt-in to receive certain advertisements, in some cases even get paid for exposing parts of his detailed profile.
- Data Management and Analytics: display reports on user's profile to give him an overview of the collected information as well as building business rating to help the customer choose services.
- Purchase service (proxy): High-end privacy where the infomediary acts as a proxy for the transactions and the delivery in order to hide the customer from the business.

And to its service provider segment:

- Customer acquisition (match) : Customer can find the service offered by the business in the repository of partners of the infomediary
- Marketing (publish to segment): For users who opted-in the infomediary can forward target advertisement on behalf of a business. In return the business gets a better return on his advertisement since all the recipients should theoretically be in the target segment.
- Market research (benchmark): the aggregated information gives the possibility to compare results.

IV. A Business Model Pattern For Privacy

In this section we propose a special case of infomediary: a third party actor which does not aggregate data and does not provide additional marketing services to its customer. In this case of a privacy geared infomediary, we do have two distinct sets of customers: the mobile user and the m-commerce company, but they can easily get together on their own. On the other hand, what they might not be able to do without the infomediarie's help is to get together in a secure, privacy friendly way. The primary goal is to limit exposure of user's private information and help them manage their profile. We will use the nine business model elements defined by BMO to describe the requirements of such a third party as can be seen in figure 3. This first description is purposely kept at a high level of abstraction, in order for the model to be usable as a pattern. This pattern will then be used to illustrate examples in the following section.

A. Third party privacy pattern

Value proposition: Protecting user's privacy. According to nokia's survey [13] users seem to want *privacy protection*. *Also two thirds of mobile phone users like the idea of keeping things simple by placing all their data in the hands of a single personal data management portal*. This strengthens the need for a service which helps manage a privacy profile in one location for multiple services and helps reduce the control lose a user feels when he has to have a different profile for each service he uses. A second result of the survey that: *in spite of their stated concerns over privacy, users are generally willing to share data as long as they remain in control and can see the tangible benefits of doing so. Monetary benefits offer the strongest incentive*; indicates that the privacy broker has some margin of operation to still be able to offer incentives to the m-commerce company to join his platform. It might even be possible to offer more advanced services, based on the full infomediary model, to mobile users. This as long as benefits are clearly explained and linked to simple and transparent control choices (*Data Management*). The value for the m-commerce company is the tools provided with the platform, which allow them to implement privacy into their application without having to worry about it (*Privacy Infringement Reduction*). Therefore, they can focus on their business value and differentiate from other services through the third party's trusted system. The third party can always be circumvented by mobile users interacting directly with the m-commerce company, but these companies for the most part implement privacy only by policy, promising not to abuse the data they are provided. On the other hand the third party, through his platform can implement real privacy by architecture, which given enough awareness on real privacy protection should provide a key differentiator.

Customer segments: From the three types of mobile user, customers being *afraid* or very *selective* about their privacy, should be interested by a strong privacy guarantee. In addition, less selective and *uninvolved* customers should welcome the ability to securely manage in a single place their preferences. As for *m-commerce services*, any one who desires to add privacy to its service, in order to differentiate or tap in the pool of afraid user should well come such an offering.

Customer Relationships: The key to attracting users is to promote the importance of privacy protection, as well as building a very strong *trust* relationship with the customer. The privacy agent has to show its users that it knows the high value a user has for his personal data and prove he cares a

