

***Portable Privacy:
Mobile Device Adoption***

Joseph H. Schuessler
University of North Texas
Joseph.schuessler@unt.edu

Bashorat Ibragimova
Texas A&M, Commerce
Bashorat_Ibragimova@tamu-commerce.edu

Abstract

Mobile devices are becoming ubiquitous in both commercial and personal environments. They come in the form of smart phones, laptops, personal digital assistants (PDAs), among others (Ng-Kruelle et al., 2003). With the proliferation of mobile devices comes the risk associated with securing personal information located on these devices. How one perceives the ability of a mobile device to secure personal information is likely to influence one's perceived utility and ultimately one's adoption of such devices. This study identifies the location where the information is stored, encryption, volume of communication, and the sensitivity of the information stored on the device as important factors for users when they are determining the utility of a portable device. Implications for researchers and practitioners are discussed.

Keywords: *IT diffusion and adoption, user acceptance of IT, IT Security, Privacy*

Introduction

Privacy is an ambiguous term with wide-ranging interpretations, depending on the lenses through which it is viewed which include cultural (Dinev et al. 2006), environmental (Moore and Dhillon 2003; Malhotra et al. 2004), legal (Cate 2002), as well as countless others. In these different contexts, much empirical research has been conducted regarding privacy concerns, but from an Information System's (IS's) perspective, much of it has been focused on how privacy relates to online environments (Dinev and Hart 2006; Dinev et al. 2006; Awad and Krishnan 2006). While some theory has been developed regarding privacy as it relates to the use of mobile devices (Ng-Kruelle et al. 2002), little, if any, empirical research has been conducted to examine how privacy enablers impact the user's perceived utility of such devices and their intention to adopt mobile technologies.

It is important to define exactly what privacy and mobile devices are and why mobile devices are unique and need to be investigated. From a legal perspective, the Supreme Court has extended the right of an individual to be free of unreasonable search and seizure to the right of privacy which has itself been extended to a variety of other rights, such as the right to make decisions about abortion, the right to not disclose certain information to the government, and the right to associate freely (Cate 2002). Privacy has been more directly defined as "the ability of the individual to control the terms under which personal information is acquired or used" (Westin

1967, p.7). Information privacy has been similarly defined as “the ability of the individual to personally control information (*italics added*) about one’s self” (Stone et al. 1983).

While providing utility by being mobile, mobile devices typically allow users varying degrees of control over personal information, provided they both understand and perceive value in exercising their control. Users can exercise their control by utilizing protective measures such as encryption, physical security, or more covert action such as misinformation. The ability of users to control their information to achieve privacy (Stone et al. 1983) will be adopted as the definition of information privacy throughout the remainder of this paper.

Smart phones, laptops, and PDAs are all examples of mobile devices (Ng-Kruelle et al. 2002). The pervasiveness of such devices is growing mainly due to improvements in network connectivity, form factors (Chan and Xiaowen 2001), and longer battery life. These drivers (Dinev et al. 2006) of utility and use in mobile devices allow such devices to store and share considerable amounts of information, including personal information. However, inhibitors (Dinev et al. 2006) such as cumbersome security measures may reduce adoption of mobile devices. Combined, drivers and inhibitors (Dinev et al. 2006) cause users and potential future users to form a “privacy calculus” (Awad and Krishnan 2006) used to determine their “price of convenience” (Ng-Kruelle et al. 2002). The effects that a privacy calculus has on consumers has been widely examined in the context of e-commerce (Phelps et al. 2000; Dinev and Hart, 2006) but as it relates to portable devices the issue has not been examined. The unique characteristic of portability makes the adoption of mobile devices unique (Ng-Kruelle et al. 2002) because trade-offs that need to be considered for the protection of personal information in order to obtain the mobility feature.

Investigating information privacy as it relates to the adoption of portable devices is important for both practitioners and researchers alike. Understanding how users perceive the net benefit of traditional security measures in the adoption of mobile devices, researchers can enhance their understanding of how users apply their “privacy calculus” (Awad and Krishnan 2006) in deciding whether or not mobile devices have utility and ultimately are adopted. For IT professionals, a better understanding of how users evaluate the utility of mobile devices can lead to better targeted solutions that limit the “inhibitors” (Dinev et al. 2006) and maximize the “drivers” (Dinev et al. 2006) when deploying or using mobile solutions.

