Asia Pacific Journal of Information Systems
Vol. 20, No. 2, June 2010

Information Privacy Concern in Context-Aware Personalized Services: Results of a Delphi Study*

Yonnim Lee**, Ohbyung Kwon**

Personalized services directly and indirectly acquire personal data, in part, to provide customers with higher-value services that are specifically context-relevant (such as place and time). Information technologies continue to mature and develop, providing greatly improved performance. Sensory networks and intelligent software can now obtain context data, and that is the cornerstone for providing personalized, context-specific services. Yet, the danger of overflowing personal information is increasing because the data retrieved by the sensors usually contains privacy information. Various technical characteristics of context-aware applications have more troubling implications for information privacy.

In parallel with increasing use of context for service personalization, information privacy concerns have also increased such as an unrestricted availability of context information. Those privacy concerns are consistently regarded as a critical issue facing context-aware personalized service success. The entire field of information privacy is growing as an important area of research, with many new definitions and terminologies, because of a need for a better understanding of information privacy concepts. Especially, it requires that the factors of information privacy should be revised according to the characteristics of new technologies.

However, previous information privacy factors of context-aware applications have at least two shortcomings. First, there has been little overview of the technology characteristics of context-aware computing. Existing studies have only focused on a small subset of the technical characteristics of context-aware computing. Therefore, there has not been a mutually exclusive set of factors that uniquely and completely describe information privacy on context-aware applications. Second, user survey has been widely used to identify factors of information privacy in most studies despite the limitation of users' knowledge and experiences about context-aware computing technology. To date, since context-aware services have not been widely deployed on a commercial scale yet, only very few people have prior experiences with context-aware person-

* This work was supported by Mid-career Researcher Program through NRF grant funded by the MEST (R01-2008-000-20696-0).

** College of Business, Kyung Hee University

alized services. It is difficult to build users' knowledge about context-aware technology even by increasing their understanding in various ways: scenarios, pictures, flash animation, etc. Nevertheless, conducting a survey, assuming that the participants have sufficient experience or understanding about the technologies shown in the survey, may not be absolutely valid. Moreover, some surveys are based solely on simplifying and hence unrealistic assumptions (e.g., they only consider location information as a context data).

A better understanding of information privacy concern in context-aware personalized services is highly needed. Hence, the purpose of this paper is to identify a generic set of factors for elemental information privacy concern in context-aware personalized services and to develop a rank-order list of information privacy concern factors. We consider overall technology characteristics to establish a mutually exclusive set of factors.

A Delphi survey, a rigorous data collection method, was deployed to obtain a reliable opinion from the experts and to produce a rank-order list. It, therefore, lends itself well to obtaining a set of universal factors of information privacy concern and its priority. An international panel of researchers and practitioners who have the expertise in privacy and context-aware system fields were involved in our research.

Delphi rounds formatting will faithfully follow the procedure for the Delphi study proposed by Okoli and Pawlowski. This will involve three general rounds: (1) brainstorming for important factors; (2) narrowing down the original list to the most important ones; and (3) ranking the list of important factors. For this round only, experts were treated as individuals, not panels. Adapted from Okoli and Pawlowski, we outlined the process of administrating the study. We performed three rounds. In the first and second rounds of the Delphi questionnaire, we gathered a set of exclusive factors for information privacy concern in context-aware personalized services. The respondents were asked to provide at least five main factors for the most appropriate understanding of the information privacy concern in the first round. To do so, some of the main factors found in the literature were presented to the participants. The second round of the questionnaire discussed the main factor provided in the first round, fleshed out with relevant sub-factors. Respondents were then requested to evaluate each sub factor's suitability against the corresponding main factors to determine the final sub-factors from the candidate factors. The sub-factors were found from the literature survey. Final factors selected by over 50% of experts. In the third round, a list of factors with corresponding questions was provided, and the respondents were requested to assess the importance of each main factor and its corresponding sub factors. Finally, we calculated the mean rank of each item to make a final result.

While analyzing the data, we focused on group consensus rather than individual insistence. To do so, a concordance analysis, which measures the consistency of the experts' responses over successive rounds of the Delphi, was adopted during the survey process.

As a result, experts reported that context data collection and high identifiable level of identical data are the most important factor in the main factors and sub factors, respectively. Additional important sub-factors included diverse types of context data collected, tracking and recording functionalities, and embedded and disappeared sensor devices. The average score of each factor is very useful for future context-aware personalized service development in the view of the information privacy.

The final factors have the following differences comparing to those proposed in other studies. First, the concern factors differ from existing studies, which are based on privacy issues that may occur during the lifecycle of acquired user information. However, our study helped to clarify these sometimes vague issues by determining which privacy concern issues are viable based on specific technical characteristics in context-aware personalized services. Since a context-aware service differs in its technical characteristics compared to other services, we selected specific characteristics that had a higher potential to increase user's privacy concerns. Secondly, this study considered privacy issues in terms of service delivery and display that were almost overlooked in existing studies by introducing IPOS as the factor division. Lastly, in each factor, it correlated the level of importance with professionals' opinions as to what extent users have privacy concerns. The reason that it did not select the traditional method questionnaire at that time is that context-aware personalized service considered the absolute lack in understanding and experience of users with new technology.

For understanding users' privacy concerns, professionals in the Delphi questionnaire process selected context data collection, tracking and recording, and sensory network as the most important factors among technological characteristics of context-aware personalized services. In the creation of a context-aware personalized services, this study demonstrates the importance and relevance of determining an optimal methodology, and which technologies and in what sequence are needed, to acquire what types of users' context information. Most studies focus on which services and systems should be provided and developed by utilizing context information on the supposition, along with the development of context-aware technology. However, the results in this study show that, in terms of users' privacy, it is necessary to pay greater attention to the activities that acquire context information. To inspect the results in the evaluation of sub factor, additional studies would be necessary for approaches on reducing users' privacy concerns toward technological characteristics such as highly identifiable level of identical data, diverse types of context data collected, tracking and recording functionality, embedded and disappearing sensor devices. The factor ranked the next highest level of importance after input is a context-aware service delivery that is related to output. The results show that delivery and display showing services to users in a context-aware personalized services toward the anywhere-anytime-any device concept have been regarded as even more important than in previous computing environment.

Considering the concern factors to develop context aware personalized services will help to increase service success rate and hopefully user acceptance for those services. Our future work will be to adopt these factors for qualifying context aware service development projects such as u-city development projects in terms of service quality and hence user acceptance.

Keywords : Information Privacy, Privacy Concern, Context-aware Computing

I. Introduction

Personalized service has received considerable attention [Mobasher, Cooley and Srivastava, 2000; Herlocker and Konstan, 2001] recently because of different service needs among users. Personalized services directly and indirectly acquire personal data, in part, to provide customers with higher-value services that are specifically context-relevant (such as place and time). Since various kinds of context information are flowing in context-aware computing environments with a wide range of networking, computing, and distributed contents and services, among those kinds of contexts, user-related context information is required to provide personalized services. Recent studies have made a great attempt to develop frameworks describing and utilizing various kinds of user-related context information to support personalized services.