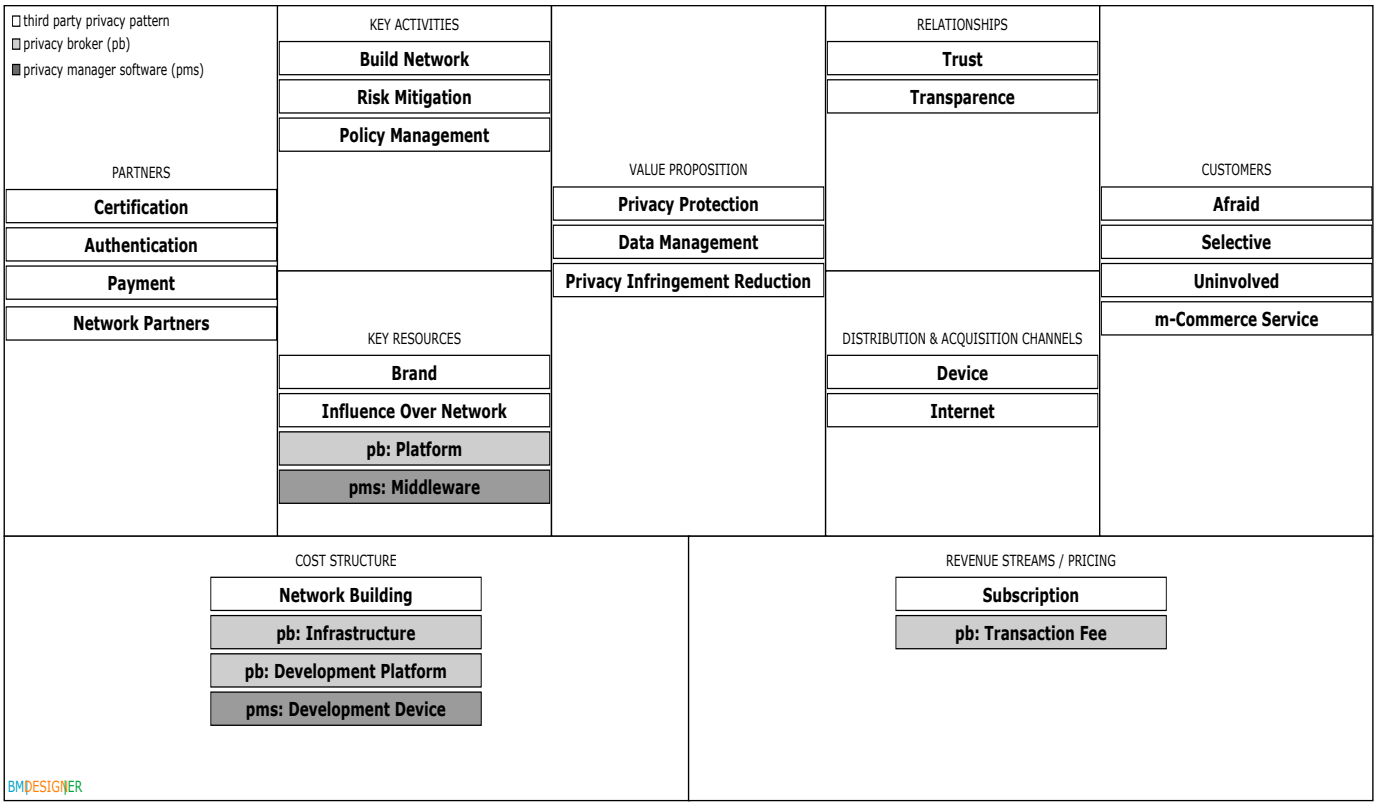

Fig. 3. Business models for privacy as value proposition

great deal for keeping it safe. This relationship is very similar which a bank has to its customers. One way to achieve this is by being *transparent*.

Channels: The platform or middleware deployed by the third party is based around the mobile *devices* he is interested to protect, as well as some kind of *Internet* presence to manage preferences.

Revenue Streams: It might be hard to make any of both segments, mobile users or m-commerce provider, pay directly for such a service. Alternative, revenue streams have to be found to subsidize the platform. There is the possibility to make revenue on premium services (*subscription*), but this is for services of the full infomediary which might contradict with the strong privacy values a third party privacy protection service should embody.

Key Activities: In addition to building its trustworthiness and staying up to date with privacy protection technologies, the third party has to be constantly *expanding its network* of customers and stay up to date with mobile device platforms. This is critical in order to maintain and enhanced its attractiveness (*Policy Management*). To assure compliance to the users' policies the privacy risk can be mitigated by implementing and mantaining a set of controls according to security frameworks such as CobiT and ISO 270001 together with privacy guidelines, as those described by the OECD [6]

Key Resources: The most important resource is to be trustful. This is represented by the *brand* value. Furthermore, in order to be able to grow the network the third party actor is in, he has to have some sort of *influence over the network*.

Key Partners: In order to guarantee the trust wordiness and security of his solution, as well as being able to certify that applications made for his platform are compliant, the third party itself has to be audited and *certified* by an external partner. The third party has also to have partnerships with mobile device manufacturer or network operators in order to realize and deploy his product (*Network Partners*). To offer additional services or implement additional privacy protection, he might also need to be in relationship with *identity* and *payment* providers.

Cost Structure: *Network building* and Policy Management activities are costly services.

