Privacy Protection Measures and Technologies in Business Organizations:

Aspects and Standards

George O.M. Yee
Aptus Research Solutions Inc., Canada & Carleton University, Canada

Information Science
REFERENCE

Managing Director: Lindsay Johnston
Senior Editorial Director: Heather Probst
Book Production Manager: Sean Woznicki
Development Manager: Joel Gamon
Development Editor: Myla Harty
Acquisitions Editor: Erika Gallagher
Typesetters: Milan Vracarich, Jr.
Print Coordinator: Jamie Snavely
Cover Design: Nick Newcomer, Greg Snader

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Privacy protection measures and technologies in business organizations: aspects and standards / George O.M. Yee and Aptus Research Solutions Inc., editors.
p. cm.
Includes bibliographical references and index.
Summary: “This book is a collection of research on privacy protection technologies and their application in business organizations”--Provided by publisher.
ISBN 978-1-61350-501-4 (hbk.) -- ISBN 978-1-61350-502-1 (ebook) -- ISBN 978-1-61350-503-8 (print & perpetual access) 1. Business--Data processing--Security measures. 2. Computer security. 3. Data protection. 4. Privacy, Right of. I. Yee, George. II. Aptus Research Solutions.
HF5548.37.P755 2012
658.4’78--dc23

2011038433

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 12
A Dynamic Privacy Manager for Compliance in Pervasive Computing

Riccardo Bonazzi
University of Lausanne, Switzerland

Zhan Liu
University of Lausanne, Switzerland

Simon Ganière
Deloitte SA, Switzerland

Yves Pigneur
University of Lausanne, Switzerland

ABSTRACT

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

INTRODUCTION

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

DOI: 10.4018/978-1-61350-501-4.ch012

before looking at how to achieve privacy from a technical point of view.

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

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

Awareness of Changes in the Technology Environment

Technology awareness concerns the understanding of the technological options for privacy management that are offered in a particular moment in time to the user. The link between pervasive computing and user's privacy risk has been addressed by many researchers, mostly in the field of location privacy. In his literature review of computational location privacy Krumm (2009) claims that "location data can be used to infer much about a person, even without a name attached to the data."(p. 4). Most applications focus on controlling access and use of user's data, or they propose security algorithms to protect/obfuscate the communication of data between two users. Krumm (2009) lists a set of solutions for location computational privacy. For example "blurring" is a security algorithm, which ensures a certain degree of location privacy by using inaccurate or at least not so accurate location information, in order to obfuscate the communication of users. Another algorithm is "Access control", which ensures that the sensitive data is only accessed by authorized people, in order to protect user's information privacy.

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

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

Awareness of Changes in the Commerce Environment

A stream of research called economics of security, which Anderson and Blakely's research belongs to, has contributed in adopting economic concepts

like "game theory with incomplete information" and "behavioral economics" into IS risk management (e.g. Acquisti, 2003). Recognizing the importance of privacy management as a business process, and a business support process, the use of a context-awareness application casts privacy management into a business perspective with benefits and costs to either party in a process. This is especially relevant for communications operators as brokers, and for communication channels between content owners (individuals, businesses) and enterprise applications.

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

1. **Actors involved in the game:** Location privacy can be modeled as a non-cooperative game among peers (Freudiger et al., 2009). In this case the *phone user* and her *peers* are identified as two selfish actors while the *attacker* is a third actor, whose goal is to obtain information about the phone user. The phone user and the peers have an interest in cooperating only once they get close enough to each other and can change pseudonyms in order to confuse the attacker. Extending the work of Hong et al. (2005) a fourth actor emerges, i.e. the *service provider*, for example a weather forecaster of the zone where the phone user is located, who wishes to establish a trusted relationship with his potential users (i.e. he does not want to be considered as an attacker). Yet few authors seem to have recognized the importance of the *privacy system designer*, even if his actions affect other actors and although his goals are not necessarily aligned with any of those previously mentioned. One might recall the statement by Palen and Dourish (2003) that privacy is the result of a set of dynamically evolving regulations between actors as their goals and level of trust change. Thus the way the system is designed might constrain the flexibility required by other actors.
2. **Added value of each actor:** Palen and Dourish (2003) clearly identify the need for the *phone user* and her *peers* of a trade-off between the advantages of being visible to the others and the risk of exposure to an *attacker*. In what concerns the *attacker* beside the evident trade-off between the risk of being caught and the advantages of stealing personal data, Anderson (2001) notices how an attacker has fewer resources than the security professionals, but aims at finding only one unknown bug to get an immediate advantage. This issue impacts the *privacy system designer* too, since he might not be the one who pays for the consequences of the theft of private data. This lack of moral hazard could lead to a phenomenon known as "liability dumping". On what concerns the *service provider*, one could expect him to look for the greatest number of potential phone users to reach with the least effort, and this could also be a case where the quest for network externalities (i.e. the search for more users to attract even more users) might be to the detriment of the security of private data. Again there is the possibility that the service provider could decide to act as an infomediary, i.e. an information intermediary (Hagel 3rd and Singer, 1999) that collects data from the *phone users* and the *privacy system designer* and dispatches aggregated data while employing best-practices for privacy management. Such data would be valuable both for the *phone users* and to the *privacy system designer*, and will reduce its value to the *attacker*.

