8-2005

Privacy issues in the era of ubiquitous commerce

Holtjona GALANXHI

Fiona Fui-hoon NAH
Singapore Management University, fionanah@smu.edu.sg

Citation

GALANXHI, Holtjona and NAH, Fiona Fui-hoon. Privacy issues in the era of ubiquitous commerce. (2005). *Proceedings of the 11th Americas Conference on Information Systems, Nebraska, USA, 2005 August 11-15*. 16, (3), 222-232.

Available at: https://ink.library.smu.edu.sg/sis_research/9519

Privacy Issues in the Era of Ubiquitous Commerce

HOLTJONA GALANXHI AND FIONA FUI-HOON NAH

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 businesses: increased convenience as well as more personalized and customized services. However, u-commerce will also bring emerging issues such as a greater degree of privacy concerns that will impact individual users, companies and society at large. This paper proposes and elaborates on a conceptual framework for privacy in the u-commerce era. This framework is developed based on Lessig's macro-level perspective and Adams' micro-level perspective. Using this framework, privacy issues related to u-commerce are discussed and future research directions are presented.

Keywords: ubiquitous commerce, u-commerce, privacy, integrative framework

INTRODUCTION

Ubiquitous commerce, also referred to as 'u-commerce', 'ultimate commerce' or 'über-commerce', extends traditional commerce 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 has the potential to create a completely new environment in business (Galanxhi-Janaqi and Nah 2004). U-commerce enables a continuous, seamless stream of communication, content and service exchanges among businesses, suppliers, employees, customers and products (Watson *et al.* 2002). Through the convergence of physical and digital means, higher levels of convenience and value are created at the expense of increased privacy concerns (i.e., personal information is captured, transmitted and distributed to provide u-commerce services).

The objectives of this paper are two-fold: (1) to integrate existing literature related to privacy in u-commerce; and (2) to provide a framework for explaining and understanding privacy issues in u-commerce. First, the concept of u-commerce, its characteristics, and emerging challenges of u-commerce applications are discussed. Second, two models of privacy that are relevant to u-commerce are described. Lastly, an integrative framework is presented. Based on the framework, suggestions and guidelines for research and practice are provided.

U-COMMERCE CHARACTERISTICS, ISSUES AND CHALLENGES

U-commerce refers to 'the use of ubiquitous networks to support personalized and uninterrupted communications and transactions between a firm and its various stakeholders to provide a level of value over, above, and beyond traditional commerce' (Watson *et al.* 2002). U-commerce involves five components, viz: electronic (e-commerce), wireless/mobile (m-commerce), television (t-commerce), voice (v-commerce), and silent commerce (s-commerce), and its full realization is greater than the simple sum of its components. This section discusses the characteristics of u-commerce and identifies issues and challenges in u-commerce.

Watson *et al.* (2002) present four characteristics of u-commerce: ubiquity, universality, uniqueness and unison. The first characteristic is *ubiquity*. Computers will be everywhere and every device will be connected to the Internet. The

Authors

Holtjona Galanxhi
(hgalanxh@unlnotes.unl.edu) is a forth year doctoral student of MIS at the University of Nebraska-Lincoln. Her research interests include ubiquitous and mobile e-commerce, silent commerce, privacy issues, HCI, and the strategic role of IS in organizations.

Fiona Fui-Hoon Nah
(fnah@unlnotes.unl.edu) is an Associate Professor of MIS at the University of Nebraska-Lincoln. She has published widely. Her research interests include ubiquitous and mobile e-commerce, HCI, computer-supported collaborative work, and theory building in information systems research.

Copyright © 2006 Electronic Markets
Volume 16 (3): 222-232. www.electronicmarkets.org DOI: 10.1080/10196780600841894
Routledge Taylor & Francis Group

omnipresence of computer chips will make them 'invisible', as people will no longer notice them (Watson *et al.* 2002). *Universality* is the second characteristic of u-commerce. Universality eliminates the problems of incompatibility caused by the lack of standardization such as the use of mobile phones in different networks. A universal device will make it possible to stay connected at any time and any place. Another characteristic of u-commerce is *uniqueness*. Uniqueness means that the information provided to users can be customized to their context and needs at specific time and place. The last characteristic of u-commerce is *unison*, which aggregates the aspects of application and data into one construct. Unison means that data is integrated and is uniform across multiple applications, and users have a consistent view of the information regardless of the device used (Junglas and Watson 2003). In the u-commerce environment, it is possible to integrate various communication systems such that there is a single interface or connection point to these systems.

Schapp and Cornelius (2001) identify three global phenomena that accelerate the growth of u-commerce: pervasiveness of technology (the explosive growth of nanotechnology and the continuing capital investments); growth of wireless networks (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 added capacity and enhanced functionality).