B. Centralized vs on-device

There is a range of possibility for technical implementation of privacy protection, intended here as algorithms, data storage and policies. As shown by interviews done by de Reuver et al. [22]: *Experts have different opinions. Some of them saw centralized personalization as a major trend in the telecommunication world, whereas others expected that most of the personalization would take place on the end-user terminal for reasons of usability, response time and privacy.*

We refer to the analysis of Dowling et al. [23] regarding alliance among parties that can maximize their payoff by cooperating although they have diverging goals (co-opetition). According to Downling et al [23] a firm that cannot avoid

this kind of co-opeting relationship in non core competences 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 competences areas can best adapt by centralizing information about the relationship through establishing an interorganizational structure (the *platform*) to share information. Hence we identify two variations of the infomediary pattern for the third party actor: the *privacy broker* and the *privacy management software*. As presented in figure 3 we illustrate in details only the elements of each pattern that differ from the standard one.

C. Privacy broker

Key Resources: The key resource is the *platform* itself. 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. We cite the solution proposed by Hong et al [24] as an example.

Cost Structure: In addition of the cost of *developing the platform*, there are the cost of the *infrastructure* and its maintenance. Which can be especially high in the case it has to scale for enormous demands for real-time transactions.

Revenue Streams: The advantage of a centralized system, is the possibility to better control transaction and have the opportunity to collect a *fee* from the m-commerce customer.

D. Privacy manager software

Key Resources: The key resource in a decentralized solution is under the shape of a *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's location privacy. We cite the analysis and the solution proposed by Freudiger et al [25] as an example. This way the user could download the application on the phone and let the software manage the phone applications accordingly 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[1]. 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. But there are no fixed infrastructure costs and once device platforms stabilize, maintenance cost should also diminish.

V. Business Model Instances

In this section, we apply the two alternative business model patterns of a third party privacy provider to tangible candidates who could implement them, since we did not identify infomediaries which are already offering such services.

[1]http://www.twofortyfouram.com/

Infomediaries were believed to be the ultimate solution for customer control over his information around the year 2000. Ten years later, no real infomediary focusing on privacy emerged.

One argument brought forth by [26] is the fact that Businesses do not sufficiently trust the third party with the storage of their transactional data, they predicted the downfall of services like ZeroKnowledge as users are still suspicious despite trusted third party reassurances. Infomediary as a standalone business model seems unfeasible due to the high cost structure and customers unwillingness to pay for such a service.

A third party privacy provider solution seems therefore only viable as an added value service for an existing business model. In addition, the company wanting to build a platform has to be large enough to be able to create a big enough base of mobile customers and m-commerce company willing to offers service through the platform, in order to make it possible for a network effect to occur. Furthermore, clients will only consider such a service if they have trust into the institution providing it. Based on the results of Nokia survey the most trusted companies are banks and communication service providers. Google is also ranked as one of the more credible company. Even if banks are ranked highest, from a technological standpoint we do not consider them as easy candidates to implement a third party privacy service. On the other hand, they could become partner or sponsor of such a system in order to inherit the trust users have in them. Nevertheless, it can also be dangerous for banks to associate with a privacy protection system where leeks might occur and damage their reputation.

For the privacy broker model we choose the mobile network operator as an ideal candidate. As for the privacy manager software we propose to apply it to an operating system provider. Additionally, we also take the case of Google who has the possibility to implement a mix of both alternatives.

A. Mobile network operators

Mobile network operators (MNO) are good candidates for deploying a privacy broker since they by nature already possess location information and have direct access to the infrastructure if required by a privacy security implementation. For Mobile network operators, location-based services represent an additional stream of revenue that can be generated from their investments in fixed infrastructure [27].

For GPS-enabled terminals, the location of the intelligence is shifting towards 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 service can become a key differentiator for mobile network operator [22].

In addition, Nokia's privacy survey [13] shows that: *Over half of the users would be happy for their CSP (Communication Service Provider) to fulfill this role and supervise all their various permissions*.

Therefore, the MNO possess already several components of a privacy broker: A large network of potential customer

who trust him, resources and partners to do transaction and payment capabilities. In some countries, MNO operate under strict telecommunication laws, which give an added bonus to their trustworthiness. Having a large investment in a fixed infrastructure, the privacy broker model seems the optimal choice, and a centralized profile management might even integrate with the user's current profile he already has with the MNO. Moreover, providing new m-commerce services like location sensitive billing might be very attractive to current phone billing possibilities. The biggest difficulty is the creation of relationships to m-commerce providers.