As technology continues to penetrate every facet of our lives, various security measures have been developed to protect private information while, at the same time, provide features and services desirable to users. Examples of protective measures include encryption, storing information in secured backend databases, as well as many others. While tradeoffs between protecting private information and utility exist in more traditional environments, the robustness of computing platforms and the control that users exercise with fixed assets limits performance impacts. However, such protective measures, when used with mobile devices, result in more significant performance degradation that in turn reduces perceived utility and usability. Thus, both drivers and inhibitors (Dinev et al. 2006) influence the adoption of mobile devices.

This study identifies any small, electronic device, capable of storing personal information, easily moved, and is typically located outside protective environments, such as the home or office, as a

mobile device (Ng-Kruele et al. 2002). Mobile devices represent unique challenges to those trying to protect information contained in them in that they are able to hold relatively large amounts of personal information, are susceptible to being lost, stolen, or having their transmissions intercepted, and they are commonly located in hard to secure locations, all of which can contribute to the loss of personal information. Compared to more traditional devices, such as desktop computers, which are bulkier, often more difficult to gain physical access to, and typically have other protective mechanisms such as firewalls and antivirus solutions, mobile devices are relatively easy to compromise.

The purpose of this paper is to investigate user perceptions of traditional security measures designed to protect personal information on mobile devices, explain how they interact with user's perceived utility and intent to use mobile devices, and provide academicians and practitioners alike a foundation with which to extend our understanding of both privacy and the adoption of mobile devices. This paper is organized as follows: first, we discuss traditional security measures and perceived utility and intention to use of mobile devices. Next, we present our methodology and data analysis, followed by a discussion of implications for practitioners and researchers. Conclusions and recommendations for future research are presented.

Theoretical Background

While privacy is often equated with security, it is distinctly different in terms of what we consider to be appropriate measures of protection. Security is seen in terms of trade-offs; the relative cost of security measures compared to the risks or likelihood of a security breach and the potential damage that might occur if such a breach were to occur. Privacy, on the other hand, has a dichotomous element in which information is thought of as either being private or not private. We typically apply security measures, with their inherent ability to provide scalable protection of assets at the expense of functionality, to facilitate information privacy, which is either protected, or not. While the two concepts are inseparable, security is a necessary but not sufficient condition used to achieve privacy. However, users often do not distinguish privacy from security and are willing to give up varying "degrees" of privacy in exchange for goods or services.

While many individuals are fully aware of the presence of mobile devices, such as cell phones and PDAs, other mobile devices, such as toll tags, are often "invisible" in spite of their ubiquity. The fact that these devices are so ubiquitous beckons the question: "Do these devices contain personal information and if so how is it protected?" Perhaps, an even more interesting question is: "How much protection and privacy are users willing to sacrifice in order to maximize the functionality of portable devices around them and ultimately decide to use those devices?" This is the heart of portable privacy; the degree of privacy users are willing to sacrifice in order to maximize functionality of portable devices. While privacy issues have been widely debated in many areas, the idea behind portable privacy has emerged only recently due to technological advances, such as long battery life, increased storage capacity, and the ease of network connectivity.

The concept of portable privacy is more than just a privacy issue though; it is also a business/marketing issue. Consumers and organizations have different opinions about the trade-

offs between privacy and functionality of products and services (Roy Morgan 2001). Roy Morgan Research (2001) found that Australian consumers felt that, in dealing with organizations, protecting their personal information was the most important aspect of the relationship. Organizations, however, felt that the quality of products and services and the efficiency of service were more important. The disparity of opinions suggests that a better understanding of consumer's concerns about the relationship between privacy and utility is needed.

Stone and Stone (1990), in the development of a privacy model, argue that an important determinant of invasion of privacy perceptions is the degree to which the subsequent release or disclosure of data is made without the employee's permission. One of the central tenets of privacy is the ability to control information about oneself. An individual's desire not only to be aware of information gathering and dissemination, but also to give permission for the gathering or dissemination, a priori, is one strategy that individuals use to protect their privacy. An extended version of the Technology Acceptance Model (TAM) was used by Lallmahamood (2007) to demonstrate a relationship between technology adoption in an online environment and privacy and security concerns. While the researchers mentioned above address privacy issues (in offline and online environments respectively), they do not consider the use of portable devices.