3. **Rules of the game:** On the one hand most authors agree on claiming that regulations concerning privacy management for pervasive technologies are still vague and ambiguous. Citing Massey et al. (2010) "specifying legally compliant requirements is challenging because legal texts are complex and ambiguous by nature" (p.119). This might be due to the hard task that aligning business, technological and legal expertise implies. On the other hand a good example of clear privacy policies that can be understood by humans and machine is the Privacy Preferences Platform as described by Reagle and Cranor (1999) and extended by Hong et al. (2005). On the technological side, many security technological solutions have been proposed and with the increasing computational power of mobile devices the number of offers is expected to grow exponentially. Yet on the business and legal side it is not clear yet how much control should be imposed on the actors involved and how much dynamism should be allowed.
4. **Tactics for the players:** Still to the best of our knowledge no author has dealt with the need of an evolution of the privacy system in the phone of the user, as a response of new ways to sense the environment and to enforce privacy policies. Among the security algorithm proposed for privacy protection Freudiger et al. (2009) have taken into account the problem of user's selfishness in their pseudonym change algorithm, but no attempt to combine different tactics and to select dynamically one that fits best a determined state of the environment has been done yet.
5. **Scope of the game:** Regarding the scope of the interaction between actors, two dimensions come up to our minds. The temporal dimension suggested by Hong et al. (2005) implies that the privacy system needs to evolve. For the data to be retained, while most authors focused on techniques to retain as little data as possible for as little time as needed, a quick consideration on the possible need in the future of data retention for regulatory compliance underlines the need of a middleware to mediate among different requirements. A second dimension to be considered is the geographical analysis, i.e. the size of physical area to be assessed. For sake of simplicity we shall assume it to be a circle, whose radius is 50 meters for the GPS-enabled mobile device and 100 meters for a Wi-Fi enabled mobile device.

Awareness of Changes in the Regulatory Environment

Regulatory awareness concerns the continuous assessment of laws and standards that apply to a determined environment. From the regulatory point of view laws on data privacy are present in different business sectors and in different countries, leading to a complex multitude of overlapping and sometimes conflicting regulations that change over time, as described by Ponemon (2000). This commonly leads to ambiguity and to address that situation a standard privacy policy language, i.e. P3P (Reagle and Cranor, 1999) has been recommended by the World Wide Web Consortium. Although P3P has been criticized for its difficulty of implementation a stream of research has grown around it. Therefore we cite the recent work of Manasdeep et al. (2010), who propose a collaborative model for data privacy and its legal enforcement to support a relationship of confidence between the operating system and the user's data repository. Another approach would be to use the set of metrics derived from privacy regulations, which can be found in Herrmann (2007).

Awareness of Changes in Social Environment

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

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

- **Sure-thing principle**: This was first introduced by the statistician Leonard Jimmy Savage (1954) and it states that a decision maker can rank all options in order of preference and choose the highest one in the ranking.
- **Independence of tastes and beliefs**: this assumption was proposed by the economists Roy Radner and Jacob Marshak (1954) and it states that the decision maker's tastes concerning the outcome of the different options are independent of the options itself, and that her beliefs about the likelihood about the different outcomes are independent of the corresponding outcomes itself. In other words the decision maker is going to assess the outcomes and the likelihood of each option without any bias.
- **Logical and adequate capacity for computing**: from the first two assumptions a third implicit assumption can be derived, i.e. that the agent should be logical and have potentially unlimited capacity of formulation.

Simon (1959) revised the rational decision model and relaxed the third assumption in his bounded rationality model. Indeed the logical approach to decision maker risk aversion does not imply risk neutrality. A rational user can be either risk neutral or risk averse. In the latter case the risk-averse user looks at the worst probable outcome (thereinafter indicated as "wpo") for each option and then chooses the option with the greatest "wpo" among the list. Therefore let us assume that someone has to make a bet on one of two options. Option A can let him win €100 or lose €50, whereas option 2 lets him win €75 or lose €25. If he wants to avoid risk he will rationally bet on the option B, since it has the greater wpo (-€25 is greater than -€50).

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

Radner (2000) has proposed a "truly bounded rationality model" that acknowledges the cost involved in decision making (observation, computation, memory, and communication) and addresses the challenges in ordering the options (inconsistency, ambiguity, and vagueness of the options, unawareness of other options that might rise in the future) using a Bayesian model. But

Figure 1. From the theoretical model to the practical application of the design guidelines

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

even such a model fails to determine the long-term outcomes of each option, making it hard to rank them properly.

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

From the literature review it seems that the user dimension has received little attention from the information system community. Hence we investigate the implications of user awareness for privacy management system design in more detail. In doing so we assume that privacy risk management is a set of actions that the user expects his devices to perform dynamically in response to his perceived environment at a determined moment in time. Our research question arises accordingly:

What are the design characteristics of a privacy management system for an opportunistic and rationally bounded user using a context-aware mobile device?

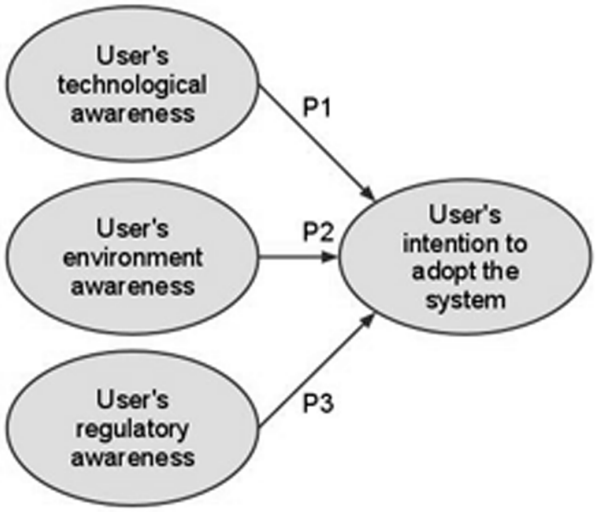
In this study we follow a research design approach using the guidelines of Peffers et al. (2007). Thus the remainder of the paper is structured as follows: we start by briefly summarizing the methodology used in this study. Then we describe the design of our solution and how we came to develop it. After that we present a prototype, which we constructed according to our design and in conclusion we describe and illustrate a first evaluating session we performed with experts in the field.

