2005

Privacy Issues in the Era of Ubiquitous Commerce

Holtjona Galanxhi
University of Nebraska - Lincoln, hgalanxh@unlnotes.unl.edu

Fiona Fui-Hoon Nah
University of Nebraska-Lincoln, fnah@unlnotes.unl.edu

Privacy Issues in the Era of Ubiquitous Commerce

Holtjona Galanxhi
University of Nebraska-Lincoln
hgalanxh@unlnotes.unl.edu

Fiona Fui-Hoon Nah
University of Nebraska-Lincoln
fnah@unlnotes.unl.edu

ABSTRACT
The vision of ubiquitous commerce (u-commerce) is realized through the convergence of electronic, mobile, television, voice and silent commerce applications. The ubiquity, universality, uniqueness, and unison of u-commerce will provide two principal benefits for individual users and companies: increased convenience as well as more personalized and customized services. However, u-commerce will also bring new issues such as a greater degree of privacy concerns that will impact individual users, companies, and the society at large. This paper proposes and elaborates on a conceptual framework for privacy in the u-commerce era. It combines Lessig's macro-level perspective – the four-factor model of privacy – with Adam's micro-level perspective – the perceived privacy factors model. Using this framework, privacy issues related to u-commerce are discussed and future research directions are presented.

Keywords
Ubiquitous commerce, u-commerce, privacy.

INTRODUCTION

Ubiquitous commerce, also referred to as "u-commerce" or "über-commerce", extends the traditional commerce (geographic, electronic, and mobile) to a world of ubiquitous networks and universal devices (Junglas and Watson 2003). It is a new paradigm that broadens and extends the Internet era and it has the potential to create a completely new environment in business (Galanxhi-Janaqi and Nah, 2004). U-commerce emerges as a continuous, seamless stream of communication, content and services exchanged among businesses, suppliers, employees, customers, and products (Watson, Pitt, Berthon and Zinkhan, 2002). Through the convergence of the physical and digital means, higher levels of convenience and value will be created. Ubiquitous commerce is realized from the combination of electronic, wireless/mobile, television, voice, and silent commerce, and its full realization is greater than the simple sum of its components.

Ubiquitous Commerce

Watson et al. (2002) present four characteristics of u-commerce: ubiquity, universality, uniqueness, and unison. The first characteristic is ubiquity. It means that computers will be everywhere and every device will be connected to the Internet. The omnipresence of computer chips will make them "invisible", as people will no longer notice them (Watson et al., 2002). U-commerce will also add universality. Universality will eliminate the problems of incompatibility caused by the lack of standardization like the use of mobile phones in different networks. A universal device will make it possible to stay connected at any time and any place. U-commerce will add uniqueness of information. Uniqueness means that the information provided to the users will be easily customized to their current context and particular needs in specific time and place. Finally, unison aggregates the aspects of application and data in one construct (Junglas and Watson, 2003). In a u-commerce environment, it is possible to integrate various communication systems such that there is a single interface or connection point to them (Watson et al., 2002).

Schapp and Cornelius (2001) identify three global phenomena that will accelerate the growth of u-commerce: pervasiveness of technology (the explosive growth of nanotechnology and the continuing capital investments); growth of wireless (one of the fastest growing distributed bases); and increasing bandwidth and connectivity (bandwidth has been doubling every nine months, and the high-speed networks of the 3G generation will provide additional capacity and enhanced functionalities).

Issues and Challenges of U-Commerce

U-commerce applications offer many benefits, but they also face challenges and raise new questions (Galanxhi-Janaqi and Nah, 2004). The higher value of u-commerce comes from the synergy created by its components. It is ironic how the same information practices that provide value to organizations and individuals also raise privacy concerns (Bloom, George and Robert, 1994). Mobile commerce faces the same problems troubling e-commerce – plus a few of its own (Siau and Shen,

2003a, 2003b; Siau, Sheng and Nah, 2003) and these concerns are even greater for u-commerce applications. For example, silent commerce applications such as the use of RFID tags can bring benefits such as greater security for children in schools. At the same time, the use of RFID tags in schools have caused privacy concerns for the parents of these children (please refer to http://www.cnn.com/2005/EDUCATION/02/17/tracking.students.ap/index.html and/or http://www.cnn.com/2005/EDUCATION/02/10/tracking.students.ap/index.html for news reports on these issues).

U-commerce inherits the privacy, trust and security concerns of e-commerce, m-commerce and other forms of digital commerce (Galanxhi-Janaqi and Nah, 2004). Security and privacy are the two biggest concerns of consumers in embracing mobile commerce (Siau, Sheng, Nah and Davis, 2004). New social issues arise as these u-commerce applications must mesh well with natural social behaviors or they will fail or lead to unforeseen outcomes (Grudin, 2002). For example, in location-based services, businesses can use the physical location data of customers to provide solicited or unsolicited information about shopping and entertainment information in their vicinity (Junglas and Spitzmüller, 2005). Employers can also track the movement of their employees and know their locations although it may raise serious privacy concerns.