However, in parallel with increasing use of context information for service personalization, information privacy concerns have also increased such as an unrestricted availability of context information. Those concerns are consistently regarded as a critical issue facing context-aware personalized service success [Jiang and Landay, 2002; Shoji and Nakajima, 2004; Kang and Bang, 2006]. Interest in information privacy rose sharply in the late 1980's due to increased database marketing and telemarketing. With advances in information technology, there is a continued, growing concern about how much individuals are able to protect their personal information, which is reflected in the information systems literature on [Beresford and Stajano, 2003; Nissenbaum, 1998]. The entire field of information privacy is growing as an important area of research, with many new definitions and terminologies, because of a need for a better understanding of information privacy concepts. Especially, it requires that the factors of information privacy should be revised according to the characteristics of new technologies.

Since context-aware computing technology certainly poses a set of new privacy challenges, issues that have not been previously considered, information privacy issues are getting attention especially on context-aware applications [Ackerman *et al.*, 2001]. Moreover, Gartner, Inc., which is the most famous information technology research and advisory firm, reports that context-aware computing will provide significant competitive advantage because enterprises can leverage context-aware computing to better target prospects, increase customer intimacy, and enhance associate productivity and collaboration. However, to introduce context-aware computing successfully, garter emphasizes that trust and privacy issues have to be addressed [Lapkin, 2009]. Prior studies have indicated that various technical characteristics of context-aware computing have raised serious privacy concerns: the collection of information from various sensors, the invisible form factor of embedded computing devices, an automatically collected computational context, push-type dissemination, sensitive context data acquisition and display, tracking of whereabouts, etc. [Cheverst *et al.*, 2002; Neustaedter and Greenberg, 2003; Cas, 2005; Junglas and Spitzmuller, 2005; Floridi, 2006; Dritsas *et al.*, 2006; Nguyen *et al.*, 2008]. One specific example includes deeply embedded sensors and

sensor networks, key parts of context-aware systems, which are specifically designed to transparently collect and use private information. Sensitive private information can live indefinitely and appear anywhere at anytime. The danger of overflowing personal information is increasing because the data retrieved by the sensors usually contains privacy information. Here is one more example. In an audio/video captured environment, which is a representative characteristic of context-aware computing, three independent privacy issues exist [Adams, 2000]. First issue is an information recipient. It is the user's concern of the person (not necessarily the actual person) who receives and/or manipulates his data. Second issue is an intended usage of the information. It is related to the user's concern of how and what his transmitted data is used for during the exchange and at a later date. Third issue is associated with context in which the information disclosure occurs. It relates to the effect on the user's acceptability to release information in different types of context. When context changes, the user may or may not be willing to release certain types of privacy related information. Like this, various technical characteristics of context-aware applications have more troubling implications for information privacy.

However, previous information privacy factors of context-aware applications have at least two shortcomings. First, there has been little overview of the technology characteristics of context-aware computing. Second, user survey has been widely used to identify factors of information privacy in most studies despite the limitation of users' knowledge and experiences about context-aware computing technology. To overcome these shortcomings, we considered the overall technology characteristics of context-aware computing to identify a generic set of factors of information privacy in context-aware applications. We also invited experts, not general users, who have a detailed knowledge of both context-aware computing technology and privacy issues, to take part in the factor identification process. To obtain the most reliable consensus of expert opinion, we adopted the Delphi method. Three rounds of Delphi surveys were conducted. The iterations of the Delphi exercise allowed the experts to refine concern factors in a very reasonable manner and decide their weighting of the factors beyond their own subjective opinions.

The aim of this paper is to identify a generic set of factors for elemental information privacy concern in context-aware personalized services and to develop a rank-order list of information privacy concern factors. Additionally, we showed how the Delphi technique was used, first, to generate a list of concern factors and then second, to derive a consensus on weighting of the factors. Through the Delphi method, we found that the newly identified factors were ranked as more important than traditional factors, such as processing and service delivery factors. This implies that earlier efforts for applying traditional factor to understand information privacy concern for context aware personalized services may need to be refocused.

The remainder of the paper is organized as follows. Section 2 reviews related works on information privacy. Section 3 describes research methods. Section 4 presents and discusses the results, and Section 5 concludes the paper with a discussion of the implications of this paper

and future research issues.

Ⅱ. Research Background

2.1 Information privacy

Information privacy was initially defined by Westin [1967] as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [Westine, 1967]. Stone, *et al.* defined information privacy as "the ability of the individual to personally control information about one's self" [Stone, *et al.*, 1983]. Clarke [1999] also defined information privacy as being a combination of personal communication privacy and personal data privacy [Clarke, 1999]. His formal definition of information privacy is "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves."

In identifying the concern factors for information privacy, Smith and Milberg designed the first set of factors for information privacy concerns in 1996 [Smith and Milberg, 1996]. They called it the Concern for Information Privacy (CFIP) and it extracted individuals' concern factors regarding organizational practices. It identified four factors as the dimensions of an individual's concern for privacy: collection, errors, secondary use, and unauthorized access to information. It described user concerns in terms of losing the ability to control the collection, handling, and use of personal information. Several studies have subsequently attempted to identify privacy concerns in more detail and to identify different types of privacy concern. <Table 1> lists various factors proposed in those studies.

Although researchers have suggested various factors in different environment to understand users' information privacy, little work has been done regarding emerging technology such as context-aware computing. Information privacy issues have remained at the forefront of user concern in today's context-aware computing environments such as context-aware personalized services. Restate, a renewal of the factor set of information privacy especially for this field is needed. This paper focuses on information privacy in context-aware personalized service.

2.2 Privacy Issues in Context-aware Services

Our generation has moved toward context-aware service applications because it offers the promise of significant user gains: the ability for systems to adapt themselves more readily to user needs, models and goals. However, according to the recent studies, the dangers of unsecured context information are increasing and worries about existing privacy problems only worsen in context-aware applications. Privacy concern issues have recently received increased attention in context-aware service application literatures.