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 is derived 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 *et al.* 1994). Mobile commerce faces the same problems troubling e-commerce, plus a few of its own (Siau and Shen, 2003a, 2003b; Siau *et al.* 2003, 2004). These concerns are even greater for u-commerce applications. For example, according to CNN news reports in February 2005, u-commerce applications involving the use of Radio Frequency Identification (RFID) tags have been implemented in some elementary schools to bring benefits such as greater security for children in their school compound; however, these applications have been strongly objected by some parents of these children because they raise privacy concerns.

Roussos and Moussouri (2004) investigate consumer perceptions on a retail u-commerce application called the MyGrocer project. Their study showed that although the proposition of MyGrocer attracted substantial interest among consumers, the most controversial aspect of the system was the intrusion of private space and time (i.e., continuous monitoring of consumption, frequent commercial communications, and data mining for personalization). 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). Furthermore, new social issues arise as these u-commerce applications must mesh well with natural social behaviours or they will either 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). Similarly, employers can track the movement of their employees and know their whereabouts at any time and any place, thus raising privacy concerns.

Organizations that address individuals' privacy concerns arising from u-commerce applications will be one step ahead of their competitors. Society, businesses and individuals can benefit from u-commerce if privacy issues are properly handled. The following section reviews the privacy literature, discusses two models of privacy relevant to u-commerce and integrates these two perspectives into a single framework.

FRAMEWORK FOR PRIVACY IN U-COMMERCE

One of the major concerns related to u-commerce, and the IT evolution in general, is privacy. Laudon and Traver (2001: 467) define privacy as 'the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state'.

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 goal is to give people the power to control the distribution of information about themselves (Langheinrich *et al.* 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 refers to 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).

Privacy is a relative concept because what is considered private in one culture may not be considered private in another. Even individuals from the same culture have different tolerance levels of privacy invasion. To recognize the multifaceted, polysemic and contradictory nature of privacy, it is necessary to not only take a technological perspective but to also look at other aspects of the stakeholders involved (Dholakia and Zwick 2004). Favourable themes, such as those referring to the omni-powerful consumer and the ultra-productive worker, that are made possible by ubiquitous applications are challenged by themes relating to privacy and workers' surveillance (Dholakia and Zwick 2004). The social and cultural contradictions of ubiquitous technologies can be viewed at three levels (Dholakia and Zwick 2004): individual, social, and global (Table 1). On one hand, anywhere-anytime technologies allow for instant and ubiquitous access to information. On the other hand, they cause a near-total loss of privacy. Similarly, although they can promote unprecedented work productivity and convenient consumption experiences, they can also bring new problems such as an increased difficulty in separating work time from leisure or private time.

Privacy concerns in u-commerce are noticeably higher than in other types of commerce. U-commerce not only inherits the privacy concerns of all of its components (e-commerce, m-commerce, v-commerce, etc.), but it also raises new privacy concerns caused by the richness of the combined personal information from these components. Such information can be easily integrated across different multiple sources and shared among third (often unknown) parties. Although location-based services can be beneficial to users (e.g., by providing customized and personalized services), they can also bring additional privacy concerns. Avoine (2004), for example, describes how the RFID banknote protection schemes compromise the privacy of bearers of banknotes.

Privacy may be the biggest barrier to the long-term success of ubiquitous computing applications (Hong *et al.* 2004). Privacy concerns existed before the rise of technologies and they are not solely related to technology. With each new technology, the threats to privacy increase. 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) explain the controversial issue of privacy in ubiquitous computing applications as follows: First, the tremendous opportunities provided by the convergence and increasing widespread deployment of sensors, wireless networking and devices of all form factors facilitate the creation of systems that can improve safety, efficiency and convenience. Second, negative media coverage raises general unease over the potential for abuse. Hence, there is fear over a potential lack of control and desire for privacy-sensitive ubiquitous applications.

In reviewing the literature, we identify two models of privacy that are relevant to u-commerce: Lessig's (1999) Socio-Level Privacy model and Adams' (1999) Users' Perceived Privacy Factors model. The Lessig's model conceptualizes privacy from a macro-environment perspective while the Adams' model views privacy from a micro or individual level. Table 2 summarizes these two models, the levels of their analysis, and their main factors relating to privacy. Each model addresses parts of the privacy problem in u-commerce from different (macro vs. micro) perspectives.

An integrative framework is presented in Figure 1 to highlight the main privacy factors (e.g., information sensitivity) and their related issues at both the macro and micro levels. The framework combines the key factors in both Lessig's (1999) Socio-Level Privacy model and Adams' (1999) Users' Perceived Privacy Factors model, and highlights the relationships among them. An integrative view is necessary because the different levels are not isolated. Both the micro- and macro-level considerations must be taken into account in order to better understand privacy concerns in u-commerce. Next, the integrative framework will be explained in detail.