To understand these concerns, we examine how users assess the utility of a portable device and ultimately, whether or not to use it. Four security issues were examined that were anticipated to impact a user's perceived utility and intention to use portable devices. The conceptual model illustrates that users' perception of encryption, the perception of sensitivity of information stored on a mobile device, the location that the information is stored, and the volume of communication will influence how they perceive a mobile device's utility and ultimately, their intention to use the mobile device. The conceptual model also illustrates perceived utility as a mediator between intention to use and the security measures. Each of these factors is discussed in further detail below.

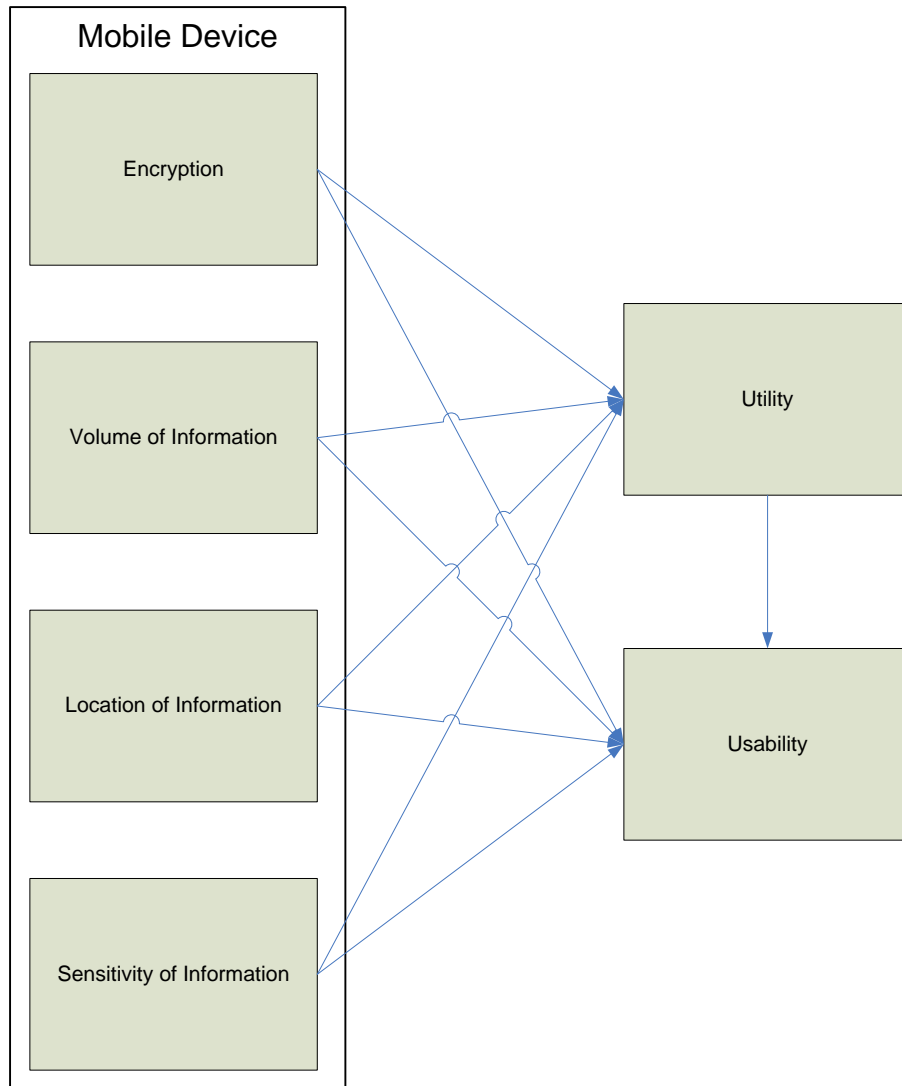


Figure 1. Conceptual Model

Sensitivity

Sensitivity is defined as “any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect” an individual’s information privacy to which they are entitled (Adapted from the National Institute of Standards and Technology’s Computer Security Resource Center ITL bulletin, Retrieved 11-3-2005).¹ Sensitivity is a relative term and describes the perception that a user has about his/her information. Two users with exactly the same information can view the sensitivity of that information differently. Ng-Kruele and colleagues (2002) argue that the sensitivity level that a user has for information privacy influences the price of convenience. The higher the sensitivity that one has for their personal information, the more “expensive” will be their price of convenience (Ng-Kruele et al. 2002). This might result in an individuals’ decision not to use a particular device or requiring additional

¹ <http://csrc.nist.gov/publications/nistbul/cs192-11.txt>

features or security measures in order to offset the high “cost” of the convenience (Ng-Kruelle et al. 2002). Hence, users with higher sensitivity levels would perceive less utility in a mobile device. Conversely, users with lower information sensitivity would likely find greater value in a mobile device and therefore be more likely to use that device. This leads to:

H1a: Sensitivity will be negatively related to utility.