Studies about privacy concern in context-aware service applications can be categorized into two types: designing a privacy preserving application and identifying new privacy-related considerations. Jiang *et al.* [2002] proposed a framework for supporting socially compatible privacy objectives in context-aware com-

<Table 1> Various Factors for Measuring Information Privacy

Source	Factor	Description
Westin, 1967	Amount of control	Individuals can exert over the type of information, and the extent of that information, revealed to others.
Smith and Milberg, 1996	Collection of personal information	Concern that extensive amounts of personally identifiable data are being collected and stored in a database.
	Unauthorized Secondary Use of personal information	Concern that information is collected from individuals for one purpose but is used for another, secondary purpose without authorization from the individuals/secondary purpose after disclosure to an external party.
	Improper Access to personal information	Concern that data about individuals are readily available to people not properly authorized to view or work with this data.
	Errors in personal information	Concern that protections against deliberate and accidental errors in personal data are inadequate.
Nowak and Phelps, 1997	Surreptitious use	Marketers can appropriate consumer information surreptitiously or without giving consumers control over its use.
	Disclose and misuse	Marketers can disclose embarrassing facts about consumers or make use of false or inaccurate information.
Wang *et al.*, 1998	Improper acquisition	Improper access, improper collection, improper monitoring.
	Improper use	Improper analysis, improper transfer.
	Privacy invasion	Unwanted solicitation.
	Improper storage	Improper storage of personal information.
Hoffman *et al.*, 1999	Environmental control	The consumer's ability to control the actions of other people in the environment during a market transaction or commercially oriented exchange.
	Secondary use of information control	The consumer's ability to control the dissemination of information related to or provided during such transaction or behaviours to those who were not present.
Malhotra *et al.*, 2004	Collection	The degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received.
	Control	An individual's concerns for whether the individual has control over personal information as manifested by the existence of voice or exit.
	Awareness of Privacy Practices	The degree to which a consumer is concerned about his/her awareness of organizational information privacy practices.
Kuo *et al.*, 2007	Protection	It refers to whether an individual can take the necessary courses of action for guarding accidental disclosures of information in a public environment.
	Non-distribution	It refers to whether a person can exert his or her control not to distribute the privacy information of others.
	Non-acquisition	It refers to whether a person has the self-confidence to refuse to acquire and use privacy information before he or she obtains the necessary authorization or permission to do so.

puting settings, and designed an application that effectively supports varying degrees of asymmetry [Jiang *et al.*, 2002]. Myles *et al.* [2003] designed privacy-preserving location sensing applications to address privacy concerns. Gandon and Sadeh [2004] designed the integration of access control mechanisms into pervasive computing infrastructure. Beresford and Stajano [2003] concentrated on location privacy, a particular type of information privacy, and developed a privacy-protecting framework based on frequently changing pseudonyms that address the fact that users avoid being identified by their current locations. They proposed a context modeling approach that addresses the challenges of assigning ownership to context information and enables users to express privacy preferences for their own information.

Other studies identify new privacy-related considerations. Jiang and Landay [2002] proposed a theoretical model for privacy control in a context aware service application. Shoji and Nakajima [2004] addressed the trade-offs between privacy and the quality of services and proposed a prototype system that controls the trade-off according to a user's requirements. Eymann and Morito [2005] proposed privacy issues of combining context-aware computing and software agent technology in a life-critical environment. Kang and Bang [2006] focused their analysis on privacy in context-aware computing environments and total protection considerations on privacy, and presented new, privacy-related considerations for the context-aware computing environment. Several studies such as Ackerman *et al.* [2001], Sacramento *et al.* [2005] stressed that information privacy has to consider laws, technology and economy, as well as the technology itself.

However, we found the current studies had three main drawbacks. First, these studies have addressed only a small subset of the privacy challenges faced context-aware service applications; for example, a single technical issue such as encryption technology or a protocol for securing the context information data transaction. Second, most systemic solutions are based on simplifying assumptions; for example, only considering location information or assuming that context information is neatly partitioned into repositories that are under the control of a single user. Lastly, to identify factors of information privacy concern, most studies have adopted user surveys. However, general users fall short of knowledge and experience simply. To date, since context-aware services have not been widely deployed on a commercial scale yet, only very few people have prior experiences with context-aware personalized services. It is difficult to build users' knowledge about context-aware technology even by increasing their understanding in various ways: scenarios, pictures, flash animation, etc.

Due to these limitations, it is crucial to develop a set of factors of information privacy concern that take into consideration wider technology characteristics. It is also important that experts who have detailed knowledge of the privacy issue as well as context-aware technologies involve in the survey to allow them take part in the identification process of information privacy concern in context-aware personalized services. In this study, a set of factors is developed based on the overall technology characteristic of context-aware service. We deploy a rigorous data collection method called

a Delphi survey involving an international panel of researchers and practitioners in the privacy and context-aware service field. This data collection method is designed to elicit and organize opinions of a panel of experts through iterative, controlled feedback.

Ⅲ. Research Methods

3.1 Delphi method

The Delphi concept was originally developed from the American defense industry. Project Delphi was the name of a study undertaken by the Rand Corporation for the US Air Force in the early 1950's concerning the use of expert opinion [Robinson, 1991]. The most recognized book on the subject is by Linstone and Turoff [1975]. Other useful reviews include Schmidt [1997] and Okoli and Pawloski [2004].

The Delphi method is a technique for eliciting and refining group judgments; a means for structuring a group communication process, and a communication device that can be applied when the consensus of experts on an uncertain issue, often intangible, is desired [Linstone and Turoff, 1975]. In contrast to a traditional survey that uses a random sample to estimate the views held by separate individuals in a target population, the Delphi Method uses interactions by a panel with relevant expertise to arrive at a consensus group response to difficult questions. The results are not designed to represent a statistical sampling of a larger population. Rather, it is a structured group interaction that proceeds through rounds of opinion collection and feedback. Each round is composed of a written survey followed by feedback to the respondents of the statistical scores for each survey question. After each round the respondents are surveyed again to determine whether their opinions have shifted after seeing the statistical results from the prior round (s). As a result of the process there is typically a convergence of opinion. Usually, after three or four rounds the convergence moves toward a stabilized group opinion. This group opinion may reflect agreement, disagreement, or some of each.

The Delphi method has proven a popular tool in information system (IS) research [Brancheau *et al.*, 1996; Hayne and Pollard, 2000; Holsapple and Joshi, 2002; Lai and Chung, 2002; Mulligan, 2002; Nambisan *et al.*, 1999; Schmidt *et al.*, 2001]. Okoli and Pawlowski [2004] proposed a systemic approach to conduct a Delphi study as a research tool in certain cases- a lack of a definitive method for conducting the research and a lack of statistical support for the conclusions drawn. They provided rigorous guidelines for the process of selecting appropriate experts for the study and gave detailed principles for making design choices during the process that ensure a valid study. This paper adopts the framework that they developed because they provide a complete guideline for a rigorous approach towards conducting Delphi methods.