Table 1. Contesting views of technological impact

Sphere of contradiction	*Dominant view*	*Contesting view*
Individual	Empowering	Threatening
Social	Liberating	Confining
Global	Equalizing power	Fostering power inequities

Source: Adapted from Dholakia and Zwick, 2004

Table 2. Lessig's and Adams' privacy models

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

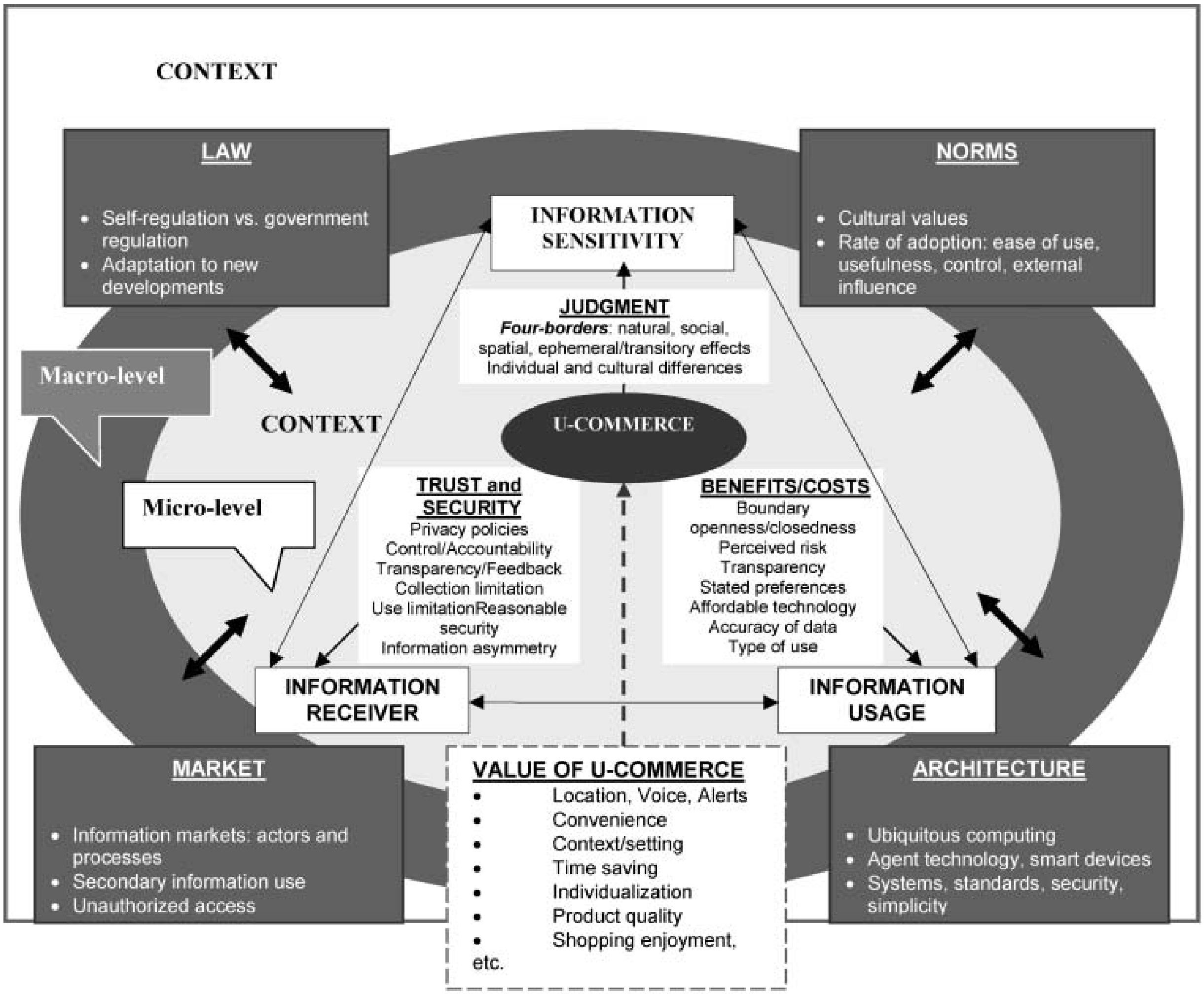

Figure 1. An integrative framework for privacy in u-commerce

Lessig's Socio-Level Privacy model

Lessig (1999) views privacy as a dynamic interaction between legal rules, social norms, market forces and code. 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) law; (2) market; (3) social norms; and (4) architecture (see Figure 1). Lessig examines how the relationships between these four forces regulate people's behaviour and provide explanations on how these forces work in combinations. Lessig also explains how improvements in technology can dramatically alter the composite constraint on people's conduct. According to Lessig, all four forces will need to be considered to solve the information privacy problem as these forces do not operate independently; they are interdependent. These four forces will be discussed next.