H1b: Sensitivity will be negatively related to intention to use.

Encryption

Both efficient and effective encryption schemes are particularly relevant to mobile devices. Because of the portability of mobile devices, they are routinely lost or stolen and are inherently more difficult to secure because they are typically located in field settings. One major advantage in the use of encryption is that it can help strengthen the protection of data on portable devices despite the fact that these devices may get lost or stolen. However, encryption features are often difficult to implement and not intuitive to end users. In a report published by the International Telecommunication Union (ITU) in April of 2005, Gow suggested that encryption would have a powerful influence on the scope of deployment of mobile devices (page 12). Because of the uncertainty involved in the encryption effectiveness, i.e., whether or not it helps or hinders user’s ability to simultaneously protect and use their portable device, the directionality of how encryption is perceived to influence utility and use is unknown. Therefore:

H2a: Encryption will be related to utility.

H2b: Encryption will be related to intention to use.

Stored Location of Information

Information can be stored on the device itself, it can be stored in a backend database and linked via a unique identifier (Gardner 2002) or some combination of the two. Most of the research conducted regarding location as it relates to mobile devices revolves around proximity of the location where the location of the device is determined for targeted marketing purposes (Duan and Canny, Working Paper; Ng-Kruelle et al. 2002; Gow 2005). Using a backend database allows administrators more control over how, when, and from where data can be accessed thus, making it more secure. However, such an approach requires that the data be transmitted to the mobile device when needed hence, creating transmission security problems as well as bandwidth performance concerns. In addition, connectivity issues may prompt users to maintain information locally on a portable device to avoid situations where they are unable to connect to the backend database. Transmission risk can be reduced but physical security becomes more of an issue when personal information is stored directly on the mobile device. The tradeoffs involved in considering location for storing data are similar to those faced by web designers. By using client-side scripts, much of the workload can be shifted from the server to the client. However, with code being executed on a client machine, the workload on the server is reduced at the expense of control over the client system. Greater security can be achieved by using server side scripting which places heavier burden on the server. Portable devices face similar concerns. By connecting to a backend database, security can be enhanced but greater demand is placed on the backend database and transmission security becomes a potential problem. Placing the information on the portable device itself can enhance utility and use at the expense of security.

The location of stored information, while not completely understood by users with regarding its influence on the use and utility of the portable device, is at least recognized as a potential security concern by IT practitioners. States, such as California, have taken steps to regulate where sensitive information can be stored and the use of encryption to access such data. California Senate Bill 682 requires not only the encryption of unique identifiers on some portable devices, such as smart card and RFID tags, but also prohibits storage of personal information on mobile devices and requires redirecting it to a secured backend database (Sarkar 2005). Legislation of that nature demonstrates understanding of the importance of the relationship between location and security but fails to incorporate performance impacts created through other mechanisms, such as encryption.

As users become more aware of information location issues, they may find that the advantage of having information on their mobile device is more convenient than having to “connect” to backend databases in order to get the most current information. Alternatively, they may feel that the advantage of having data stored in backend databases, where it can be protected and more frequently backed up as a greater advantage.

H3a: Location of information will be related to utility.

H3b: Location of information will be related to intention to use.

Volume

Regular transmissions using the 802.11x protocol allow potential intruders to become aware of and eventually access wireless access points, even those not broadcasting their Service Set IDs with Wired Equivalent Privacy (WEP) enabled (Berghel and Uecker 2004). RFID faces similar vulnerability issues (Weis et al. 2003). Physical security is threatened by locating information directly on mobile devices. However, the volume of communication is likely to increase thus, affecting transmission security, by locating information on portable devices linked to backend databases. Corroni (1999) discussed the concept of dynamic security which can adjust to differing security needs based on, among other things, the volume of communication a particular device has. Portable devices that transmit greater volumes of information more frequently require scalable security mechanisms capable of adapting to changing demands of communication volumes on these portable devices. Therefore, the more portable devices must communicate with backend databases and other portable devices, the more likely they are to influence one’s perceived utility and their intention to use a portable device. Users are likely to value their ability to use their mobile devices at their convenience, regardless of connectivity or other related issues. Therefore, the more that users use their mobile device, the more utility they should have with the device. This leads to the following hypotheses:

H4a: Volume of communication will be positively related to utility.