METHODOLOGY

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

We adopt a design science research methodology and we refer to existing guidelines for design theories (Gregor and Jones, 2007). The theories for design and action "give explicit prescriptions on how to design and develop an artifact, whether it is a technological product or a managerial intervention" (Gregor and Jones 2007, p.233). Therefore we advance in three steps as illustrated in Figure 1.

Figure 2. Our theoretical model



THEORETICAL FRAMEWORK

From the literature review we derive a set of constructs presented in Figure 2.

The first construct is technology awareness, which we define as the possibility for the mobile user to receive updates about the security solutions available on the phone currently used. We suggest measuring this construct using the number of technological updates sent to the user's mobile device.

The second constructs concerns context awareness, which we define as the possibility for the mobile user to receive updates about the privacy risk of the zone where she is currently located. We suggest measuring this construct using the number of sensor updates sent to the user's mobile device.

The third construct is the regulatory awareness, which we define as the possibility for the mobile user to receive updates about the best combination "security solution"-"privacy risk" according to security frameworks and laws. We suggest measuring this construct using the number of rule updates sent to the user's mobile device.

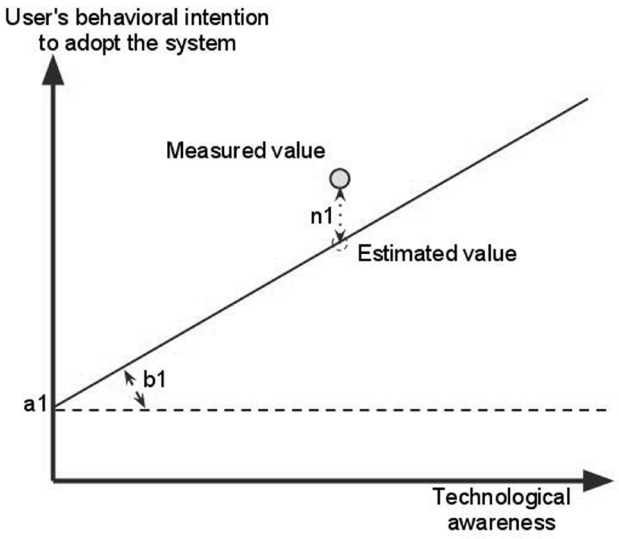
The fourth construct concerns the user's behavioral intention to adopt the system and it is based on the theory of reasoned action of Fishbein and Ajzen (1975), whose explanatory power has been proved in the past by means of two metanalyses conducted by Sheppard et al. (1988).

The technology adoption model of Davis (1989) and its later extension called Unified Theory of Acceptance and Use of Technology of Venkatesh (2003) stated that a user's perceived usefulness increases the user's intention to use the system. User's awareness of the security technologies available supports the realization of user's identity protection. Therefore we claim that a user's behavioral intention to adopt the system follows the user's technological awareness in a linear way, as illustrated by Figure 3. Our first proposition can be expressed by the following formula:

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

Where "a1" is constant that represents the fact that the user would adopt the system even if it does not offer any technological awareness. "a2" is a positive coefficient representing the relationship between the two constructs. "n1" is usually

Figure 3. User's behavioral intention to adopt the system follows the user's technological awareness in a linear way



used in linear regression models to represent the difference between our estimated values and the actual values that are measured in reality. This difference is a consequence of variables that are missing in our equation.

The technology adoption model of Davis (1989) and its later extension called Unified Theory of Acceptance and Use of Technology of Venkatesh (2003) also assess that a user's perceived efficiency increases the user's intention to use the system. User's awareness of the surrounding environment allows him/her to clearly decide what security technology to use and how to reduce waste of energy. We base this claim on the previous analysis of a user's bounded rationality and the consequent need of simplification. Therefore we claim that a user's behavioral intention to adopt the system follows the user's context awareness in a linear way.

Our second proposition can be expressed by the following formula:

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

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

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

User's trust can be towards other people's good intentions or towards the system capacity to protect the user's data. According to this theory a user's awareness of the regulatory environment allows

this person to understand the system's controls to reduce the environmental risk, and that increases the user's trust in the system and her intention to adopt it. We ground this claim on the previous analysis of user's co-opting relationship with the surrounding mobile users and the consequent need for mutual trust. Therefore we claim that a user's behavioral intention to adopt the system follows the user's regulatory awareness in a linear way

Our third proposition can be expressed by the following formula:

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

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

SOLUTIONS AND RECOMMENDATIONS

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

Business Implications of our Model

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

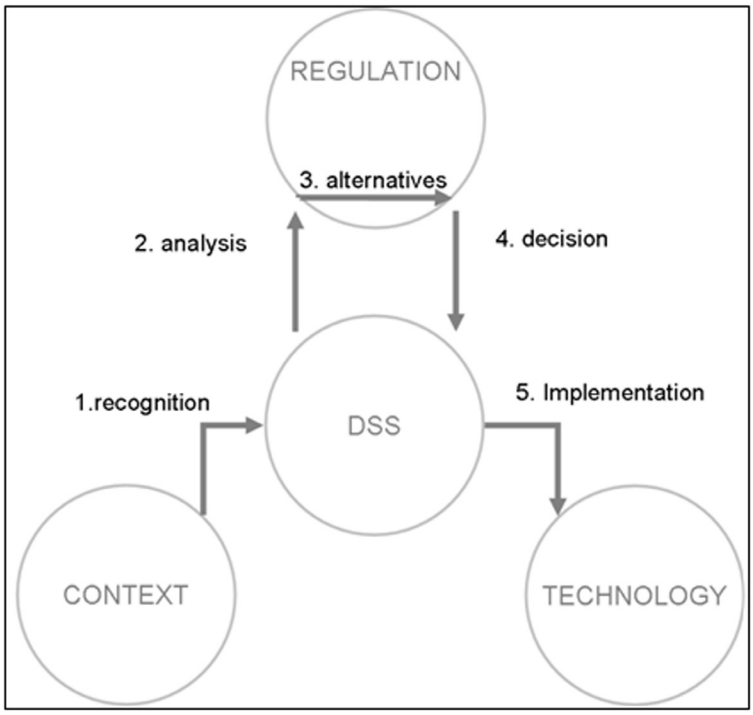
To give more data control ownership to users can lead to new value propositions, which in turn can defferentiate a firm from its competitor. A practical example of a firm that is currently gaining money from allowing the users to fine-tune their privacy preferences is the case Allow Ltd described by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