Law/legislation. Two regulatory philosophies on privacy have emerged – the US model of self-regulation and the EU model of government regulation. The US model views privacy as both property and commodity, while the EU model views privacy as a basic civil right (Zwick and Dholakia 2001). Consequently, the approaches for handling privacy issues have been different depending on the conception adopted. The US model encourages voluntary actions by industry groups or certifying agencies, while the EU emphasizes the creation of a legal framework of privacy protection. The main problem with the self-regulatory approach is the conflict of interest between information collectors and the party/parties whose information is collected. There is an inherent tension between u-commerce users' 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 them.

The regulatory approach is also problematic for two reasons. First, the concept of privacy varies for different individuals, groups, and societies. Second, this approach sees privacy as static in time or at least as foreseeable; but in a world of fast technological developments, people's attitudes may change with time as they see more benefits or risks arising from new applications. Consequently, legislation needs to adapt quickly to changes in u-commerce development.

Market. Although the legal base protecting privacy has evolved over nearly 100 years in the US, most people feel that their privacy level has declined (Laudon 1996). The reason might be that most of the legislation has failed to keep pace with technological developments that affect privacy. In order to reduce privacy invasion, the regulation approach should not be left to work by itself. It is necessary to develop solutions that rely on more powerful and less wasteful mechanisms such as markets (Laudon 1996). According to Laudon, privacy invasion has partially resulted from market failures to prevent information collected to be used without individuals' consent. While the legal perspective aims at developing a legal base to protect privacy, the market perspective aims at allowing the supply and demand forces to determine the acceptable levels of information collection, use and sharing. Instead of imposing stronger privacy laws, Laudon advocates that the solution is to strengthen the current information markets to increase fairness. He suggests the creation of a National Information Market (NIM), where information is bought and sold at a market price reflected by equilibrium between supply and demand. This market would be the only legal place where information used for secondary purposes is exchanged and where unauthorized use of information (which is the greatest threat to individual privacy) can be minimized (Laudon 1996).

Social norms. Claims about privacy are strongly supported by cultural assumptions (Laudon 1996). It is difficult, however, to translate the general cultural value statements and individual claims into law, because in all societies there are competing claims by different parties (e.g., government, private organizations) for the sake of national security, public health and other valued social ends.

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 emails may not be illegal, but it may be regarded as socially unacceptable. In such cases, companies may decide to create policies and procedures although they may not be required by law. Social norms are a cultural phenomenon. Companies that engage in u-commerce initiatives need to take social norms into account. Social norms may influence the way devices are used in a given society and the need for 'humanization of devices' can also differ across 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 achieve it, and the architecture/technology provides him with a means to accomplish the goal (Lessig 1999). Privacy concerns could be overcome by using technical solutions. For example, 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 need to be addressed (Schapp and Cornelius 2001). Information technology can play multiple roles in addressing privacy; it can form part of the context, transform boundaries, mediate presentations etc. (Palen and Dourish 2003).

Lessig's model is appropriate for analysing privacy issues from a macro-environment perspective (see Figure 1). When an individual decides to disclose personal, private and/or sensitive information in a given situation, he/she makes this decision based on the evaluation of four forces – law, social norms, market and architecture/technology. However, perceptions on privacy at the individual (micro) level are also critical in making informed decisions. Next, we discuss privacy at the individual level, based on Adams' model.

Adams' Perceived Privacy Factors model

In a u-commerce environment, obtaining information about 'who, where, what and how' becomes easier since u-commerce applications track and share information to provide the services (e.g., location-based services). As shown in Figure 1, Adams (1999) identifies three main factors influencing privacy – information sensitivity, information receiver and information usage.

Information sensitivity. Information sensitivity refers to the u-commerce user's perception of the data being transmitted and the information as interpreted by the receiver (Adams and Sasse 2001). It relates to the importance of information and the potential consequences if the information is shared with other parties. Information sensitivity is relevant to both individuals and organizations (Adams 1999).

Users assess information sensitivity by means of making their best *judgements* (Adams and Sasse 2001). Sensitivity of information depends on the perception of the people involved and the importance and relevance of the information. Perceived sensitivity levels are affected by one's perception of the data transmitted and how public or private the broadcast 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 (see Figure 1) that can be violated:

1. *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, it is possible to penetrate natural borders, such as walls and even geographical distances.
2. *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 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.
3. *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.
4. *Borders due to ephemeral or transitory effects* relate to the assumption that most of the events happening in our life 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, private communications made during instant messaging is considered transitory by most. However, it is possible for these accounts to be recorded (without consent from the users) and possibly made public at a later date. A related concern is that these accounts could be interpreted completely out of context at a different time.

U-commerce makes surveillance less expensive and creates new opportunities for each of the above border crossings. Furthermore, ubiquitous computing applications tend to remove the desirable boundaries between work and personal life (Davis 2002; Marx 2001).

Adams and Sasse (2001) stress 'perception' in viewing privacy 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. People often find themselves trading off some degree of privacy to gain something they value (Acquisti and Grossklags 2005; Dinev and Hart 2003). For example, one may agree to disclose location information via the GPS system of a mobile phone so assistance is available in case of an emergency.