A FRAMEWORK FOR PRIVACY IN U-COMMERCE ERA

One of the main concerns related to u-commerce, and the IT evolution in general, is privacy. "Privacy, as Ethan Katsh defines it, is the power to control what others can come to know about you. People gain knowledge about you in only two ways - through monitoring or searching...." (Lessig, 1999, p. 143).

This paper focuses on privacy issues in u-commerce since privacy concerns in these types of applications are noticeably higher than in other types of commerce. Those concerns include all the privacy concerns of u-commerce components (i.e., e-commerce, m-commerce, etc.) plus additional ones. When a user shifts from wired to wireless applications, location identification and privacy concerns are increased because more information about them is now available and such information can be easily integrated from different sources and shared among different (sometimes unknown) parties. Although location-based services can be beneficial to users (e.g., by providing customized and personalized information), they can also bring additional privacy concerns. Avoine (2005), for example, describes how the RFID banknote protection schemes compromise the privacy of banknotes' bearers. Minch (2004) identified thirteen specific privacy issues associated with products and services in location-aware applications, which belong to one of the following nine categories: information collection, information retention, information usage, information disclosure, standard-based regulation, governmental regulation, industry/trade group regulation, advocacy/public interest group regulation, and marketplace regulation.

Privacy may be the biggest barrier to the long-term success of ubiquitous computing applications (Hong, Ng, Lederer and Landay, 2004). Privacy concerns existed before the rise of technologies and they are not related only to technology. With each new technology, the threats to privacy have increased. Some of the main concerns include: the kind of information that can be gathered about a person; the parties/persons who have access to the information; how the information will be used; protection of personal information against theft or other unauthorized use; accountability of the entities that gather important and sensitive information.

Hong et al. (2004) list two main reasons why privacy has always been a controversial issue for ubiquitous computing applications. First, the tremendous opportunities provided by the convergence and increasing widespread deployment of sensors, wireless networking, and devices of all form factors allow the creation of systems that can improve safety, efficiency, and convenience. Second, the numerous interviews, essays, books, and instances of negative media coverage indicate a general unease over the potential for abuse. Hence, there is fear over a potential lack of control and desire for privacy-sensitive ubiquitous applications.

Lessig (1999) distinguishes between several motives for the protection of privacy:

- *Privacy as Empowerment*. This motive refers to the informational view of privacy. In this perspective, the aim is to give people the power to control the publication and distribution of information about themselves (Langheinrich, Coroamã, Bohn and Mattern, 2005).
- *Privacy as Utility*. This motive has to do with "the right to be left alone" (Warren and Brandeis, 1980); its objective is to minimize intrusion.
- *Privacy as Dignity*. The dignity motive involves being free from unsubstantiated suspicion and it also focuses on the equilibrium of information available between two people (Langheinrich et al., 2005)
- *Privacy as a Regulating Agent*. This motive relates to the privacy laws and moral norms which can be seen as a tool to regulate and control information collection and use. This concept sees privacy as a way to limit the power of the state to regulate (Lessig, 1999).

This paper presents and discusses two models of privacy: Lessig's (1999) Socio-Level Privacy model and Adams' (1999) Users' Perceived Privacy Factors model. The two models are discussed in the context of u-commerce environment. Table 1 summarizes each model, the level of their analysis, and the main factors regarding privacy issues. Each model addresses parts of the privacy problem from different perspectives. Drawing on these two models, an integrative framework for privacy in u-commerce and its related issues are presented in Figure 1.

MODEL	LEVEL OF ANALYSIS	FACTORS
Lessig (1999): Socio-Level of Privacy	Macro – society	Legislation/Law, Social Norms, Market, Architecture/Technology
Adams (1999): Users' Perceived Privacy Factors	Micro – individuals	Information Sensitivity, Information Receiver, Information Usage, Context