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

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

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

Figure 4. Information flow to support risk management decisions



Framework

Figure 4 shows the information flows among the four constructs of our framework illustrated in Figure 2.

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

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

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

The third step is the alternatives generation (defined by Straub and Welke, 1998), "the generation of solutions to meet organizational needs specified during risk analysis". A set of regulations might match the context. The profile that has the highest fit is automatically selected.

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

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

Table 1. Operationalization of variables for the scenarios

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

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

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

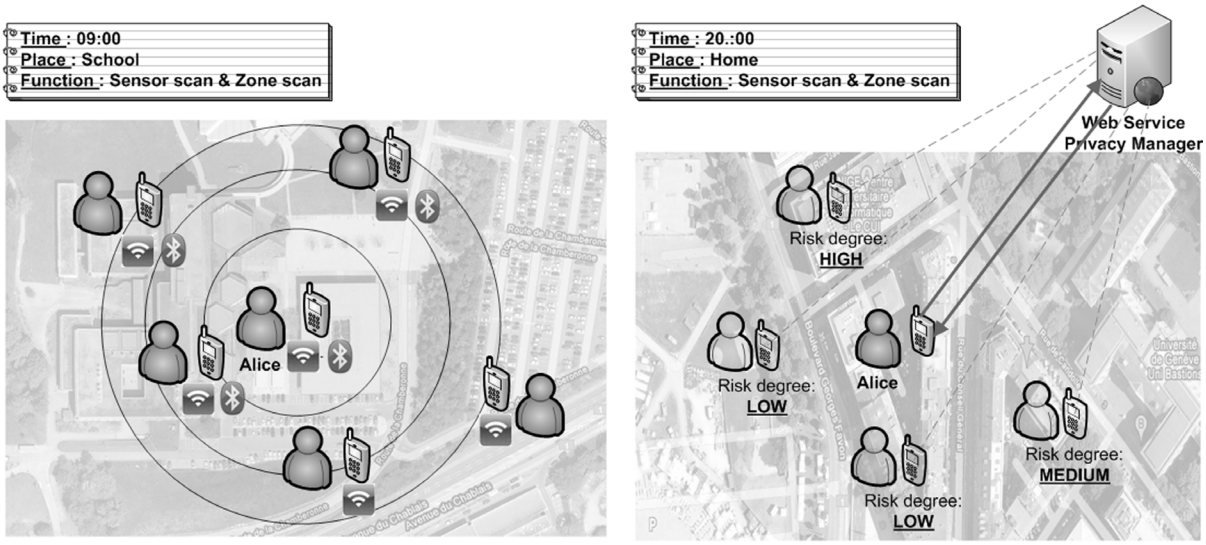
We operationalize the construct of our model, as illustrated in Table 1.We obtain 2^n different scenarios, where n is the number of constructs in our model, and 2 is the value that each construct can get (0=Low or 1=High, see Table 2). For the sake of clarity, we briefly describe each scenario, and we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

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

Table 2. Eight scenarios obtained by combining the three dimensions of our theoretical model

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

Figure 5. The first example (on the left side) and the second example (on the right side)



tion and regulation: information about the available optimal technological configuration to protect the user's privacy is constantly updated from the central system. A set of profiles has to be manually changed. Predefined rules are constantly updated from a central system. A log of the user's previous risk exposure can be seen to let you enable /disable the privacy functionalities. For this scenario, we have found the following application for Android: "MyAndroid protection 2.0". The fifth scenario describes the software that contains the information about the privacy risks of the user's current location and where this information is constantly being updated. For this scenario, we have found the following application for Android: "Glympse". The sixth scenario describes the software that combines the information of context and regulation. For this scenario, we have found the following applications for Android: "Locale", "Setting profiles full" and "Toggle settings". The seventh scenario describes the software that combines the information of context and technological solution. For this scenario, we have found no application for android but web services exists: "General crime", "Homicides" and "Victims". The last scenario includes all of the above three constructs. However, we could not find a corresponding application. Therefore in the rest of the paper we wish to explore the last scenario more in details. We start by illustrating two examples to distinguish the eighth scenario from the other seven, as illustrated by Figure 5.

Example 1: Sensors Analysis for Unknown Environments

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

Table 3. The five steps of risk management decision making in our two examples

	Exemple 1 – Part 1	**Exemple 1 – Part 2**	**Exemple 2 – Part 1**	**Exemple 2 – Part 2**
Step 1. recognition	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data.	Wi-Fi and Bluetooth sensor data. Zone information from infomediary
Step 2. analysis	Many connections	Few connections	Many connections	Many connections. Risky zone.
Step 3. alternatives	"Medium" profile is ranked as first, "Low" profile is ranked as second	"Low" profile is ranked as first, "Medium" profile is ranked as second	"Medium" profile is ranked as first, "Low" profile is ranked as second	"Medium" profile is ranked as first, "Low" profile is ranked as second
Step 4. decision	"Medium" profile is automatically chosen. "Blurring" and "access control" algorithms are chosen to obfuscate the user's position and to protect user's data	"Low" profile is automatically chosen. "Access control" algorithm is chosen.	None profile is imposed by the user. No security algorithm is chosen.	"Medium" profile is automatically chosen. "Blurring" and "access control" algorithms are chosen to obfuscate the user's position and to protect user's data
Step 5. implementation	"Blurring" and "Access control" are executed	"Access control" is executed	No security algorithm is executed	"Blurring" and "Access control" are executed