B. Operating system provider

Operating system providers of mobile devices are in a good position to influence privacy protection in their platform. They have direct access to the raw sensor of the phone and can define what information is exposed to applications through their APIs. Moreover, they have the possibility to integrate the privacy middleware directly into the operating system and thereby target there whole market at once. In addition, they might have an easier job integrating a user friendly profile management into the system. Providing a privacy system can further help them expand the dominance of their operating system market share. Also, since most of modern operating system for phones already posses a market place the contact with m-commerce companies, the second consumer segment, is already established.

C. Google

Google appears to be an ideal candidate for becoming a centralized service for managing users privacy profile. They already offer single sign on user authentication, they have a mobile phone operating system (Android), which includes location applications (Latitude), they are used to handle private information like emails (Gmail) and documents (Google Docs). In addition, Google has already implemented some aspects of an infomediary with their Google health offering, as well as their dashboard which gives user's an overview of all their Google services and settings.

Google is in a special position where they can choose to implement either a privacy broker model around their server infrastructure or integrate a privacy manager into their Android operating system. This gives them the unique opportunity to also choose a mix of both alternatives, which could be more independent (phone based middleware) as well as when needed support real-time centralized server based privacy mediation.

The caveats is that Google is a private company and their main business model is to sell targeted advertising, which might conflict with privacy protection ideals.

D. Privacy market

Another variation on the informediary model would be to create a market for user's information. This third party would not be about privacy protection, but about means for clients to monetize and profit from their own information profiles, while still being in control of who gets what. Companies could put in offers for specific customer segment information, and customers could publish their profile with detailed information and control which type of offer can access each part of it. The third party's role would be to guarantee the transactions and quality of the data by providing the appropriate market tools.

VI. Testable Propositions

The proposed framework presented in section II supports the following propositions:

- **P1**: There is a inverted u-shaped relationship between the payoff of the user and the personal data disclosed
- **P2**: There is a u-shaped relationship between the payoff of the company and the personal data disclosed
- **P3**: The amount of personalization available and the control over user personal data have a moderating effect over the user and the company's payoffs

Once the first three propositions are verified we introduce a set of propositions regarding our variations of the infomediary pattern. We refers to the resource based theory extended by Dowling et al [23] for alliances among coopetiting actors and we assess that:

- **P4**: If the user's personal data affects the core competences of the provider, then the *privacy broker* business model is more likely to be implemented
- **P5**: If the user's personal data does not affect the core competences of the provider, then the *privacy management software* business model is more likely to be implemented

VII. Discussions And Conclusion

In this paper we introduced the business model of a trusted third party agent which can help in protecting privacy while enabling location based services. We referred to the business model ontology of Osterwalder and Pigneur and we identified two possible variations of a pattern for a privacy protection 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 and we concluded with a set of testable propositions. Hence the contribution of this paper is threefold:

- We present a clear framework to classify an enterprise's position in relation to its competitors in what concerns the trade-off between user's location privacy and personalization of the service offered.
- We call for better and more privacy friendly business models and we present two possible examples of these models.
- We argue by mean of an instantiation that the mobile platform can play a key role at multiple levels (OS, device manufacturer, operator) in the implementation of these new business models.

Our proposed framework is to be considered as an initial step to conceive a tool to support strategic decisions. The current payoff formulas have been conceived for illustration purpose and for that reason do not capture all the complexity of the real system.

We also wish to explore the evolution of the privacy issue in the future. Privacy has gained awareness in the last years but we are only at the beginning of it being a technological trend. The definition of privacy guidelines within a common framework has just started and there are no largely adopted solution integrated into a platform. As long as there are no standard, and no real added value, or perceived added value, to enforce privacy there is always the possibility to go directly to the vendor and to use raw data from the phone's sensors. According to Bonneau [14] there is no incentive to provide good privacy control functionality for business, because it does not help them differentiate from other services. Therefore, privacy protection has a bootstrapping problem: users do not seem to be fighting for privacy and business have no incentives to implement it. We argue that it is a social responsibility for companies to start leading the privacy movement instead of waiting for users to ask for it.

Supposing that no third-party actor emerges some firms might be implementing some elements of our proposed pattern to add privacy risk mitigation in their value proposition and to 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 our initial assumption regarding the existence of a third party actor. As proposed by Dowling et al [23] the best strategy for a firm is to internalize the third party, if it involves its core competences. This again might rise strategic issues about service integration and business model unbundling.