Table 1: Lessig's and Adams' Privacy Models

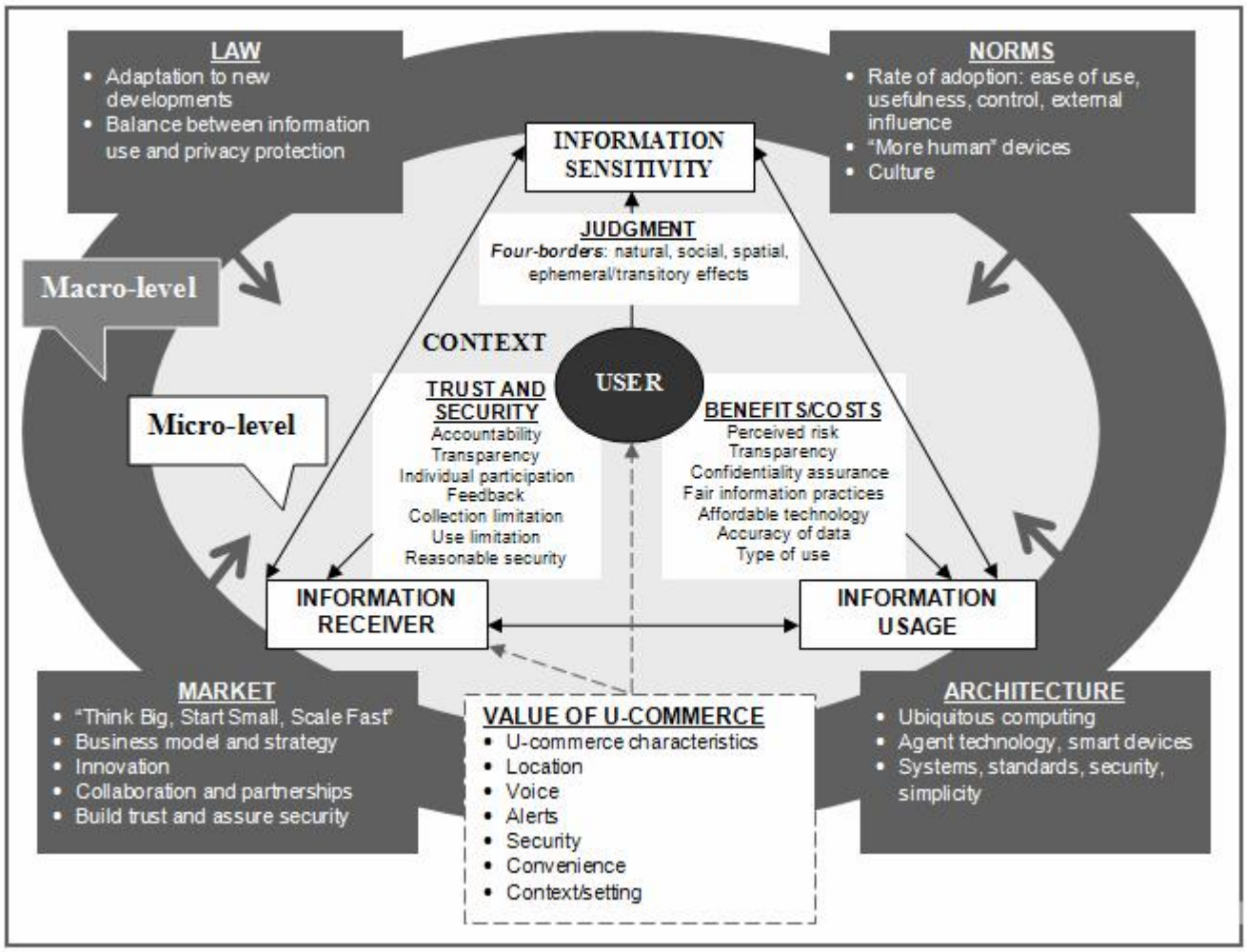

Figure 1: An Integrative Framework for Privacy in U-commerce

Lessig's Model: Socio-Level of Privacy

Lessig (1999) views privacy as a dynamic interaction of legal rules, social norms, market forces, and code. In addition to law, privacy can be regulated through norms, market, and architecture. He proposes a socio-level model of privacy which views privacy at a given place and time as dependent on the convergence of four forces: (1) the law, (2) social norms, (3) the

market, and (4) the architecture (refer to Figure 1). Lessig examines how the relationships between these four forces regulate people's behavior and provide explanations on how these forces work in combinations, and how improvements in technology can dramatically alter the composite constraint on people's conduct. According to Lessig, all four forces are needed to solve the information privacy problems faced. It is important to understand that in this model, factors do not operate independently; they are interdependent. These four forces will be discussed next.

Law/Legislation

In the u-commerce environment, legislation needs to keep up with the numerous changes of u-commerce development Another issue that exists is an inherent tension between the individual's privacy interest and the data collectors' desire to maximize the commercial use of personal data. This tension continues to be an obstacle to enactment of comprehensive privacy legislation (Beldiman, 2002). The key is finding the right balance between the two.

Market

Another factor in Lessig's model is market which refers to privacy regulator (Laudon, 1996; Varian, 1997). Hann, Kui, Lee and Png (2002) have shown that individuals' concerns about privacy are not absolute as they are willing to trade off privacy concerns for economic benefits.