Prior studies that have used the Delphi method in information systems research can be divided into two research streams. Business issue forecasting and identification represent one stream. Czinkota and Ronkainen [1997] forecasted changes in the international business environment over the next decade and the impact of these changes on corporate practices

through the experts from policy, business and academic communities. Kendall *et al.* [1992] forecasted the role of the systems analyst in the 21st century as a result of systems analysts' discussion. Brancheau *et al.* [1996] identified the most critical issues facing IS executives in the coming 3~5 years with senior IS executives. Schmidt *et al.* [2001] identified common risk factors for software projects as a foundation for theory building about IS project risk management through three panels of experienced software project managers from Hong Kong, Finland and the United States. Lai and Chung [2002] identified a prioritized list of international data communications activities vital to multinational corporations in managing information exchanges for control and implementation of global business strategies from IS executives' opinions.

Technology issue identification represents a second stream of application of the Delphi method. Viehland and Hughes [2002] identified 12 future scenarios related to the potential success of the Wireless Application Protocol (WAP) through industry and academic experts. Mulligan [2002] developed a capability-based typology of information technologies within the financial services industry from the discussion of members of 11 different organizations. Along with this research stream, we adopt the Delphi method to identify factors of information privacy concern in context-aware service application.

3.2 Selection of the Delphi method

We selected the Delphi method for finding the factors of privacy concerns in providing context-aware services. The Delphi method is a highly formalized method of communication that is designed to extract the maximum amount of unbiased information from a panel of experts. Further, it is appropriate for collecting opinions from geographically dispersed experts [Helle *et al.*, 2003]. It, therefore, lends itself well to obtaining a set of universal factors of information privacy concern and its priority. More specific reasons are as follows:

1. This study is an investigation of factors that would influence users' concern in context-aware personalized services. This complex issue requires knowledge from people who understand the different social and technical issues there. However, most of users do not have sufficient knowledge and experience because context-aware services have not been widely deployed on a commercial scale yet. Therefore, we expect that a Delphi study which depends on the opinion of the expert would be more appropriate method for our study.
2. Through a Delphi method, it is possible to collect a data from a panel of experts. This panel study is a more appropriate method for the research, rather than collecting any individual expert's opinions.
3. The size of a Delphi survey depends on the homogeneity of the expert population and whether the study searches for qualitative or quantitative results [Delbecq *et al.*, 1975]. As this research searches for qualitative information that may help identify concern factors in context-aware personalized services, a small group of ten participants is considered adequate.
4. There were many prior studies which are

related to Delphi studies and we can use them. For example, the Delphi study proposed by Schmidt would serve to solicit opinions from experts and to have them rank the according to their importance. Guideline presented by Okoli and Pawlowski [2004] would help to choose appropriate experts and to administer the survey process.

To carefully cope with the validity and reliability of the Delphi method, the following guidelines are completely adopted:

1. Panel selection: only the experts who have substantial experiences on information privacy issues, as well as context-aware systems, were carefully selected from the literatures and then invited.
2. The experts did not know who have been invited. This anonymity can get rid of any distortion caused by interpersonal conflicts and group think.
3. Format of Delphi rounds: We performed according to three-round format, which is recommended by the Delphi method literature.
4. The summary of results in the previous round is submitted to the experts to let them identify the group memory. This contributes to discern what are consented and what are controversial.

3.3 Panel Selection

The success of Delphi method depends principally on careful selection of the panelists, not on the size of the panel group. The panel size depends on the number needed to have a representative pooling of views and is commonly thought to be ten to fifty members in the final round of the process. According to Hasson *et al.* [2000], "there are no universally agreed criteria for the selection of experts" and "no magic formula to help researchers decide on who are the experts and how many there should be." Since the selected experts must have knowledge of the subject area, however, participants cannot be selected randomly [Okoli and Pawloski, 2004].

In this study, a group of experts was selected to provide opinions on the suitability of a certain context-aware computing characteristic for a given criterion. Since the information solicited requires in-depth knowledge and sound experience about the various technology characteristics of context-aware computing and users' privacy concern or attitude, a purposive approach was adopted to select this focused group of experts [Morgan, 1998; Neustaedter and Greenberg, 2003]. The following criteria were devised to correctly identify eligible participants for the Delphi surveys.

1. Possess long and in-depth research experience in the privacy sector;
2. Expert-level; has a detailed knowledge of all the technology characteristics of context-aware computing;
3. Is directly or recently involved in the context-aware development projects.

In order to obtain the most valuable opinions, only practitioners who met all the above sampling criteria were selected. As a result, ten members of the panel represent a wide distribution of professional people, with three from public client organizations, three from private consultant groups, and four who are university-level academics. We also made a conscious

effort to balance the panel with respect to geographic distribution to avoid cultural differences that could reflect privacy perceptions. Hence, five out of ten panelists were selected from America, three from Europe and the remaining two from Asia. The composition of this group of experts provides a balanced view for the Delphi survey. <Table 2> shows more detailed information about experts.

3.4 Format of Delphi rounds

Delphi rounds formatting will faithfully follow the procedure for the Delphi study proposed by Okoli and Pawlowski. This will involve three general rounds: (1) brainstorming for important factors; (2) narrowing down the original list to the most important ones; and (3) ranking the list of important factors. For this round only, experts were treated as individuals, not panels.

Adapted from Okoli and Pawlowski, we outlined the process of administrating the study. We performed three rounds. In the first and second rounds of the Delphi questionnaire, we gathered a set of exclusive factor for information privacy concern in context-aware personalized services. The respondents were asked to provide at least five main factors for the most appropriate understanding of the information privacy concern in the first round. To do so, some of the main factors found in the literature were presented to the participants. The second round of the questionnaire discussed the main factor provided in the first round, fleshed out with relevant sub-factor. Respondents were then requested to evaluate each sub factor's suitability against the corresponding main factors to determine the final sub-factors from the candidate factors. The sub-factors were found from the literature survey. Final factors selected by over 50% of experts. In the

<Table 2> List of the Panel of Experts for the Delphi Method

Expert #	Sex	Occupation	Position	Major career field
1	Male	Professor	Professor	Privacy Agent in context-aware computing, User acceptance in context-aware computing environment
2	Male	Consultant	Senior	Privacy service development for context-aware mobile computing
3	Male	Practitioner	Manager	Privacy preserving system design
4	Male	Professor	Professor	Privacy concerns pertaining to location-based services
5	Male	Practitioner	Senior research engineer	Privacy and information integrity in wearable computing
6	Male	Professor	Professor	Design for privacy in ubiquitous computing environments
7	Male	Official	Assistant director	Privacy-preserving public displays
8	Male	Consultant	Senior	Privacy issues in the ubiquitous commerce
9	Female	Professor	Associate professor	Location privacy in ubiquitous computing
10	Male	Consultant	Senior	Privacy issues in the context-aware computing

third round, a list of factor with corresponding questions was provided, and the respondents were requested to assess the importance of each main factor and its corresponding sub factors. Finally, we calculate mean rank of each item to make a final result. The Delphi survey was carried out for seven months (from October, 2008 to April, 2009). After pre-recruiting panels, Delphi round 1 questionnaire was sent to experts in October 2008. We asked them to return the questionnaire by e-mail. If we received no reply, we re-sent the questionnaire after 3 weeks and again after 4 weeks. First round took much longer than we expected, so round 2 questionnaire was sent in January 2009. Lastly, third round carried out from March 2009 to April 2009.