Concerning privacy perceptions, Privacy & American Business (P&AB) identifies three categories of people (Taylor, 2003):

1. Privacy fundamentalists – people who feel that they have lost a lot of privacy and are strongly resistant to further privacy erosions;
2. Privacy unconcerned – people who have no real concerns and anxiety about privacy and how their information is being collected and used; and
3. Privacy pragmatists – people who have strong concerns about privacy, but who are willing to allow some degree of access and use of their information as long as they understand the reasons for its use and see tangible benefits from its use.

Harris Interactive Poll found that the number of privacy pragmatists has increased from 54% in 1999 to 64% in 2003; the number of privacy unconcerned has declined from 22% in 1999 to 10% in 2003; and the number of privacy fundamentalists has remained about the same from 24% in 1999 to 26% in 2003 (Taylor 2003).

People have different perceptions and beliefs about privacy. Therefore, their responses to privacy issues raised by u-commerce applications can vary substantially. Historical and cultural differences can influence information sensitivity. For example, Europeans tend to take the perspective of 'fundamentalists', while in Africa, the Middle East, India, China and Southeast Asia, privacy protections are almost non-existent because of the relatively larger proportion of 'unconcerned' (Cline 2005). People in the US, on the other hand, tend to take the perspective of 'pragmatists' by practicing free commerce with no or little government interference. Although there are noticeable differences across regions and countries, in general, all three segments can be found in any region or country. Therefore, it is necessary to know more about the customers and the segment(s) they belong to (e.g., 'fundamentalist', 'unconcerned', 'pragmatist') in order to provide users with appropriate control of their information.

Information receiver. Information receiver refers to the u-commerce user's perception of the entity (person or organization) that receives and/or manipulates data about the user. Trust and security are two main issues. If the receiver is perceived as trustworthy and the data are kept secured, then concerns for privacy may be alleviated.

Problems related to *trust* include accountability, transparency, feedback, and collection and use limitations. Hoffman *et al.* (1999) have 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 their customers (Nah and Davis 2002; Siau *et al.* 2003, 2004).

The user's perception of being vulnerable to the information receiver can enable or restrict self-expression and personal development with electronic communications (Adams 1999). To build and foster trust, businesses have to assure customers that the information being gathered is limited to that necessary to deliver the service. 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 gathering such information can be grouped into three main categories (listed in order of increasing threats of privacy violation):

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

Privacy policies must be clear and must make distinctions between different types of uses of information. Transparency is very important to users, because they need to know what is happening to their personal data and that companies are responsible about the use of the information they gather. Elliott and Cunningham (2005) identify three main issues concerning the data organizations collect: information quality (i.e., data should be filtered, aggregated and entered without errors); information controls (i.e., determine access rights and compliance with legal and privacy restrictions); and information interpretation (i.e., consistency and transparency in the use of information by organizations).

Furthermore, there are various issues related to privacy policies and individuals' stated preferences. Schwaig *et al.* (2005) studied privacy and fair information practices of Fortune 500 companies and found that organizations were only partially complying with the federal standards. Organizations were also more concerned about the existence of a privacy policy than using the privacy policy as a communicative action means (i.e., content and enforcement). Additionally, there is often a discrepancy between users' stated preferences and their actual behaviours. For example, Berendt *et al.* (2005) find that given the right circumstances (e.g., if an online exchange is entertaining and appropriate benefits are offered in return for information revelation), users often forget about their stated preferences by revealing their private information willingly. Another finding from this study indicated that product category and type of privacy statements had no significant impact on users' behaviour. These findings have implications on addressing privacy issues in u-commerce applications – i.e., to impact users' behaviour, additional means such as Platform for Privacy Preferences (P3P) may need to be used.

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 *et al.* (2002) identify four high-level constructs for trust in e-commerce: disposition to trust; institution-based trust; trusting beliefs; and trusting intentions. McKnight *et al.* (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 (such as the Internet or wireless environment). Trusting beliefs refer to perceptions about the vendors' attributes that are beneficial to the truster. Finally, trusting intentions relate to the willingness or intention to depend on the trustee. Similarly, these four types of trust are also relevant for the study of u-commerce.

Another issue related to privacy concerns is *security* (see Figure 1). Establishing 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 *et al.* (2001) identify three components of security:

1. *Hostility*: The systems must provide enough mediated and stored information in order to prevent or track dishonest practices by merchants, customers and other players.
2. *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.
3. *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, networks and 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 security breaches or absence of appropriate internal controls, or when the personal information provided for one purpose is reused for unrelated purposes without the individual's consent (Culnan and Armstrong 1999).