For a successful implementation of u-commerce, Visa, which is heavily involved in u-commerce initiatives, suggests using the "Think Big, Start Small and Scale Fast" strategy. "Thinking big" means being visionary and recognizing the potential. "Starting small" means testing markets, understanding security issues, checking systems, and fine-tuning offerings to make them as simple and compelling as possible. And finally, "scaling fast" means recognizing when to pull out all the stops and quickly expand scope and scale (Schapp and Cornelius, 2001). Companies that take measures to assure the privacy of their customers will be in a better competitive position in the long run.

Social Norms

On one hand, social norms will influence the rate of adoption of u-commerce applications. On the other hand, they will also influence concerns about privacy issues raised by the u-commerce era. For example, sending spam e-mails may not be illegal, but it may be socially unacceptable. In such cases, companies may decide to create policies and procedures although it may not be required by law. Social norms are a cultural phenomenon and companies that engage in u-commerce initiatives need to take social norms into account. Furthermore, social norms may influence the way devices are used in a given society and the degree of the need for a 'humanization of devices' which may be different in different cultures.

Architecture/Technology

The last factor from Lessig's model is architecture. This refers to the technological context: what can and cannot be private is partially dependent on technological capability, and technology varies across temporal and spatial contexts (Lessig, 1999). The architecture/technology will affect how the cyberspace is regulated. Creators of an architecture/technology decide what they want to achieve and how they want to do it and the architecture/technology provides him with a means to accomplish the goal (Lessig, 1999). Privacy concerns can be solved through technical solutions. Therefore, ubiquitous computing, agent technology, smart devices (among other technologies) can be deployed with privacy concerns in mind. Additionally, issues relating to systems, standards, security, and simplicity should also be addressed (Schapp and Cornelius, 2001).

Macro vs. Micro Forces

Lessig's model (Figure 1) is appropriate for conceptually analyzing privacy issues from a macro-environment perspective. When an individual decides to disclose personal, private and/or sensitive information in a given situation, he/she makes this decision based on information about these four forces. However, one's knowledge about these four forces may be limited, which suggests the important role of education in this aspect.

Adams' Model: Users' Perceived Privacy Factors

At a more personal level, privacy can be classified into: territorial privacy (who and where), communication privacy (what and how), bodily privacy (who and where); and information privacy (what, who, where, how) (Langheinrich, 2002). In a ubiquitous commerce environment, obtaining information about who, where, what, and how becomes easier. As shown in Figure 1, Adams (1999) identifies three main privacy factors – information sensitivity, information receiver, and information usage – which operate in any given context.

Information Sensitivity

Information sensitivity relates to the user's perception of the data being transmitted and the information as interpreted by the receiver (Adams and Sasse, 2001). It has to do with the importance of information and potential consequences if shared with other parties. Information sensitivity can be relevant to both individuals and organizations (Adams, 1999).

Judgment: Sensitivity of information depends on the perception of the people involved and the importance and relevance of the information. Users assess information sensitivity by means of judgments via a flexible scale rather than a simple binary (private vs. not private) distinction (Adams and Sasse, 2001). The perceived sensitivity levels will be affected by their perception of the data transmitted and how public or private the broadcast situation is (Adams and Sasse, 2001). Therefore, judgments about the same situation may not result in the same level of perceived information sensitivity for different users.

Marx (2001) discussed the "cross-bordering" concept and identified four kinds of borders (Figure 1) that can be violated:

- *Natural borders* relate to the senses and the underlying assumption that physical barriers restrict what other people are entitled to perceive about us. For example, if alone at home, the assumption is that nobody can see you through the physical walls. However, in u-commerce, for instance, it is possible to penetrate natural borders, such as walls and even geographical distances.
- *Social borders* are expectations about social roles. For example, doctors, lawyers, or members of the clergy are expected to maintain confidentiality. Ubiquity of computers increases the chances that the information could go beyond the social borders of people. For example, social borders may be violated if health-related data are made known to third parties other than physicians, family members, employers, and health insurance personnel.
- *Spatial or temporal borders* involve the assumption that elements of personal biography of individuals are isolated and unavailable. Possible breaches may occur when information from various periods or aspects of one's life is integrated or put together. Such digitized information about someone can be found and referred to at a later date.
- *Borders due to ephemeral or transitory effects* have to do with the assumption that there are some things in our life that are passing and temporary, and no one would think about or refer to them at a later time. These accounts are not meant to be captured through hidden video or audio means, or otherwise preserved or given new meaning. For example, if someone is running for the president today, it is possible that he/she would not like to have the history of his/her purchases and entertaining lifestyle from 20-30 years ago published in some magazine today and perhaps even completely put out of their context!