H4b: Volume of communication will be positively related to intention to use.

Utility and Intention to Use

Utility and intention to use are the dependent variables which encryption, sensitivity, location, and volume are hypothesized to influence. Corroni (1999) suggested that the security of a mobile device often suffers at the expense of making it easier to use. Thus, the utility of a device is often higher when security is minimized or absent. On the other hand, the more user values encryption and the more sensitivity, location, and volume of information needs are met, the more

utility users will perceive in a particular device. This would suggest that security measures may result in trade-offs that are more difficult to determine. Regardless of the trade-offs that a user considers in determining the utility of a portable device, expectancy theory (Wilton and Myers 1986) suggests that the more utility that a user perceives a device to have, the more likely they would be to use the device.

H5: Utility will be positively related to intention to use.

For purposes of our analysis, the purpose of use is not considered in the current study though the motivations for use are certain to vary among users. For example, certain users are likely to use portable devices for pleasure (downloading music/video files) or for task-oriented purposes, such as work. Additionally, we assume that the use of portable devices is optional and not required. This assumption does not hold in certain situations.

Method

Data were gathered using a self-administered survey instrument. An iterative process of instrument development expanded the initial set of constructs (location, sensitivity, volume, encryption, and use) to include utility. With five items per construct, the survey was administered to several undergraduate classes of university students at a Southwestern university with a relatively large commuter student body. While student “demographics and psychographics” are often dissimilar to the general population as a whole, student subjects can make good subjects depending on the context of the study (Patzner 1996). Patzner argues that, among other reasons, students can be appropriate “When products and behaviors of interest to the researcher are characteristic of such subjects” (page 56). We argue that students were an appropriate population in the context of the current study because they commonly use and are familiar with various types of portable devices, such as PDAs, toll tags, cellular phones and so on. A total of 339 surveys were distributed, with 322 of the surveys returned and considered usable, representing a 94.99 percent response rate. Participation was voluntary, although to encourage participation, bonus points were awarded to each participant completing the survey.

A principal components factor analysis with varimax rotation (see Table 1) was performed. Items were removed which loaded on multiple factors. Items were examined within each construct to see if they loaded highly on the intended construct (an example of convergent validity) and discriminant validity was assessed by looking for items loading on factors other than the intended factor (Cook and Campbell 1979). One item (L5) hypothesized to be associated with the location construct loaded on the sensitivity construct instead. Due to the strength of the loading, it was decided to retain that item in the sensitivity construct. Loadings of .45 to .54 are considered fair, .55 to .62 are considered good, .63 to .70 are considered very good, and above .71 are considered excellent (Comrey 1973). As can be seen in Table 2, the lowest factor loading, after removal of cross loaded items (and the retention of L5 as a sensitivity item), was .662 which is deemed very good, according to Comrey (1973). The amount of variance is also significant at 59.99 percent.

| | Encryption | Location | Sensitivity | Volume |
|--|------------|----------|-------------|--------|
| (E1) Encryption helps protect my data on portable devices. | .815 | | | |
| (E2) Information on portable devices has | .798 | | | |

| | | | | |
|---|-------|-------|-------|-------|
| different encryption needs. | | | | |
| (E5) Transmissions of information between a portable device and other devices should be encrypted. | .719 | | | |
| (L1) Portable devices are safe to store personal information on. | | .742 | | |
| (L3) Information should be stored on portable devices rather than a backend database. | | .847 | | |
| (L5) The location of information (whether on a portable device or in a backend database) should change depending on my needs. | | | .701 | |
| (S1) Information stored on portable devices varies in their sensitivity. | | | .684 | |
| (S3) The more sensitive information is, the more a portable device should secure that information. | | | .685 | |
| (S4) There are different sensitivity levels of information stored on portable devices. | | | .727 | |
| (V2) The more often I use a portable device, the less secure it will be. | | | | .741 |
| (V3) The volume of communication my portable device has with other devices increases the risk of stolen/captured information. | | | | .683 |
| (V4) Communication is less secure when there are many portable devices trying to communicate. | | | | .757 |
| (V5) Portable devices that automatically communicate with other devices are less secure. | | | | .662 |
| Cronbach's alpha | .722 | .444 | .706 | .724 |
| Total variance explained (59.990%) | 17.40 | 17.07 | 15.41 | 10.11 |