Samuelson (2000) and Varian (1997) show that asymmetric information (i.e., one party taking part in a transaction having more/better information than the other) can influence market, social and legal forces by impeding these forces from being applied to achieve privacy goals (Jiang 2002). The Principle of Minimum Asymmetry requires developing privacy-aware systems that minimize the asymmetry of information between the owners and collectors of data (Jiang 2002).

Information usage. The third factor of Adams' privacy model is information usage. Transparency in information usage is valued and can build trust in users. Hann *et al.* (2002) show that users trade off benefits and costs in disclosing personal information.

The four characteristics (i.e., ubiquity, universality, uniqueness and unison) provide the two main benefits of u-commerce applications: convenience, and personalized and customized services. 'We all love services that save us time and money' (Imhoff 2005) such as information personalization and customization. The key value drivers of u-commerce are: 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); alerts (notify people of a variety of events); and security (the removal of human elements from transactions) (Accenture 2002). A user will compare perceived benefits to perceived privacy threats in making decisions about personal information disclosure.

Altman (1975) propose a model that views privacy as a dialectic and dynamic boundary regulation process. In this view, individuals seek to optimize their accessibility along an openness/closedness spectrum (Palen and Dourish 2003). First, privacy is seen as a dialectic process where it is conditioned not only by people's expectations and experiences but also by other people with whom they interact. Second, privacy is seen as a dynamic process since it is under continuous boundary negotiation and management. Boundaries change dynamically as the context changes and they reflect the tension between conflicting goals (Palen and Dourish 2003).

Privacy management involves satisfying a number of needs and balancing a number of tensions (Palen and Dourish 2003). For individuals, it involves balancing the need for privacy with getting the benefits from u-commerce applications. For organizations, privacy management means balancing the need to obtain the necessary information to provide u-commerce products and services and satisfy their marketing needs while safeguarding individuals' privacy. In the US privacy model, the consumer and the marketer are 'homo economicus' and exchange partner entities (Zwick and Dholakia 2001). Research (e.g., Hann *et al.* 2002) has shown that individuals' concerns about privacy are not absolute as they are willing to trade off privacy concerns for economic benefits. Roussos and Moussouri (2004) found that in their u-commerce application (MyGrocer project), the implications of different trade-offs between more advanced functionality and privacy protection were a core issue for the design of the system. However, a related problem is that often the benefits resulting from u-commerce applications are indirect and invisible to the consumers, and consequently easily discounted (Roussos and Moussouri 2004).

Saeed and Leitch (2003) define privacy risk as 'the buyer's perception of risk towards exposure of sensitive information and misuse of sensitive information on their trading activities'. They have identified privacy policies (disclosure of information collected and its probable uses) as the only control tool to reduce perceived risk by the consumers. These privacy policies can be self-developed or they can be third party solutions such as eTRUST and Better Business Bureau (BBB) (Saeed and Leitch 2003). Imhoff (2005) suggests that the key to successful privacy policies is finding the balance between the individual's need for privacy and the public's need to understand who this individual is.

If individuals perceive that the privacy policies are enforced by organizations, the perceived risk will be lower and they will be more willing to disclose information that is necessary to provide a given u-commerce service. Therefore, it is important to make the benefits more tangible and visible to alleviate the perceived risks for potential privacy invasion. 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(s) 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 (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).

Zwick and Dholakia (2004) argued that current organizational strategies to maintain control over one's identity in the electronic marketplace are inadequate, because they 'are based on an obsolete ontological distinction between the "real" customer and his or her digital representation'. Instead, they suggest that consumers should be given access to companies' customer databases so they can maintain a sense of control over their identities in the marketplace (Zwick and Dholakia 2004).

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 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 because 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 (locus of control, conscientiousness, neuroticism and openness to experience) that need to be taken into account to assess privacy in the context of location-based services.

Value of u-commerce. When deciding whether to disclose personal information, a user compares the value to be received from a u-commerce application with the cost of decreased privacy (Acquisti and Grossklags 2005, Dinev and Hart, 2003). The purpose of u-commerce is to create higher levels of convenience and added value through the convergence of physical and digital means. Location, voice and alerts have been identified as key value drivers for u-commerce (Accenture 2001). A true u-commerce application knows the context of your physical location as well as your profile of preferences. The location and personal preferences are then matched with relevant services and products. In order to overcome current problems with user interface on mobile devices (e.g., small screens and keypads), voice capabilities — speech-to-text and text-to-speech – are vital value drivers of u-commerce. As applications become ubiquitous, new opportunities for value creation will emerge such as providing 'intelligent' rather than 'pre-programmed' alerts. These value drivers set the context for increased convenience. Sheng *et al.* (2005) examine the values of u-commerce and identified ten fundamental objectives: maximize convenience; maximize time saving; maximize reliability of services; maximize security; maximize privacy; maximize individualization; maximize product quality; maximize safety/health; minimize cost; and maximize shopping enjoyment. When benefits are more visible and valuable, and protection of information privacy is strictly enforced, individuals would be more willing to share their personal information.