Adams and Sasse (2001) stress "perception" since people's reactions are based on their individual perceptions regarding events. Privacy is not an absolute concept, and the desire for privacy can conflict with other things people value. For example, people often find themselves trading off some degree of privacy to gain something they value.

Ubiquitous commerce makes surveillance less expensive and therefore, it creates new opportunities for each of the above border crossings. More generally, ubiquitous computing applications tend to remove the desirable boundaries between work and personal life (Marx, 2001). Anytime/anyplace computing by its very nature has the potential to intrude into personal time and space because boundaries between work and personal time and space become fuzzy (Davis, 2002).

Information Receiver

Information receiver in Figure 1 refers to the user's perception of the entity (person or organization) that receives and/or manipulates data about the user. Again, Adams and Sasse (2001) stress perception because is considered more relevant. Trust and security are the two main issues related to information receiver.

Trust: As shown in Figure 1, problems related to trust include accountability, transparency, individual participation, feedback, and collection and use limitations. Research from Hoffman, Novak and Peralta (1999) has shown that "almost 95% of consumers have declined to provide personal information to websites and 63% of these indicated this is because they do not trust those collecting the data". One of the main challenges of businesses is to determine how to gain and sustain the trust of its customers (Nah and Davis, 2002; Siau et al., 2003, 2004).

The users' perception of being vulnerable to or trusting the information receiver can enable or restrict self-expression and personal development within multimedia communications (Adams, 1999). To build and foster trust, businesses also have to assure customers that the information being gathered is limited to what is necessary to deliver the service that the customer values. Some companies are using the "opt in" policy, which means that the company guarantees that no personal information will be shared unless a customer provides the consent. The various uses of information by organizations that gather such information can be grouped into three main categories as follows (in order of increasing threats of privacy violation):

- § Use of information for closely related needs of the specific customer and the activity he/she performs with the company;
- § Used for marketing purposes – for example, special offers, but not directly related to the activities the client performs with the company;
- § Used by third parties or selling information to other companies.

The privacy policies must be clear and must make distinctions between different types of uses of information. Transparency is the key. Companies need to take responsibility for the use of the information they gather, not just by protecting it from outsiders, but also by building internal policies and guidelines that prevent the misuse of information. Culnan and Armstrong (1999) emphasize that procedural fairness serves as an intermediary to trust when interchangeable organizational agents exercise considerable delegated power on behalf of customers.

McKnight, Choudhury and Kacmar (2002) have identified four high-level constructs for trust in e-commerce: disposition to trust; institution-based trust; trusting beliefs; and trusting intentions. McKnight and colleagues (2002) define disposition to trust as "a general propensity to trust others, which can also influence an individual's beliefs and intentions towards a Web-based vendor". Institution-based trust is the sociological dimension of trust and it relates to an individual's perceptions of the institutional environment (i.e., the Internet in this case) (McKnight et al., 2002). Trusting beliefs refer to perceptions about the vendors' attributes that are beneficial to the truster (McKnight et al., 2002). Finally, trusting intentions relate to the willingness to depend or intention to depend on the trustee (McKnight et al., 2002). All these four types of trust are relevant for the study of u-commerce. In u-commerce applications, not only does each of these trust factors needs to be taken into account, but there might also be some interactions between them.

Security: The second issue related to privacy concerns is adequate security (Figure 1). Established trust among parties is only a necessary, but not sufficient, factor to create a safe-for-privacy environment. How about the third parties "sniffing" in between? How about the safety of the receiver's databases?

Siau, Lim, and Shen (2001) identify three components of security:

- § *Hostility:* The systems must provide enough mediated and stored information in order to prevent or track dishonest practices by merchants, customers, and other players.
- § *Information security*: Each party involved should be able to authenticate its counterparts and the senders of messages, keep the communication content confidential, and make sure that messages received are not tampered with.
- § *Vulnerability:* Security is even more vulnerable in the u-commerce environment since the data is generally transmitted wirelessly and can be accessed from multiple locations and types of devices.

Companies must set up their privacy policies and procedures to protect their databases, their networks and their applications. Langheinrich (2002) suggests that security should be provided based on the sensitivity of the data collected. An individual's privacy may be invaded if there is unauthorized access to personal information as a result of a security breach or absence of appropriate internal controls, or when the personal information provided for one purpose is reused for unrelated purposes without an individual's knowledge or consent (Culnan and Armstrong, 1999).

Information Usage

As shown in Figure 1, the third factor of the Adams' privacy model is information usage. Users create perceptions about how their information is used. Hence transparency is valued and can build trust among users. There is a trade-off between benefits and costs in disclosing information.