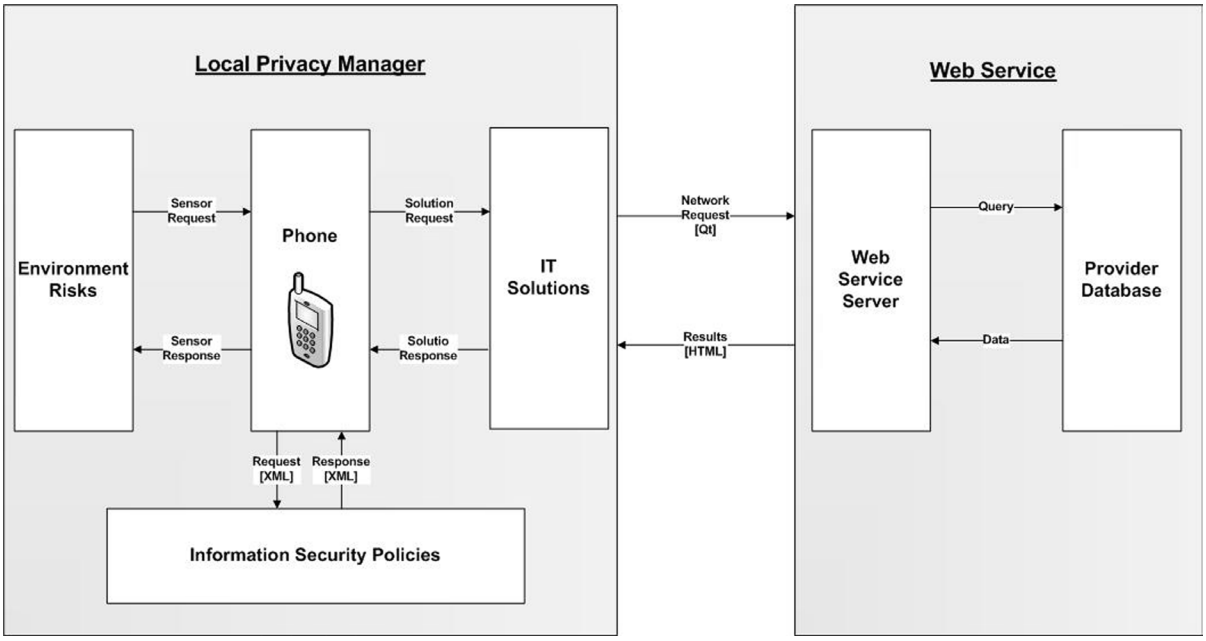
buys a book when she is in the university. "Privacy Manager" detects that there are many unknown connections around her current position. "Privacy Manager" reports it and adopts two technological solutions (blurring and access control) to protect her online purchasing. After lunch, Alice goes for a walk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

Example 2: Aggregated Historical Data for Known Environments

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

Table 3 links the two examples to the data flow for decision support presented in figure 4. As previously said the security algorithms have already been implemented with success in mobile applications. Therefore we shall present a prototype that illustrates how to enforce a set of security profile according to contextual privacy risk, which is assessed by means of data sensors collection and zone risk updates sent by a trusted third party.

Figure 6. System architecture



IMPLEMENTATION

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

System Architecture

Figure 6 shows the local privacy manager's interaction with the components of the privacy architecture and the web service.

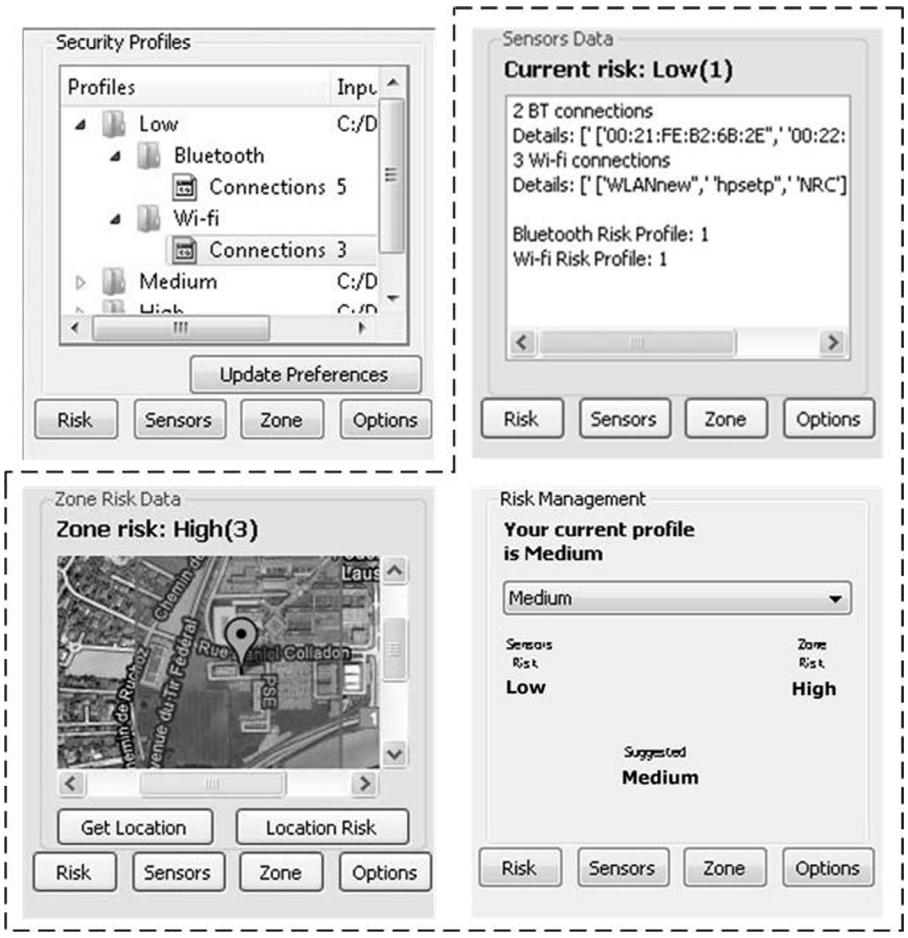
For the configuration of a user's located privacy policies, we use a XML file to store user's preferences on the phone. It allows the user to edit, create and delete their privacy policies at any time. Detecting the risk of environment is done by using the python socket architecture (Python Software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