Table 1: Factor Loadings

An inter-item correlation was also performed to analyze convergent and divergent validity further. Items within a construct should correlate more highly with other items within the same construct and less with items from other constructs. These results are presented in Table 2. Finally, the composite reliability (internal consistency) of each construct was measured using Cronbach's alpha (Cronbach 1951). Hair and colleagues (1998) explain that Cronbach's alpha levels of .70 or higher are desirable, though .60 and higher are acceptable for newly developed scales. As can be seen in Table 1 above, Cronbach's alphas for each factor were over the .70 threshold, except for the Location construct which was .444. Problems associated with this construct will be discussed later in this section.

| | E1 | E2 | E5 | L1 | L3 | L5 | S1 | S3 |
|----|----------|----------|----------|-----------|-------|----------|----------|----------|
| E2 | .582(**) | | | | | | | |
| E5 | .447(**) | .377(**) | | | | | | |
| L1 | .106 | .000 | -.068 | | | | | |
| L3 | .102 | .044 | .084 | .297(**) | | | | |
| L5 | .259(**) | .213(**) | .131(*) | .096 | .043 | | | |
| S1 | .270(**) | .284(**) | .183(**) | .045 | .028 | .369(**) | | |
| S3 | .250(**) | .241(**) | .292(**) | .057 | .062 | .342(**) | .348(**) | |
| S4 | .243(**) | .175(**) | .168(**) | .037 | .084 | .322(**) | .392(**) | .492(**) |
| V2 | -.018 | .031 | .087 | -.225(**) | .002 | -.017 | .097 | .072 |
| V3 | .174(**) | .190(**) | .207(**) | -.102 | -.001 | .222(**) | .270(**) | .269(**) |
| V4 | .233(**) | .263(**) | .145(**) | -.097 | .084 | .179(**) | .222(**) | .256(**) |

| | | | | | | | | |
|----|----------|----------|----------|-----------|------|----------|----------|----------|
| V5 | .235(**) | .227(**) | .254(**) | -.148(**) | .102 | .199(**) | .203(**) | .354(**) |
|----|----------|----------|----------|-----------|------|----------|----------|----------|

** Pearson Correlation is significant at the 0.01 level (1-tailed). * Pearson Correlation is significant at the 0.05 level (1-tailed).

| | | | | |
|----|----------|----------|----------|----------|
| | S4 | V2 | V3 | V4 |
| V2 | .143(**) | | | |
| V3 | .246(**) | .357(**) | | |
| V4 | .224(**) | .362(**) | .537(**) | |
| V5 | .267(**) | .313(**) | .369(**) | .485(**) |

Table 2: Exogenous Inter-Item Correlations

Convergent validity for the endogenous variables were also assessed. With the lowest factor loading of .713 shown in Table 3, the loadings were excellent, according to Comrey (1973). Similar to the sensitivity and location constructs above, one utility item (T5) loaded on the Intention to Use construct. The Use construct was retained due to the strength of the loading.

| | Utility | Use |
|--|---------|-------|
| (T3) I am less likely to use portable devices that aren't secure. | .793 | |
| (T5) I am more likely to use a portable device when my personal information is protected. | .758 | |
| (T2) I would not use portable devices because of security concerns. | .713 | |
| (U1) The utility of a portable device is strongly associated with the security of the technologies involved. | | .763 |
| (U5) Portable devices with many features are difficult to use. | | .734 |
| (T5) I am more likely to use a portable device when my personal information is protected. | | .716 |
| Cronbach's alpha | .647 | .592 |
| Total variance explained (58.261%) | 30.86 | 27.40 |

Table 3: Factor Loadings of Endogenous Variables

An inter-item correlation was performed to analyze convergent and divergent validity further among the endogenous items (Table 4). Items correlated more highly with items from the same factor and less with items from the other factor, thus, displaying divergent validity. Reliability using Cronbach's alpha, was .647 for Utility and .592 for intention to use. Given the fact that it was a newly developed scale, the Cronbach's alpha for Utility was deemed acceptable. Also, because this is a newly developed scale, the Cronbach's alpha of .592 for intention to use is so close to the .60 threshold, and the theoretical design of the model, that the intention to use construct was used despite its relatively low Cronbach's alpha.