Benefits and Costs: The four characteristics (i.e., ubiquity, universality, uniqueness, and unison) provide the two chief benefits of u-commerce applications: convenience, and personalized and customized services. The key value drivers of u-commerce consist of: location (a true u-commerce application knows the context of your physical location as well as your profile of preferences and matches those with relevant services and products); voice (speech-to-text and text-to-speech processing are value drivers of u-commerce); alerts (which can notify people of a variety of events); and security (the removal of the human element from many transactions will be possible) (Accenture, 2002). The user will compare the perceived benefits to the perceived privacy threats and make decisions about personal information disclosure.

Therefore, the perceived risks for potential privacy invasion should be minimized. Companies can accomplish this by offering openness and transparency and there should be no secret and unknown record-keeping (Langheinrich, 2002). There

should also be transparency about the type of use for the information collected. Additionally, fair information practices and confidentiality assurance to users may alleviate the privacy concerns and encourage disclosure of personal information (e.g., Culnan and Armstrong, 1999).

Similarly, the privacy-protecting features of the technology used in u-commerce applications should be affordable and easy to use, and control-related variables should also be emphasized. If someone feels more in control of his/her environment, the information disclosure will be perceived as less threatening to privacy (Junglas and Spitzmüller, 2005). Increased control will lower the perceived risk by users since users can adjust the disclosure level according their needs and preferences. Another concern of users is the accuracy of data. Control can be increased by offering individual participation, where the subject of a record should be able to see and correct his/her record (Langheinrich, 2002).

Mayer, Davis and Schoorman (1995) see trust and risk as inseparably intertwined since trust involves the willingness to take risks. In general, by increasing trust, the perceived risk can be lowered, and vice versa - increased perceived risk will damage trust.

Context

With digitization, the capture, storage and transmission of information are easier. When referred at a later time, information may lose its context and as a consequence may be misinterpreted or be misunderstood. Since communications happen in a given context, the context plays an important role. When removed from the context, information is moving into another coordinative system and its evaluation becomes more complicated.

There is some interaction between the type of information revealed and familiarity with the person/entity receiving it as someone who is personally known to the user may incur higher privacy risks than a complete stranger (Adams, 1999). Moreover, Junglas and Spitzmüller (2005) suggest a number of user characteristics that need to be taken into account concerning privacy in the context of location-based services. These characteristics include locus of control, conscientiousness, neuroticism, and openness to experience.

The Three-Layer Model

The two privacy models described above are combined to provide a more comprehensive framework on privacy issues (Figure 1). These models complement one another by highlighting the different dimensions and levels related to privacy. Privacy has no rigid boundaries and it is not confined only to business or legislation (as depicted in the three-layer model, Figure 2). Figure 2 provides another view of the integrative framework presented in Figure 1. The micro-level in Figure 2 refers to the individual users' perspective (Adams, 1999), while the macro-level refers to Lessig's (1999) perspective on privacy. Each level is important in order to fully address privacy issues. Therefore, it is important for organizations to ground their knowledge, and consequently their solutions, regarding privacy issues on both perspectives. The knowledge at each level can serve as input to the other levels for appropriately responding to privacy issues.

CONCLUSION

This paper combines two models of privacy and discusses them in the context of u-commerce. It also elaborates on issues that will need to be addressed to relieve privacy concerns in u-commerce and to encourage u-commerce adoption. The perceived privacy factors model (Adams, 1999) and four forces model (Lessig, 1999) are combined, and the resulting framework can create synergy and provide guidelines for investigating the interactions among variables that relate to privacy issues at more than one level of analysis. For example, the way users perceive sensitivity of information – a micro-level factor – may depend on one or more macro-level factors such as social norms; in this case, what is perceived to be sensitive information for a society may not be perceived as such in another. On the other hand, social norms may change with time because of the way information sensitivity are perceived by users and handled by business organizations. The factors at the same level or at different levels of the models described above do not operate in isolation. They influence one another. Therefore, an integrative framework becomes important when addressing privacy issues and concerns in u-commerce.

There are a number of questions that future research needs to focus on: What and how should/could companies do to optimize the use of information they have gathered while preserving customers' privacy? What should/could be done to develop trust with consumers in the u-commerce era? In what ways is trust in a brick-and-mortar situation similar to and different from that in the u-commerce era? What other variables need to be taken into account? How can security be strengthened? Can security technologies used in online e-commerce applications be adapted for other u-commerce applications? What role does transparency play in the u-commerce scenario? How can privacy concerns in the u-commerce environment be addressed (e.g., from the business and organizational perspectives)? Can security be improved without

reducing the convenience of operations? Can information about the context be captured in such a way that it gives accurate information, while protecting people's privacy/anonymity?

This paper provides a comprehensive framework for future research relating to privacy in the u-commerce era. Additionally, it contributes to practice by highlighting and discussing a list of relevant issues in deploying u-commerce initiatives such as by retailers, service providers, device manufacturers or other organizations.