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

Implementation Details

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

Figure 7. The Graphic User Interfaces: Configuration interfaces (top left corner); Sensor analysis interfaces (top right corner); Zone risk analysis interfaces (bottom left corner); Risk management interface (bottom right corner)



the web-enabled application can be written and deployed across embedded operating systems.

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

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

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

Graphical User Interface

The designed application aims at a clear layout and a high degree of user friendliness. For a complete review of the graphical user interface, in Figure 7, we focus on the design of the activity, information and interaction. For the user who is a first time user of this application, a welcome page is proposed and used for the configuration

of privacy policies, which explains the purpose and the content of the local risk degree, and its proposed privacy policies on related risk. From this starting page, the user has the option to define the degree of attack for each phone's technology, for example the Bluetooth, Wi-Fi, GPRS and so on. Privacy policies are represented by a list that contains a large related security application which could be selected by the user to enforce the rule that fits the current risk degree. All the information about the status change is stored in a file for future use of compliance checking against privacy policies. If a technology or related security application is not listed in the privacy policies list, users can create a new one at any time. Once the local privacy policies are configured by the user, then the 3 main functions of application of the privacy manager are available for use.

Recalling Table 3 we illustrate how to implement the five steps of the decision support for privacy risk management. The first function offers a physical sensor that continuously collects diverse information from the environment. It keeps detecting context information of the technologies of different devices around the user, in order to get an updated context degree of risk in real time, including the technology's name, its MAC address and the specific identification, as well as the number of connections for each technology. In addition, each technology's risk profile is calculated automatically to conform to the user's risk degree configuration. The information of ranking, which represents the average of current risk between all of the technologies detected— is presented at the bottom of the screen.

The second function shows the information about zone risk, which includes 2 tasks: displaying the user's current position and obtaining this position's historical risk.

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

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

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

Focusing on a zone's risk data sharing, the second button named "location risk" which is set up to allow the phone to contact our online web service to send the information regarding the user's current located risk data to the Web Service Server This web server provides interface to users who authorize to access the application. A database is used to store all information about user's risk. Then the web server will return to

the users a risk level which is calculated by the average in a similar area in real time (i.e. each 10 minutes). And here the similar area is defined as a specified area, which is a circumference of a circle with its radius of 500 meters. Finally, the web service will deliver in return the average of the risk degree reported by others users in the same geographic area in an earlier period of time. In order to distinguish the degree of risk in a specific area, an alarm system is integrated, and by using different colors on the map to signify the degree of risk, for example, blue signifies low risk in this area and red signifies high risk.

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

DISCUSSION

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

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

FUTURE RESEARCH DIRECTIONS

In the close future we are going to improve the prototype using the outcome of our preliminary test before testing it on a larger scale using the guidelines illustrated in Table 4. Yet we believe that by now our proposed design makes a contribution since it is a first attempt at empowering the user with a system that allows him to manage the dynamically privacy risk according to his own preference and perceptions. Future research

Table 4. Testing guidelines

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

directions that we envisage from our work are the following ones:

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

CONCLUSION

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

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

REFERENCES

Acquisti, A., Dingledine, R., & Syverson, P. (2003). On the economics of anonymity. In Wright, R. N. (Ed.), *Financial cryptography, LNCS 2742*. Springer-Verlag. doi:10.1007/978-3-540-45126-6_7

Anderson, R. (2001). Why information security is hard-an economic perspective. In *Proceedings 17th Annual Computer Security Applications Conference, 2001* (pp. 358-365). New Orleans, LA: IEEE.

Angwin, J., & Steel, E. (2011). *Web's hot new commodity: Privacy*. Retrieved March 15, 2011, from http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html

Barkhuus, L. (2004). Privacy in location-based services, concern vs. coolness. In *Proceedings of Workshop paper in Mobile HCI 2004 workshop: Location System Privacy and Control*. Glasgow, UK.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 Workshop on New Security Paradigms*. Cloudcroft, New Mexico.

Bonazzi, R., Fritscher, B., & Pigneur, Y. (2010, October). Business model considerations for privacy protection in a mobile location based context. *Proceedings of the Second International Workshop on Business Models for Mobile Platforms IEEE*. Retrieved March 15, 2011, from http://people.hec.unil.ch/ypigneur/files/2010/08/10_bmmp.pdf

Capra, L., Emmerich, W., & Mascolo, C. (2003). CARISMA: Context-aware reflective middleware system for mobile applications. *IEEE Transactions on Software Engineering*, *29*(10), 929–945. doi:10.1109/TSE.2003.1237173

Chen, G., & Kotz, D. (2000). *A survey of context-aware mobile computing research*. Tech. Rep. TR2000-381, Dartmouth, November 2000.