As further work, there exists the possibility to leverage our proposed privacy business model pattern in other economical contexts, which involve incomplete agreements and lack of trust amongst involved parties. For example, an ecology friendly business model seems to have many elements in common with our pattern.

ACKNOWLEDGMENT

The work presented in this paper was supported by the Nokia Research Center (NRC) at Lausanne under name *Pervacy Project*.

REFERENCES

[1] D. S. Herrmann, *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*, 1st ed. Auerbach Publications, 2007.

[2] S. Figge, "Situation-dependent services–a challenge for mobile network operators," *Journal of Business Research*, vol. 57, no. 12, pp. 1416–1422, 2004.

[3] C. Looney, L. Jessup, and J. Valacich, "Emerging business models for mobile brokerage services," *Communications of the ACM*, vol. 47, no. 6, pp. 71–77, 2004.

[4] G. Giaglis, P. Kourouthanassis, and A. Tsamakos, "Towards a classification framework for mobile location services," *Mobile commerce: technology, theory, and applications*, pp. 67–85, 2002.

[5] H. Sheng, 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.

[6] O. for Economic Co-operation and Development, *OECD guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing, 2002.

[7] R. Wauters, "Mobile Location-Based services could rake in $12.7 billion by 2014," http://techcrunch.com/2010/02/23/location-based-services-revenue/, Feb. 2010.

[8] S. Gregor and D. Jones, "The anatomy of a design theory," *Journal of the Association for Information Systems*, vol. 8, no. 5, p. 312, May 2007.

[9] L. Palen and P. Dourish, "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, 2003, p. 136.

[10] R. K. Chellappa and R. G. Sin, "Personalization versus privacy: An empirical examination of the online consumers dilemma," *Information Technology and Management*, vol. 6, no. 2, p. 181202, 2005.

[11] T. K. Das and B. S. Teng, "Trust, control, and risk in strategic alliances: An integrated framework," *Organization Studies*, vol. 22, no. 2, p. 257, 2001.

[12] H. de Vos, T. Haaker, M. Teerling, and M. Kleijnen, "Consumer value of context aware and location based mobile services," in *Proceedings of the 21st Bled e-Conference e-Collaboration: Overcoming Boundaries through Multi-channel Interaction, Slovenia*, 2008, pp. 50–62.

[13] N. S. Networks, "Privacy survey 2009," Nokia Siemens Networks, Tech. Rep., 2009.

[14] J. Bonneau and S. Preibusch, "The privacy jungle: On the market for data protection in social networks," in *The Eighth Workshop on the Economics of Information Security (WEIS 2009)*, 2009.

[15] KPMG, "Consumers and convergence, challenges and opportunities in meeting next generation customer needs," KPMG, Tech. Rep., 2006.

[16] D. J. Teece, "Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy," *Research policy*, vol. 15, no. 6, p. 285, 1986.

[17] A. Osterwalder and Y. Pigneur, "An e-business model ontology for modeling e-business," in *15th Bled Electronic Commerce Conference*. Bled, Slovenia, 2002, p. 1719.

[18] J. Hagel and M. Singer, *Net worth: shaping markets when customers make the rules*. Harvard Business Press, 1999.

[19] B. Fritscher and Y. Pigneur, "Supporting Business Model Modelling: A Compromise between Creativity and Constraints," *Task Models and Diagrams for User Interface Design*, pp. 28–43, 2010.

[20] A. Osterwalder and Y. Pigneur, *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. Wiley, 2010.

[21] D. Evans and R. Schmalensee, "The industrial organization of markets with two-sided platforms," *NBER working paper*, 2005.

[22] 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.

[23] M. J. Dowling, W. D. Roering, B. A. Carlin, and J. Wisnieski, "Multifaceted relationships under coopetition: Description and theory," *Journal of Management Inquiry*, vol. 5, no. 2, p. 155, 1996.

[24] 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*, 2005, p. 8.

[25] J. Freudiger, M. Manshaei, J. Hubaux, and D. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 324–337.

[26] D. Jutla and P. Bodorik, "A client-side business model for electronic privacy," in *16th Bled eCommerce Conference and Transformation*, 2003, pp. 463–479.

[27] B. Rao and L. Minakakis, "Evolution of mobile location-based services," *Communications of the ACM*, vol. 46, no. 12, p. 65, 2003.