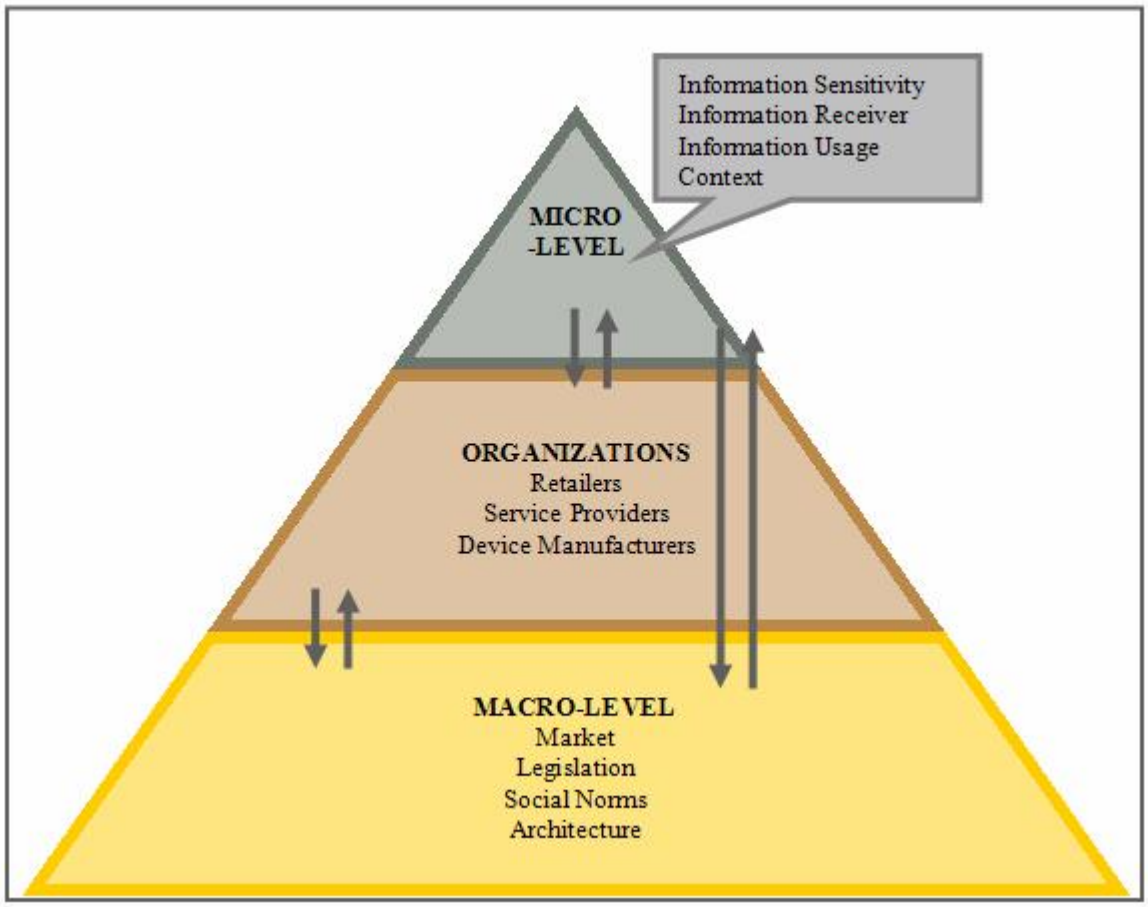

Figure 2: The Three-Layer Model

REFERENCES

1. Accenture (2002) The value drivers of uCommerce, Retrieved on September 2003 from http://www.accenture.com/xd/xd.asp?it=enwebandxd=services%5Ctechnology%5Cvision%5Cucom_valuedrivers.xml.
2. Adams, A. (1999) Users' perception of privacy in multimedia communication, *Proceedings of CHI' 99*, Pittsburgh, PA.
3. Adams, A. and Sasse, M. A. (2001) Privacy in multimedia communications: protecting users not just data, in *Proceedings of IMH HCI'01*, 49-64.
4. Avoine, G. (2004). Privacy issues in RFIF banknote protection schemes. Retrieved May 2, 2005, from http://www.vs.inf.ethz.ch/edu/SS2005/DS/papers/rfid/avoine-banknotes.pdf
5. Beldiman, D. (2002) An information society approach to privacy legislation: How to enhance privacy while maximizing information value, *Review of Intellectual Property Law*, 2, 1, 71-94.
6. Bloom, P.N., George, R.M. and Robert, A. (1994) Avoiding misuse of information technologies: legal and societal considerations, *Journal of Marketing*, 58, 1, 98-110.
7. Culnan, M.J. and Armstrong, P.K. (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, *Organization Science*, 10, 1, 104-115.