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, *7*(2), 165–181. doi:10.1016/j.elerap.2007.02.001

Das, T. K., & Teng, B. S. (2000). A resource-based theory of strategic alliances. *Journal of Management*, *26*(1), 31–61.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly*, *13*(3), 319–340. doi:10.2307/249008

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley Pub.

Freudiger, J., Manshaei, M., Hubaux, J. P., & Parkes, D. C. (2009). On non-cooperative location privacy: A game-theoretic analysis. In *Proceedings of ACM Conference on Computer and Communications Security (CCS),* Chicago, USA.

Gallivan, M. J., & Depledge, G. (2003). Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, *13*(2), 159–190. doi:10.1046/j.1365-2575.2003.00146.x

Google Inc. (2010). *Google Maps API - Geocoding*. Retrieved March 15, 2011, from http://code.google.com/apis/maps/documentation/services.html#Geocoding

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, *8*(5), 312–325.

Hagel, J. III, & Singer, M. (1999). *Net worth* (1st ed.). Harvard Business Press.

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI* (1st ed.). Auerbach Publications. doi:10.1201/9781420013283

Hong, D., Yuan, M., & Shen, V. Y. (2005). Dynamic privacy management: A plug-in service for the middleware in pervasive computing. In *Proceedings of the 7th International Conference on Human Computer Interaction with Mobile Devices & Services*. Salzburg, Austria.

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, *13*(6), 391–399. doi:10.1007/s00779-008-0212-5

Manasdeep, A. S., Jolly, D. S., Singh, A. K., Srivastava, M. A., & Singh, M. S. (2010). A proposed model for data privacy providing legal protection by e-court. *International Journal of Engineering Science and Technology*, *2*(4), 649–657.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. doi:10.1016/0167-9236(94)00041-2

Massey, A. K., Otto, P. N., Hayward, L. J., & Antón, A. I. (2009). Evaluating existing security and privacy requirements for legal compliance. *Requirements Engineering*, *15*(1), 119–137. doi:10.1007/s00766-009-0089-5

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192–222. doi:10.1287/isre.2.3.192

Nalebuff, B., & Brandenburger, A. (1997). Co-opetition: Competitive and cooperative business strategies for the digital economy. *Strategy and Leadership*, *25*(6), 28–35. doi:10.1108/eb054655

Oxford English Dictionary. (2010.). *Privacy*. Retrieved March 15, 2011, from http://www.askoxford.com

Palen, L., & Dourish, P. (2003). Unpacking privacy for a networked world. In *Proceedings of the ACM Special Interest Group on Computer-Human Interaction (SIGCHI) Conference on Human Factors in Computing Systems*, Florida, USA.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. doi:10.2753/MIS0742-1222240302

Ponemon, L. (2000). *Privacy risk management*. Long Beach, CA, USA: Presentation for The National Council of Higher Education Loan Programs.

Porter, M. E. (1998). *Competitive strategy: Techniques for analyzing industries and competitors* (1st ed.). Free Press.

Python Software Foundation. (2010). *Socket — Low-level networking interface — Python v2.6.4 documentation*. Retrieved March 15, 2011, from http://docs.python.org/library/socket.html

Radner, R. (2000). Costly and bounded rationality in individual and team decision-making. *Industrial and Corporate Change*, *9*(4), 623–655. doi:10.1093/icc/9.4.623

Radner, R., & Marschak, J. (1954). Note on some proposed decision criteria. In Thrall, R. M. (Eds.), *Decision processes*. John Wiley.

Reagle, J., & Cranor, L. F. (1999). The platform for privacy preferences. *Communications of the ACM*, *42*(2), 55. doi:10.1145/293411.293455

Rosson, M. B., & Carroll, J. M. (2002). *Usability engineering: Scenario-based development of human-computer interaction*. Morgan Kaufmann Pub.

Savage, L. J. (1954). *The foundations of statistics* (2nd ed.). New York, NY: Wiley.

Schilit, B., Adams, N., Want, R., et al. (1994). Context-aware computing applications. In *Proceedings of the Workshop on Mobile Computing Systems and Application.* Santa Cruz, CA, (pp. 85–90).

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010). Google Android: A comprehensive security assessment. *IEEE Security & Privacy*, *8*(2), 35–44. doi:10.1109/MSP.2010.2

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *The Journal of Consumer Research*, *15*(3), 325–343. doi:10.1086/209170

Shokri, R., Freudiger, J., Jadliwala, M., & Hubaux, J. P. (2009). A distortion-based metric for location privacy. In *Proceedings of WPES'09, ACM Workshop on Privacy in the Electronic Society* (WPES), Chicago, IL, USA.

Simon, H. A. (1959). Theories of decision-making in economics and behavioral science. *The American Economic Review*, *49*(3), 253–283.

Simon, H. A. (1987). Bounded rationality. In Eatwell, J. (Eds.), *The New Palgrave*. London, UK: Maemillan.

Straub, D., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quart.*, *22*(4), 441–469. doi:10.2307/249551

Thompson, J. D. (1967). *Organizations in action: Social science bases of administrative theory*. McGraw-Hill Companies.

Tversky, A., & Kahncman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *28*(5), 1124–1134. doi:10.1126/science.185.4157.1124

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of Information Technology: Toward a unified view. *Management Information Systems Quarterly*, *27*(3), 425–478.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly*, *26*(2), xiii–xxiii.

ADDITIONAL READING

Abowd, G. D., Atkeson, C. G., Hong, J., Long, S., Kooper, R., & Pinkerton, M. (1997). Cyberguide: a mobile context-aware tour guide. *Wireless Networks*, *3*(5), 421–433. doi:10.1023/A:1019194325861

Acquisti, A., Dingledine, R., & Syverson, P. (2003). On the economics of anonymity. In Wright, R. N. (Ed.), *Financial Cryptography. Springer-Verlag, LNCS 2742*.