While analyzing the data, we focused on group consensus rather than individual insistence. To do so, a concordance analysis, which measures the consistency of the experts' responses over successive rounds of the Delphi, was adopted during the survey process.

Ⅳ. Results and Analysis

4.1 Delphi round one

To begin, an invitation letter was sent to panel members. The letter explained the purpose of the research, and then informed the members that there would be three rounds of questionnaires. In the first round, two groups of questions were presented to the panel of experts. The first group of survey questions asked the experts to provide at least four major factors that influence users' concern about information privacy in context-aware personalized services. In the questionnaire, a list of six main factors from previous studies was also included as references.

1. "Would you please select four main factors in the following list, which you believe are the major factor for information privacy concern in context-aware personalized services? The followings are six of the factor found in previous research studies and literature. [Context-awareness, Tracking and recording, Sensory network, Processing, Service delivery, Storage]"

   The second question is given to the experts to state their opinion about main factor:

2. "Would you please state your opinion about terminology and classification of the main factor? You are welcome to add, delete or modify the factor."

   The factors suggested by the experts were carefully analyzed and a list of factors was formed. <Table 3> shows all the factors provided by experts in the first round. Altogether all six factors were retained and no factor was newly added during the survey.

<Table 3> Factor Provided by the Panel of Experts in Delphi Round One

Factor	Frequency of criterion by experts
Context data collection	80%
Tracking and recording	70%
Sensory network	70%
Context-aware processing	60%
Context-aware service delivery	60%
Context data Storage	60%

However, there were some opinions about the main factor as follows.

- "The main factor name is very broad. It needs more detail particularly processing and storage factor."
- "The main factor can be classified by IPOS model. If so, the intended meaning of the main factor will be clearer."

<Table 4> Sub Factor Identified from Literature Survey

Division	Main factor	Sub factor	Explanation	Major literature references
Input	Context data collection	Awareness functionality	Concerns for the fact that the context is detected	Junglas and Spitzmuller, 2005
		Diverse type of context data which be collected	Concerns for many type of context data which be collected	Spiekermann, 2005
		High identifiable level of identical data	Concerns for high identifiable level of identical data which is used to identify a user in context-aware system	Chellappa and Sin, 2005
		Various subject which collects context data	Concerns for various subjects which collect context data	Spiekermann, 2005
		Autonomous awareness	Concerns for collecting context data automatically without notice	Floridi, 2006
	Tracking and recording	Tracking and recording functionality	Concerns for tracking and recording technologies they track and record a user's context periodically	Nguyen *et al.*, 2008
		Continuous tracking	Concerns for continuous tracking and recording events	Langheinrich, 2002
	Sensor and infrastructure	Embedded and disappearing sensor devices	Concerns for embeddedness and disappearance of sensor devices	Scheffler and Schnor, 2005; Soppera and Burbridge, 2004
		Advanced sensing capabilities of sensors	Concerns for the sensing capabilities of sensors- capabilities exceeding those of the human senses	Cas, 2005; Neustaedter and Greenberg, 2003; Dritsas *et al.*, 2006
Process	Context-aware processing	Risk of disembodiment or disassociation	Concerns for the prevalent risk of disembodiment or disassociation because much more data is being collected	Spiekermann, 2005; Hui *et al.*, 2006
		Autonomous decision	Concerns for autonomous decision by the system on how and when to use, or to pass on, the collected information	Cas, 2005
		Advanced capability in artificial intelligence	Concerns for the advances in artificial intelligence and in data mining techniques	Dritsas *et al.*, 2006
Output	Context-aware service delivery	Push-type delivery	Concern for push-type dissemination- the system automatically delivers new context-aware services by contextual events	Cheverst *et al.*, 2002; Sakagami *et al.*, 1998; Beer *et al.*, 2007
		Interrupted delivery	Concerns for being interrupted while engaging in other tasks by proactive delivery	Palen and Dourish, 2003
		Sensitive information on public display	Concerns for sensitive information for a particular user of a display is observed by another user or a bystander	Kuhn, 2005; Friedman, 2006
Storage	Context data Storage	Excessive store of data	Concerns for the excessive store of sensor-based context data as well as higher-level inferred context	Spiekermann, 2005; Hui *et al.*, 2006

The main factors were revised to reflect these opinions. That is, we categorized the main factor into four groups in terms of IPOS (Input-Process-Output-Storage) model and rephrased their name as indicated in <Table 4>. IPOS is an underlying conceptual model of a general application. Because the model is widely used to convey systems' fundamentals, it is most suitable for clarifying our factor based on technology characteristics of context-aware personalized services. It consists of four distinct components: system's inputs, outputs, processing steps, and storage. In our division, input, processing, and output and storage represent information privacy concerns in input stage, processing stage, output stage and storage stage in context-data handling, respectively.

4.2 Delphi Round Two

The second round of the questionnaire addressed the main and sub factor provided in the first round. The experts were asked to indicate the suitability of each sub factor against each main factor to select the final sub factor, using a simple scale: very suitable, suitable,

<Table 5> Delphi Round Two Results: Frequency Distribution and Percentage

Division	Main factor	Sub factor	% of experts who stated the factor as either very suitable or suitable	Very suitable	Suitable	Not suitable
Input	Context data collection	Awareness functionality	40%	2	2	6
		Diverse type of context data which be collected	100%	7	3	0
		High identifiable level of identical data	90%	5	4	1
		Various subject which collects context data	40%	3	1	6
		Autonomous awareness	80%	2	6	2
	Tracking and recording	Tracking and recording functionality	100%	7	3	0
		Continuous tracking	80%	6	2	2
	Sensory network	Embedded and disappearing sensor devices	80%	4	4	2
		Advanced sensing capabilities of sensors	90%	6	3	1
Process	Context-aware processing	Risk of disembodiment or disassociation	40%	3	1	6
		Autonomous decision	80%	4	4	2
		Advanced capability in artificial intelligence	90%	5	4	1
Output	Context-aware service delivery	Push-type delivery	90%	6	3	1
		Interrupted delivery	70%	5	2	3
		Sensitive information on public display	80%	5	3	2
Storage	Context data Storage	Excessive store of data	100%	6	4	0

and not suitable.

The sub factors (see <Table 4>) were identified as a result of the literature survey. In the questionnaire, these explanations were included. The total frequency distribution of the experts who suggested the factors in round one and a percentage of the experts for each factor were also stated.