CONCLUSION

This paper reviews two models of privacy and discusses them in the context of u-commerce. These two models complement one another by highlighting the different dimensions and levels related to privacy. The paper 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 integrated into a framework, which provides guidance for setting privacy practices and highlights directions for future research in u-commerce.

Privacy has no rigid boundaries and it is not confined only to one single perspective (i.e., micro vs. macro). 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 one 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 is perceived by different 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, it is important for organizations to ground their knowledge, and consequently their solutions, regarding privacy issues on both (macro and micro) perspectives.

An integrative framework becomes important when addressing privacy issues and concerns in u-commerce. Future research may investigate the relationships among the identified privacy factors, such as the impact of culture (i.e., different social norms) on u-commerce adoption and diffusion, or the impact of organizations' sensitivity to consumers' privacy concerns on their success in deploying u-commerce applications. Questions that will need to be answered in future research include: What and how should/could companies optimize the use of information they have gathered while preserving customers' privacy? How can trust with consumers be fostered in the u-commerce era? In what ways is trust in an e-commerce context 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 u-commerce applications? How can privacy concerns in the u-commerce environment be addressed (e.g., from the business and organizational perspectives)? Can information about the context be captured in such a way that it protects people's privacy/anonymity while it increases transparency? Certainly, the answers to these questions may entail multiple empirical studies to test and assess various aspects of the framework.

In conclusion, the integrative framework not only provides a comprehensive list of factors to assess and understand privacy concerns in u-commerce, but it also provides suggestions and directions for future research. The integrative framework provides guidance in two ways: First, it identifies and elaborates on the privacy factors and the relevant issues that need to be considered in the context of u-commerce. Second, the framework presents the multi-faceted nature of privacy issues and highlights the multitude of perspectives to consider when implementing privacy policies or novel u-commerce applications. In future research, quantitative analyses of privacy assessments can be carried out and these assessments can be compared across multiple settings and contexts.

References

Accenture (2001) 'The Unexpected eEurope', online at: http://www.accenture.com/NR/rdonlyres/C102FB70-D0DF-4D36-9FF2-254AC2CF14EF/0/exec_summary.pdf (accessed 25 March 2006).

Accenture (2002) 'The Value Drivers of uCommerce', online at: http://www.accenture.com/xd/xd.asp?it=enwebandxd=services%5Ctechnology%5Cvision%5Cucom_valuedrivers.xml (accessed 30 September 2003).

Acquisti, A. and Grossklags, J. (2005) 'Privacy and Rationality in Individual Decision Making', *IEEE Security and Privacy* 3(1): 26–33.

Adams, A. (1999) 'Users' Perception of Privacy in Multimedia Communication', *Proceedings of CHI' 99*, Pittsburgh, PA.

Adams, A. and Sasse, M. A. (2001) 'Privacy in Multimedia Communications: Protecting Users Not Just Data', *Proceedings of IMH HCI'01*, 49–64.

Altman, I. (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*, Monterey, CA: Brooks/Cole.

Avoine, G. (2004) 'Privacy Issues in RFID Banknote Protection Schemes', online at : http://www.vs.inf.ethz.ch/edu/SS2005/DS/papers/rfid/avoine-banknotes.pdf (accessed 25 March 2006).

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.

Berendt, B., Günther, O. and Spiekermann, S. (2005) 'Privacy in e-commerce: Stated Preferences vs. Actual Behavior', *Communications of the ACM* 48(4): 101–6.

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.

Cline, J. (2005, May 16) 'Global CRM *requires different privacy approaches*', *ComputerWorld*, online at: http://www.computerworld.com/printthis/2005/0,4814,101766,00.html (accessed 25 March 2006).

Culnan, M. J. and Armstrong, P. K. (1999) 'Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation', *Organization Science* 10(1): 104–15.

Davis, G. B. (2002) 'Anytime/anyplace Computing and the Future of Knowledge Work', *Communications of ACM* 45(12): 67–73.

Dholakia, N. and Zwick, D. (2004) 'Cultural Contradictions of the Anytime, Anywhere Economy: Reframing Communication Technology', *Telematics and Informatics* 21(2): 123–41.

Dinev, T. and Hart, P. (2003) 'Privacy Concerns and Internet Use – A Model of Trade-off Factors', *Academy of Management Meeting*, Seattle.

Elliott, T. and Cunningham, D. (2005) 'The Burden of Trusted Information', *DM Review*, 18–33.

Galanxhi-Janaqi, H. and Nah, F. (2004) 'U-Commerce: Emerging Trends and Research Issues', *Industrial Management and Data Systems* 104(9): 744–55.

Grudin, J. (2002) 'Group Dynamics and Ubiquitous Computing', *Communications of ACM* 45(12): 74–8.