8. Davis, G.B. (2002) Anytime/anyplace computing and the future of knowledge work, *Communications of ACM*, 45, 12, 67-73.
9. Galanxhi-Janaqi, H. and Nah, F. (2004) U-Commerce: Emerging trends and research issues, *Industrial Management and Data Systems*, 104, 9, 744-755.
10. Grudin, J. (2002) Group dynamics and ubiquitous computing, *Communications of ACM*, 45, 12, 74-78.
11. Hann, I.H., Kui, K.L., Lee, T.S., and Png, I.P.L. (2002) Online information privacy: Measuring the cost-benefit trade-off, *Proceedings, 23rd International Conference on Information Systems* 2002.
12. Hoffman, D. L., Novak, T. P. and Peralta, M. (1999) Building consumer trust online, *Communications of the ACM*, 42, 4, 80-85.
13. Hong, J.I., Ng, J.D., Lederer, S. and Landay, J.A. (2004) Privacy risk models for designing privacy-sensitive ubiquitous computing systems, *DIS – Designing Interactive Systems*, August 1-4, Cambridge, Massachusetts.
14. Junglas, I.A. and Spitzmüller, C. (2005) A research model for studying privacy concerns pertaining to location-based services, *Proceedings of the 38th Hawaii International Conference on Systems Sciences.*
15. Junglas, I.A. and Watson, R.T. (2003) U-commerce: An experimental investigation of ubiquity and uniqueness, *Proceedings of the International Conference on Information Systems*, Seattle, WA, 414-426.
16. Langheinrich M. (2002) Privacy invasions in ubiquitous computing, *Privacy in Ubicomp'2002*, Göteborg, Sweden.
17. Langheinrich, M., Coroamã, V., Bohn, J. and Mattern, F. (2005) Living in a smart environment – Implications for the coming ubiquitous information society, *Telecommunications Review*, 15, 1. Retrieved on February 2005 from http://www.vs.inf.ethz.ch/publ/papers/sktelecom2005.pdf.
18. Laudon, K. C. (1996) Markets and privacy, *Communications of the ACM*, 39, 9, 92-104.
19. Lessig L. (1999). Code and Other Laws of Cyberspace, Basic Books, New York, NY.
20. Marx, G.T. (2001) Murky conceptual waters: the public and the private, *Ethics and Information Technology*, 3, 3, 157–169.
21. Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995) An integrative model of organizational trust, *Academy of Management Review*, 30, 709-734.
22. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334-359.
23. Minch, R. P. (2004). Privacy Issues in Location-Aware Mobile Devices. Paper presented at the 37th Hawaii International Conference on System Sciences, Big Island, HI, USA.
24. Nah, F. and Davis, S. (2002) HCI research issues in e-commerce, *Journal of Electronic Commerce Research*, 3, 3, 98-113. Available http://www.csulb.edu/web/journals/jecr/issues/20023/paper1.pdf
25. Schapp, S. and Cornelius R.D. (2001) U-Commerce: Leading the world of payments. white paper, Retrieved on December 2002 from http://www.corporate.visa.com/av/ucomm/u_whitepaper.pdf
26. Siau K., Lim, E. and Shen, Z. (2001), Mobile commerce: Promises, challenges, and research agenda, *Journal of Database Management*, 12, 3, 4-13.
27. Siau, K. and Shen, Z. (2003a) Building customer trust in mobile commerce, *Communications of the ACM*, 46, 4, 91-94.
28. Siau, K. and Shen, Z. (2003b) Mobile communications and mobile services. *International Journal of Mobile Communications*, 1, 1/2, 3-14.
29. Siau, K., Sheng, H. and Nah, F. (2003) Development of a framework for trust in mobile commerce. *Proceedings of the Second Annual Workshop on HCI Research in MIS (HCI/MIS'03)*, Seattle, Washington, USA, December 2003, 85-89. Extended abstract available at: http://cte.rockhurst.edu/sighci/icis_2003/HCI03_14.pdf .
30. Siau, K., Sheng, H., Nah, F. and Davis, S. (2004) A qualitative investigation on consumer trust in mobile commerce, *International Journal of Electronic Business*, 2, 3, 283-300.
31. Varian, H. (1997) Economic aspects of personal privacy, in U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*, June 1997.
32. Warren, S. and Brandeis, L. (1980) The Right to Privacy, *Harvard Law Review*, 4, 193-220.
33. Watson R.T., Pitt L.F., Berthon P. and Zinkhan G.M. (2002). U-Commerce: Expanding the universe of marketing, *Journal of the Academy of Marketing Science*, 30, 4, 333-348.