<Table 5> shows the indication of suitability of each sub factor by the ten experts. From the second round, factors that received only 50% agreement or below in the category of very suitable or suitable were removed in the next round. As a result, only thirteen sub factors remained in the third round.

4.3 Delphi Round Three

The experts were asked to indicate the importance of the six main factor that had been selected in round one of the Delphi survey and thirteen sub factors that had been selected in round two, using a seven-point Likert scale from "extremely important" (7) to "extremely unimportant" (1). The total frequency distribution and percentage of the experts who selected the sub factors in round two were also stated. <Table 6> and <Table 7> show the numeric results of Delphi round three.

<Table 6> Importance of Main Factor for Information Privacy Concern on a 7-point Likert Scale (Higher Values Indicate Higher Importance)

Division	Main factor	Average
Input	Context data collection	6.2
	Tracking and recording	5.8
	Sensory network	5.6
Process	Context-aware processing	4.8
Output	Context-aware service delivery	5.5
Storage	Context data Storage	4.6

<Table 7> Importance of Sub Factor for Information Privacy Concern on a 7-point Likert Scale (Higher Values Indicate Higher Importance)

Division	Main factor	Sub factor	Average
Input	Context data collection	Diverse type of context data which be collected	5.9
		High identifiable level of identical data	6.2
		Autonomous awareness	5.5
	Tracking and recording	Tracking and recording functionality	5.8
		Continuous tracking	5.3
	Sensory network	Embedded and disappearing sensor devices	5.6
		Advanced sensing capabilities of sensors	5.2
Process	Context-aware processing	Autonomous decision	4.8
		Advanced capability in artificial intelligence	4.2
Output	Context-aware service delivery	Push-type delivery	4.5
		Interrupted delivery	4.8
		Sensitive information on public display	5.5
Storage	Context data Storage	Excessive store of data	4.5

Experts reported that context data collection and high identifiable level of identical data are the most important factor in the main factors and sub factors, respectively. Additional important sub-factors included the diverse type of context data collected, tracking and recording functionalities, and embedded and disappearing sensor devices. The average score of each factor is very useful for future context-aware personalized service development in the view of the information privacy.

The further explanation of the results shown in <Table 6> and <Table 7> in terms of the final factors themselves and the importance of each are as follows.

The final factors have the following differences comparing to those proposed in other studies. First, the concern factors in <Table 6> differ from existing studies' which are based on privacy issues that may occur during the lifecycle of acquired user information. However, our study helped to clarify these sometimes vague issues by determining which privacy concern issues are viable based on specific technical characteristics in context-aware personalized services. Since a context-aware service differs in its technical characteristics compared to other services, we selected specific characteristics that had a higher potential to increase user's privacy concerns. Secondly, this study considered privacy issues in terms of service delivery and display that were almost overlooked in existing studies by introducing IPOS as the factor division. Lastly, in each factor, it correlated the level of importance with professionals' opinions as to what extent users have privacy concerns. The reason that it did not select the traditional method questionnaire at that time is that context-aware personalized service considered the absolute lack in understanding and experience of users with new technology.

For understanding users' privacy concerns, professionals in the Delphi questionnaire process selected context data collection, tracking and recording, and sensory network as the most important factors among technological characteristics of context-aware personalized services. In the creation of a context-aware personalized services, this study demonstrates the importance and relevance of determining an optimal methodology, and which technologies and in what sequence are needed, to acquire what types of users' context information. Most studies focus on which services and systems should be provided and developed by utilizing context information on the supposition, along with the development of context-aware technology. However, the results in this study show that, in terms of users' privacy, it is necessary to pay greater attention to the activities that acquire context information. To inspect the results in the evaluation of sub factor, additional studies would be necessary for approaches on reducing users' privacy concerns toward technological characteristics such as highly identifiable level of identical data, diverse types of context data collected, tracking and recording functionality, embedded and disappearing sensor devices. The factor ranked the next highest level of importance after input is a context-aware service delivery that is related to output. The results show that delivery and display showing services to users in a context-aware personalized services toward the anywhere-

anytime-any device concept have been regarded as even more important than in previous computing environment. For example, 'sensitive information on public display', which is one of the high-ranked factors (5.5/7.0), was identified even though it has not been considered in traditional technology.

The results appeared in <Table 6> and <Table 7> may be different according to the evaluating experts' characteristics. Particularly, the experts' propensity to individualism can be affected by cultural differences. In our study, we invited 80% of the experts from western countries. However, we could not find any statistically different evaluating results between western and Asian experts. Moreover, since we focus on the relative importance among the factors, not the values *per se*, the possibility of the impact or distort due to cultural difference will not be remarkable.

V. Conclusion

In comparison to traditional information services, context aware personalized services acquire high volumes of context data. By using a variety of user interactions to provide as natural an interface as possible so as to increase user intention to use them, they deliver a wide and growing range of context-based information. These data and interface varieties, however, lead users to new privacy concerns.

In this paper, we identified a generic set of factors for elemental information privacy concern in context-aware personalized services and to develop a rank-order list of information privacy concern factors to understand information privacy issues in context aware personalized services. Using the Delphi method with respondents who have expertise in context aware computing privacy issues, the following main factors emerged: context-awareness, tracking, recording, sensors, and infrastructure. One interesting finding was that the newly identified factors were ranked as more important than traditional factor, such as processing and service delivery factors. This implies that earlier efforts for applying traditional factor to understand information privacy concern for context aware personalized services may need to be refocused. Moreover, the weight values will be used in future context-aware personalized service development in the view of the information privacy.

Specifically, the results of this study can be summarized in three points. First, through dividing privacy concern factors by input-process-output-storage perspective, we obtained balanced result in finding privacy concern factors. Prior studies tends to overlook these things, even four components are necessary components in system and service development. For example, most of researchers have focused on input division rather than output or storage division in HCI area. However, our result shows that output privacy concern factors can be very concerned factors. Especially, there is much room for consideration about privacy issues for context-aware services based on public display.

Second, through extracting privacy concern factors based on context-aware technical characteristics, we found new privacy concern factors which had not been normally considered. For example, lots of push-type delivery context-aware services have been introduced recently like 'When user enters a specific place,

a context-aware service agent places a personalized ad on a digital billboard'. However, there was little discussion about privacy issues about these kinds of services. Our study found push-type delivery related privacy concern factor. And it indicated that the factor was significant.

Finally, we did not simply list up privacy concern factors, but we derived the weight valued of each factors. It can be used a guideline for context-aware personalized service providers or system developers. It is impossible to consider all kinds of privacy issues in real development environments. So, if developers use the proposed criteria and weights, they can select most important privacy concern factors and determine the priority for their own service or system. Moreover, some of the factors found from the Delphi method are novel: they have not addressed in the conventional computer-based services.