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 of the 23rd International Conference on Information Systems.*

Hoffman, D. L., Novak, T. P. and Peralta, M. (1999) 'Building Consumer Trust Online', *Communications of the ACM* 42(4): 80–5.

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, MA.

Imhoff, C. (2005) 'Can You Keep a Secret? Some Companies Can and Apparently Some Can't!', *DM Review*: 48–51.

Jiang, X. (2002) 'Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social', *Paper presented at the Ubicomp 2002 Workshop on Socially Informed Design of Privacy-Enhancing Solutions in Ubiquitous Computing*, Göteborg, Sweden.

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.*

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: 414–26.

Langheinrich, M. (2002) 'Privacy Invasions in Ubiquitous Computing', *Privacy in Ubicomp'2002*, Göteborg, Sweden.

Langheinrich, M., Coroamă, V., Bohn, J. and Mattern, F. (2005) 'Living in a Smart Environment – Implications for the Coming Ubiquitous Information Society', *Telecommunications Review* 15(1), online at: http://

www.vs.inf.ethz.ch/publ/papers/sktelecom2005.pdf (accessed 25 March 2005).

Laudon, K. C. (1996) 'Markets and Privacy', *Communications of the ACM* 39(9): 92–104.

Laudon, K. C. and Traver, C. (2001) *E-commerce: Business, Technology, Society*, Boston, MA: Addison-Wesley.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*, New York: Basic Books.

Marx, G. T. (2001) 'Murky Conceptual Waters: The Public and the Private', *Ethics and Information Technology* 3(3): 157–69.

McKnight, D. H., Choudhury, V. and Kacmar, C. (2002) 'Developing and Validating Trust Measures for e-commerce: An Integrative Typology', *Information Systems Research* 13(3): 334–59.

Nah, F. and Davis, S. (2002) 'HCI Research Issues in e-commerce', *Journal of Electronic Commerce Research* 3(3): 98–113, online at: http://www.csulb.edu/web/journals/jecr/issues/20023/paper1.pdf.

Palen, L. and Dourish, P. (2003) 'Unpacking "Privacy" for a Networked World', *Proceedings of the SIGCHI conference on Human Factors in Computing Systems (CHI2003)*, Fort Lauderdale, FL.

Robins, K. and Webster, F. (1999) *Times of the Technoculture*, London and New York: Routledge.

Roussos, G. and Moussouri, T. (2004) 'Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce', *Personal and Ubiquitous Computing* 8(8): 416–29.

Saeed, K. and Leitch, R. A. (2003) 'Controlling Sourcing Risk in Electronic Marketplaces', *Electronic Markets* 13(2): 163–72.

Samuelson, P. (2000) 'Privacy as Intellectual Property?', *Stanford Law Review* 52: 1125–71.

Schapp, S. and Cornelius, R. D. (2001) 'U-Commerce: Leading the World of Payments', online at: http://corporate.visa.com/md/dl/documents/downloads/u_whitepaper.pdf (accessed 25 March 2006).

Schwaig, K. S., Kane, G. C. and Storey, V. C. (2005) 'Privacy, Fair Information Practices and the Fortune 500: The Virtual Reality Compliance', *The Data Base for Advances in Information Systems* 36(1): 49–63.

Sheng, H., Nah, F. and Siau, K. (2005) 'Values of Silent Commerce: A Study Using Value-Focused Thinking Approach', *Proceedings of the Eleventh Americas Conference on Information Systems*, Omaha, NE, 11–14 August: 1869–81.

Siau, K., Lim, E. and Shen, Z. (2001) 'Mobile Commerce: Promises, Challenges, and Research Agenda', *Journal of Database Management* 12(3): 4–13.

Siau, K. and Shen, Z. (2003a) 'Building Customer Trust in Mobile Commerce', *Communications of the ACM* 46(4): 91–4.

Siau, K. and Shen, Z. (2003b) 'Mobile Communications and Mobile Services', *International Journal of Mobile Communications* 1(1/2): 3–14.

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, WA, December 2003: 85–9, (extended abstract online at: http://cte.rockhurst.edu/sighci/icis_2003/HCI03_14.pdf).

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.

Taylor, H. (2003) 'Most People are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade it off for Other Benefits', online at: http://www.harrisinteractive.com/harris_poll/index.asp?PID=365 (accessed 25 March 2006).

Varian, H. (1997) 'Economic Aspects of Personal Privacy', in US Department of Commerce, *Privacy and Self-Regulation in the Information Age*, June 1997.

Warren, S. and Brandeis, L. (1980) 'The Right to Privacy', *Harvard Law Review* 4: 193–220.

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): 333–48.

Zwick, D. and Dholakia, N. (2001) 'Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right', *Electronic Markets* 11(2): 116–20.

Zwick, D. and Dholakia, N. (2004) 'Whose Identity is it anyway? Consumer Representation in the Age of Database Marketing', *Journal of Macromarketing* 24(1): 31–43.