Anderson, R. (2001). Why information security is hard-an economic perspective. In *Proceedings 17th Annual Computer Security Applications Conference, 2001.* (pp. 358-365). Presented at the ACSAC 2001, New Orleans, Louisiana: IEEE.

Barkhuus, L. (2004). Privacy in Location-Based Services, Concern vs. Coolness. In *Proceedings of Workshop paper in Mobile HCI 2004 workshop: Location System Privacy and Control*. Glasgow.

Biegel, G., & Cahill, V. (2004) 'A framework for developing mobile, context-aware applications', *Proceedings of the 2nd IEEE Conference on Pervasive Computing and Communication*, pp.361–365.

Burrell, J. and Gay, G. (2002) 'E-graffiti: evaluating real-world use of a context-aware system', *Interacting with Computers – Special Issue on Universal Usability*, Vol. 14, No. 4, pp.301–312.

Capra, L., Emmerich, W., & Mascolo, C. (2003). CARISMA: Context-aware reflective middleware system for mobile applications. *IEEE Transactions on Software Engineering*, *29*(10), 929–945. doi:10.1109/TSE.2003.1237173

Chen, G., & Kotz, D. (2000). *A survey of context-aware mobile computing research*.

Chen, H., Finin, T., & Joshi, A. (2003). *'An ontology for context-aware pervasive computing environments', The Knowledge Engineering Review* (*Vol. 18*, pp. 197–207). Cambridge University Press.

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, *7*(2), 165–181. doi:10.1016/j.elerap.2007.02.001

Fahy, P., & Clarke, S. (2004) 'CASS – a middleware for mobile context-aware applications', *Workshop on Context Awareness*, MobiSys 2004.

Freudiger, J., Manshaei, M., Hubaux, J. P., & Parkes, D. C. (2009). On Non-Cooperative Location Privacy: A Game-Theoretic Analysis. In *Proceedings of ACM Conference on Computer and Communications Security (CCS)*.

Gu, T., Pung, H. K., & Zhang, D. Q. (2004a) 'A middleware for building context-aware mobile services', *Proceedings of IEEE Vehicular Technology Conference (VTC),* Milan, Italy.

Harter, A., Hopper, A., Steggles, P., Ward, A., & Webster, P. (2002). The anatomy of a context-aware application. *Wireless Networks*, *8*(2–3), 187–197. doi:10.1023/A:1013767926256

Hofer, T., Schwinger, W., Pichler, M., Leonhartsberger, G., & Altmann, J. (2002) 'Context-awareness on mobile devices – the hydrogen approach', *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, pp.292–302.

Hong, D., Yuan, M., & Shen, V. Y. (2005). Dynamic privacy management: a plug-in service for the middleware in pervasive computing (p. 8).

Indulska, J., & Sutton, P. (2003) 'Location management in pervasive systems', CRPITS'03: *Proceedings of the Australasian Information Security Workshop*, pp.143–151.

Korpipää, P., & Mäntyjärvi, J. (2003) 'An ontology for mobile device sensor-based context awareness', *Proceedings of CONTEXT*, 2003, Vol. 2680 of Lecture Notes in Computer Science, pp.451–458.

Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, *13*(6), 391–399. doi:10.1007/s00779-008-0212-5

Palen, L., & Dourish, P. (2003). Unpacking privacy for a networked world. In *Proceedings of the ACM Special Interest Group on Computer-Human Interaction (SIGCHI) conference on Human factors in computing systems* (p. 136). Presented at the Conference on Human Factors in Computing Systems, Florida,USA.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. doi:10.2753/MIS0742-1222240302

Ponemon, L. (2000, June 7). *Privacy Risk Management. Presentation for The National Council of Higher Education Loan Programs*. Presented at the NCHELP Convention, Long Beach, CA, USA.

Rosson, M. B., & Carroll, J. M. (2002). *Usability engineering: scenario-based development of human-computer interaction*. Morgan Kaufmann Pub.

Salber, D., Dey, A. K., & Abowd, G. D. (1999) 'The context toolkit: aiding the development of context-aware applications', *Proceedings of the ACM CHI*, Pittsburgh, PA, pp.434–441.

Schilit, B., Adams, N., Want, R., & Associates. (1994). Context-aware computing applications. In *Proceedings of the workshop on mobile computing systems and applications* (pp. 85–90).

Shokri, R., Freudiger, J., Jadliwala, M., & Hubaux, J. P. (2009). A Distortion-Based Metric for Location Privacy. In *Proceedings of WPES'09*. Presented at the ACM Workshop on Privacy in the Electronic Society (WPES), Chicago, IL; USA.

Straub, D., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quart.*, *22*(4), 441–469. doi:10.2307/249551

KEY TERMS AND DEFINITIONS

Bounded Rationality: A rational approach to decision, taking into consideration the player's biases and cognitive limitations.

Context-Aware Technologies: A set of technical solutions that can sense the change in the environment and adapt accordingly.

Contingency Theory: A class of behavioral theory that claims that the optimal course of action is contingent (dependent) upon both the internal and external situations. Such theory postulates that impacts of environmental factors are systemic (=part of the system), rather than entirely situational.

Infomediary: an information intermediary that gathers data and dispatch aggregated analyses.

Middleware: A software layer that situates between the application and the network to provide powerful abstractions and mechanisms that relieve programmers from dealing with low-level details that can change in time.

Opportunism: The agent's act of optimizing the personal payoff, no matter what occurs to other agents.

Privacy: a state in which one is not observed or disturbed by others.

Privacy Risk Management: the identification, assessment, and prioritization of risks caused by the collection and dissemination of user's data.

Risk Aversion: A concept based on human behavior, according to which an agent tries to minimize its loss chance.

Regulatory Awareness: The continuous assessment of laws and standards that apply to a determined/defined environment.