Considering the concern factors to develop context aware personalized services will help to increase service success rate and hopefully user acceptance for those services. Our future work will be to adopt these factors for qualifying context aware service development projects such as u-city development projects in terms of service quality and hence user acceptance.

〈References〉

[1] Ackerman, M., Darrel, T., and Weitzner, D.J., "Privacy in Context," *Human-Computer Interaction*, Vol. 16, No. 2/4, 2001, pp. 167-176.

[2] Adams, A., "Multimedia Information Changes the Whole Privacy Ballgame," *Proceedings of Computers, Freedom, and Privacy*, 2000.

[3] Beer, T., Rasinger, J., and Hopken, W., "Exploiting E-C-A Rules for Defining and Processing Context-Aware Push Messages," *Lecture Notes in Computer Science*, Vol. 4824, 2007, pp. 199-206.

[4] Beresford, A.R. and Stajano, F., "Location Privacy in Pervasive Computing," *IEEE Pervasive Computing*, Vol. 2, No. 1, 2003, pp. 46-55.

[5] Bookbinder, J.H., Imada, S.J., and Lynch, M., "The Future of Logistics in Canada: A Delphi-Based Forecast," *Logistics and Transportation Review*, Vol. 30, No. 1, 2004, pp. 95-112.

[6] Brancheau, J.C., Janz, B.D., and Wetherbe, J.C., "Key Issues in Information Systems Management: 1994~1995 SIM Delphi Results," *MIS Quarterly*, Vol. 20, No. 2, 1996, pp. 225-242.

[7] Cas, J., "Privacy in Pervasive Computing Environments-a Contradiction in Terms?," *IEEE Technology and Society Magazine*, 2005, pp. 24-33.

[8] Chellappa, R.K. and Sin, R.G., "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, Vol. 6, No. 2/3, 2005, pp. 181-202.

[9] Cheverst, K., Mitchell, K., and Davies, N., "Exploring Context-aware Information Push," *Personal and Ubiquitous Computing*, Vol. 6, No. 4, 2002, pp. 276-281.

[10] Clarke, R., "Internet Privacy Concerns Confirm the Case for Intervention," *Communi-*

cations of the ACM, Vol. 42, No. 2, 1999, pp. 60-67.

[11] Czinkota, M.R. and Ronkainen, I.A., "International Business and Trade in the Next Decade: Report From a Delphi Study," *Journal of International Business Studies*, Vol. 28, No. 4, 1997, pp. 827-844.

[12] Delbecq, A.L., Gustafsson, D.H., and Van de Van, A.H., *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processed*, Scott-Foresman and Co. Glenview, IL, 1975.

[13] Dritsas, S., Gritzalis, D., and Lambrinoudakis, C., "Protecting Privacy and Anonymity in Pervasive Computing: Trends and Perspectives," *Telematics and informatics*, Vol. 23, No. 3, 2006, pp. 196-210.

[14] Edmunds, H., *The Focus Group Research Handbook*, NTC Business Books, 1999.

[15] Eymann, T. and Morito, H., "Privacy Issues of Combining Ubiquitous Computing and Software Agent Technology in a Life-Critical Environment," *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, Den Haag, IEEE Press, 2004.

[16] Floridi, L., "Four Challenges for a Theory of Informational Privacy," *Ethics and Information Technology*, Vol. 3, No. 8, 2006, pp. 109-119.

[17] Friedman, B., Kahn Jr., P.H., Hagman, J., and Severson, R.L., "The Watcher and the Watched: Social Judgments about Privacy in a Public Place," *Human-Computer Interaction*, Vol. 21, No. 2, 2006, pp. 235-272.

[18] Gandon, F.L. and Sadeh, N.M., "Semantic Web Technologies to Reconcile Privacy and Context Awareness," *Web Semantics: Science, Services and Agents on the World Wide Web*, Vol. 1, No. 3, 2004, pp. 241-260.

[19] Hasson, F., Keeney, S., and McKenna, H., "Research Guidelines for the Delphi Survey Technique," *Journal of Advanced Nursing*, Vol. 32, No. 4, 2000, pp. 1008-1015.

[20] Hayne, S. and Pollard, C., "A Comparative Analysis of Critical Issues Facing Canadian Information Systems Personnel: A National and Global Perspective," *Information and Management*, Vol. 38, No. 2, 2000, pp. 73-86.

[21] Helle, M.R., Reijnown, M., and Mannermaa, J.P., "Using a Delphi Survey to Access the Value of Pharmaceutical Process Validation. Part 1: Survey Methodology," *Pharmaceutical Technology Europe*, Vol. 15, No. 4, 2003, p. 43.

[22] Herlocker, J. and Konstan, J., "Content-Independent, Task-Focused Recommendations," *IEEE Internet Computing*, Vol. 5, 2001, pp. 40-47.

[23] Hoffman, D.L., Novak, T.P., and Peralta, M.A., "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *The Information Society*, Vol. 15, No. 2, 1999, pp. 129-140.

[24] Holsapple, P. and Joshi, K., "Knowledge Manipulation Activities: Results of a Delphi study," *Information and Management*, Vol. 39, No. 6, 2002, pp. 477-490.

[25] Hui, K.L., Tan, B.C.Y., and Goh, C.Y., "Online Information Disclosure: Motivators and Measurements," *ACM Transactions on Internet Technology*, Vol. 6, No. 4, 2006, pp. 415-441.

[26] Jiang, X. and Landay, J.A., "Modeling Pri-

vacy Control in Context-Aware Systems," *IEEE Pervasive Computing*, Vol. 1, No. 3, 2002, pp. 59-63.

[27] Jiang, X., Hong, J.I., and Landay, J.A., "Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing," *UbiComp 2002*, 2002, pp. 176-193.

[28] Junglas, I.A. and Spitzmuller, C., "A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services," *Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences, (HICSS'05)*, 2005, pp. 180-182.

[29] Kang, J.M. and Bang, K.C., "A Study on Protection Technology and Scope about Information Privacy in Ubiquitous Sensing Network Environment," *Journal of Digital Society*, Vol. 7, No. 4, 2006, pp. 301-308.

[30] Kendall, J.E., Kendall, K.E., Smithson, S., and Angell, I.O., "SEER: A Divergent Methodology Applied to Forecasting the Future Roles of the Systems Analyst," *Human Systems Management*, Vol. 11, No. 3, 1992, pp. 123-135.

[31] Kuhn, M.G., "Electromagnetic Eavesdropping Risks of Flat-Panel Displays," *Lecture Notes in Computer Science*, Vol. 3424, 2005, pp. 88-107.

[32] Kuo, F.Y., Lin, C.S., and Hsu, M.H., "Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices," *Journal of Business Ethics*, Vol. 73, No. 2, 2007, pp. 145-160.

[33] Lai, V. and Chung, W., "Managing International Data Communications," *Information and Management*, Vol. 45, No. 3, 2002, pp. 89-93.

[34] Langheinrich, M., "Privacy Invasions in Ubiquitous Computing, Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing," *UbiComp 2002*, 2002, Göteborg, Sweden.

[35] Lapkin, A., "Context-Aware Computing: Four Questions CIOs Should be Asking," *Gartner Special Report* (http://www.gartner.com/DisplayDocument?ref = g_search &id = 1144612&subref = simplesearch), 2009.

[36] Linstone, H. and Turoff, M., *The Delphi Method: Techniques and Applications*. Addison Wesley, Reading, MA, 1975, pp. 3-12.

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

[38] Mobasher, B., Cooley, R., and Srivastava, J., "Automatic Personalization Based on Web Usage Mining," *Communications of the ACM*, Vol. 43, No. 8, 2000, pp. 142-151.

[39] Morgan, D.L., *The Focus Group Guidebook*, Focus Group Kit 1, Sage, Beverly Hills, CA, 1998.

[40] Mulligan, P., "Specification of a Capability-Based IT Classification Framework," *Information and Management*, Vol. 39, No. 8, 2002, pp. 647-658.

[41] Myles, G., Friday, A., and Davies, N., "Preserving Privacy in Environments with Location-Based Applications," *IEEE Pervasive Computing*, Vol. 2, No. 1, 2003, pp. 56-64.

[42] Nambisan, S., Agarwal, R. and Tanniru,

M., "Organizational Mechanisms for Enhancing User Innovation in Information Technology," *MIS Quarterly*, Vol. 23, No. 3, 1999, pp. 365-395.

[43] Neustaedter, C. and Greenberg, S., "The Design of a Context-Aware Home Media Space for Balancing Privacy and Awareness," *UbiComp 2003*, 2003, pp. 297-314.

[44] Nguyen, D.H., Kobsa, A., and Hayes, G. R., "An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies," *Proceedings of the 10th International Conference on Ubiquitous Computing*, 2008, pp. 182-191.

[45] Nissenbaum, H., "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy*, Vol. 17, No. 5/6, 1998, pp. 559-596.

[46] Nowak, G.J. and Phelps, J., "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When Privacy Matters," *Journal of Direct Marketing*, Vol. 11, No. 4, 1997, pp. 94-109.

[47] Okoli, C. and Pawloski, S., "The Delphi Method as a Research Tool: An Example, Design, Considerations and Applications," *Information and Management*, Vol. 42, No. 1, 2004, pp. 15-29.

[48] Palen, L. and Dourish, P., "Unpacking "Privacy" for a Networked World," *Human Factors in Computing Systems: CHI 2003*, Vol. 5, No. 1, 2003, pp. 129-136.

[49] Robinson, J.B.L., "Delphi Methodology for Economic Impact Assessment," *Journal of Transportation Engineering*, Vol. 117, No. 3, 1991, pp. 335-349.

[50] Sacramento, V., Endler, M., and Nascimento, F.N., "A Privacy Service for Context-aware Mobile Computing," *First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 2005, pp. 182-193.

[51] Sakagami, H., Kamba, T., Sugiura, A., and Koseki, Y., "Effective Personalization of Push-Type Systems-Visualizing Information Freshness," *Computer Networks and ISDN Systems*, Vol. 30, No. 1/7, 1998, pp. 53-63.

[52] Scheffler, T. and Schnor, B., "Privacy Requirements for Embedded Sensor Devices," *IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications*, Vol. 2, 2005, pp. 790-794.

[53] Schmidt, R.C., "Managing Delphi Surveys Using Nonparametric Statistical Techniques," *Decision Sciences*, Vol. 28, No. 3, 1997, pp. 763-774.

[54] Schmidt, R.C., Lyytinen, K., Keil, M., and Cule, P., "Identifying Software Project Risks: An International Delphi Study," *Journal of Management Information Systems*, Vol. 17, No. 4, 2001, pp. 5-36.

[55] Shoji, T. and Nakajima, T., "Privacy-Concern for Context-Aware Environments," *Proceedings of IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems*, 2004, pp. 85-89.

[56] Smith, H.J. and Milberg, S.J., "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS quarterly*, Vol. 20, No. 2, 1996, pp. 167-196.

[57] Soppera, A. and Burbridge, T., "Maintaining Privacy in Pervasive Computing-Enabling Acceptance of Sensor-Based Services," *BT Technology Journal*, Vol. 22, No. 3,

2004, pp. 106-118.

[58] Spiekermann, S., "Perceived Control: Scales for Privacy in Ubiquitous Computing Environments," *Proceedings of 10th International Conference on User Modeling*, 2005.

[59] Stone, E.F., Gardner, D.G., Geugal, H.G., and McClure, S., "A Field Experiment Comparing Information-Privacy Values, Beliefs and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology*, Vol. 68, No. 3, 1983, pp. 459-468.

[60] Viehland, D. and Hughes, J., "The Future of the Wireless Application Protocol," *Proceedings of the Eighth Americas Conference on Information Systems*, Dallas, 2002, pp. 1883-1891.

[61] Wang, H., Lee, M.K.O., and Wang, C., "Consumer Privacy Concerns about Internet Marketing," *Communications of the ACM*, Vol. 41, No. 3, 1998, pp. 63-70.

[62] Westin, A., *Privacy and freedom*. New York: Athaneum, 1967.

◆ About the Authors ◆

Yonnim Lee

Yonnim Lee is enrolled in a doctoral course at Department of International Business at Kyung Hee University at this present and also she is working for Sookmyung Women's University as a part-time lecturer. Also she is at work for Research Center for Ubiquitous Business and Services (RCUBS) as a researcher and takes part in UCN projects for Ministry of Knowledge Economy as well as Subjects of Assistance Projects for Specific Fundamental Study for Ministry of Education, Science and Technology. She received a bachelor's degree majored in management and economics from Handong Global University in 2000 and a master's degree from Ewha Woman's University in 2003. After receiving the master's degree, she worked as an IT consultant at fields of financing and IT consulting. Recently she is studying with interest in context aware system, privacy issues in context aware computing, energy control system, etc.

Ohbyung Kwon

Dr. Ohbyung Kwon is presently a professor at School of Management, Kyung Hee University, South Korea, where he initially joined in 2004. In 2002, he worked Institute of Software Research International (ISRI) at Carnegie Mellon University to perform myCAMPUS project on context-aware computing, web service and semantic web. He received MS and PhD degree at KAIST in 1990 and 1995, respectively. He is now an adjunct professor at San Diego State University (SDSU). His current research interests include context-aware services, case-based reasoning and DSS. He has presented various papers in leading information system journals including Decision Support Systems, Simulation, International Journal of Computer Integrated Manufacturing, and Behavior and Information Technology.