| | | | | | |
|----|-----------|----------|----------|----------|---------|
| | U1 | U5 | T2 | T3 | T5 |
| U5 | .325(**) | | | | |
| T2 | -.108(*) | .038 | | | |
| T3 | -.062 | -.068 | .386(**) | | |
| T5 | -.154(**) | .004 | .286(**) | .473(**) | |
| T1 | .296(**) | .344(**) | .194(**) | .110(*) | .110(*) |

** Correlation is significant at the 0.01 level (2-tailed). * Correlation is significant at the 0.05 level (2-tailed).

Table 4. Endogenous Inter-Item Correlations

A Structural Equation Model (SEM) using LISREL was created to assess the proposed model. The LISREL analysis used a sample covariance matrix as input and a maximum likelihood solution. Using the two-step approach proposed by Anderson and Gerbing (1988), the measurement model was developed followed by creation of the structural model. The two-step procedure allows for the analysis of measurement items prior to the structural influences. The matrices of indicator error variances and covariances were examined for latent variables by looking at theta deltas and theta epsilons to see which, if any, could be set to improve the measurement model.

It was at this point that the problems with the Location construct became evident. Running the exogenous measurement model with all exogenous items and theorized constructs was not positive definite. Attempts to rectify the issue using the LISREL output suggestions of setting the admissibility (AD) to greater than 255 or “off” were unsuccessful. As a result, the Location construct was dropped from the model. Finally, the structural model was added to the measurement model by including the hypothesized gammas. The results are discussed in the following section.

Analysis

The measurement model was developed in LISREL with the variance/covariance matrices for the respective constructs were created using SPSS 12.0. The Encryption, Location, Utility, and Use were either perfectly fit or had negative degrees of freedom and therefore, fit statistics were not calculated. However, the fit statistics for the measurement model (Table 5) indicate good fit for both Volume and Sensitivity. With the measurement model in place, the variance/covariance matrix was produced for all factors using SPSS. The results are shown in Table 6 along with the correlations between each factor. Finally, the structural model was created in order to assess the overall validity of the model. The structural model resulted in a GFI of .94 and an AGFI of .92. Table 7 presents results of hypotheses testing and fit statistics. Since Location construct was dropped from the original model, hypotheses 4a and 4b were not tested. The standardized structural model is shown in Figure 2.

| | Reliability | X ² (df) | Factor Structure Diagnostics | | | | |
|-------------|-------------|---------------------|------------------------------|-------|------|------|------|
| | | | P-Value | RMSR | GFI | AGFI | NFI |
| Encryption | 0.722 | 0(0) | 1.000 | - | - | - | - |
| Volume | 0.724 | 5.07(2) | 0.079 | 0.043 | 1.00 | 0.98 | 0.99 |
| Sensitivity | 0.706 | 11.42(2) | 0.003 | 0.057 | 0.99 | 0.95 | 0.98 |
| Location | 0.444 | - | - | - | - | - | - |
| Utility | 0.647 | 0(0) | 1.000 | - | - | - | - |
| Use | 0.592 | 0(0) | 1.000 | - | - | - | - |

Table 5. Measurement Model Fit Statistic

| | | Mean | SD | E | V | S | L | T | U |
|------------|---|--------|---------|----------------|------|------|------|------|------|
| Encryption | E | 4.6455 | 1.12262 | (0.722) | .411 | .492 | .056 | .025 | .511 |

| | | | | | | | | | |
|-------------|---|--------|---------|--------|----------------|----------------|----------------|----------------|----------------|
| Volume | V | 4.5790 | 1.15270 | .316** | (0.724) | .600 | -.167 | .321 | .416 |
| Sensitivity | S | 4.9154 | 1.05332 | .414** | .493** | (0.706) | .090 | .076 | .599 |
| Location | L | 3.9461 | 1.27464 | .039 | -.114* | .068 | (0.444) | -.100 | .218 |
| Utility | T | 3.7639 | 1.15323 | .019 | .241** | .063 | -.068 | (0.647) | .014 |
| Use | U | 5.1141 | 1.12000 | .409** | .323** | .510** | .154** | .011 | (0.592) |

** Significant at the .01 level, * Significant at the .05 level (Note: The diagonal represent the construct's Cronbach alpha. The bottom diagonal is the correlation matrix and the upper diagonal is the variance/covariance matrix.)

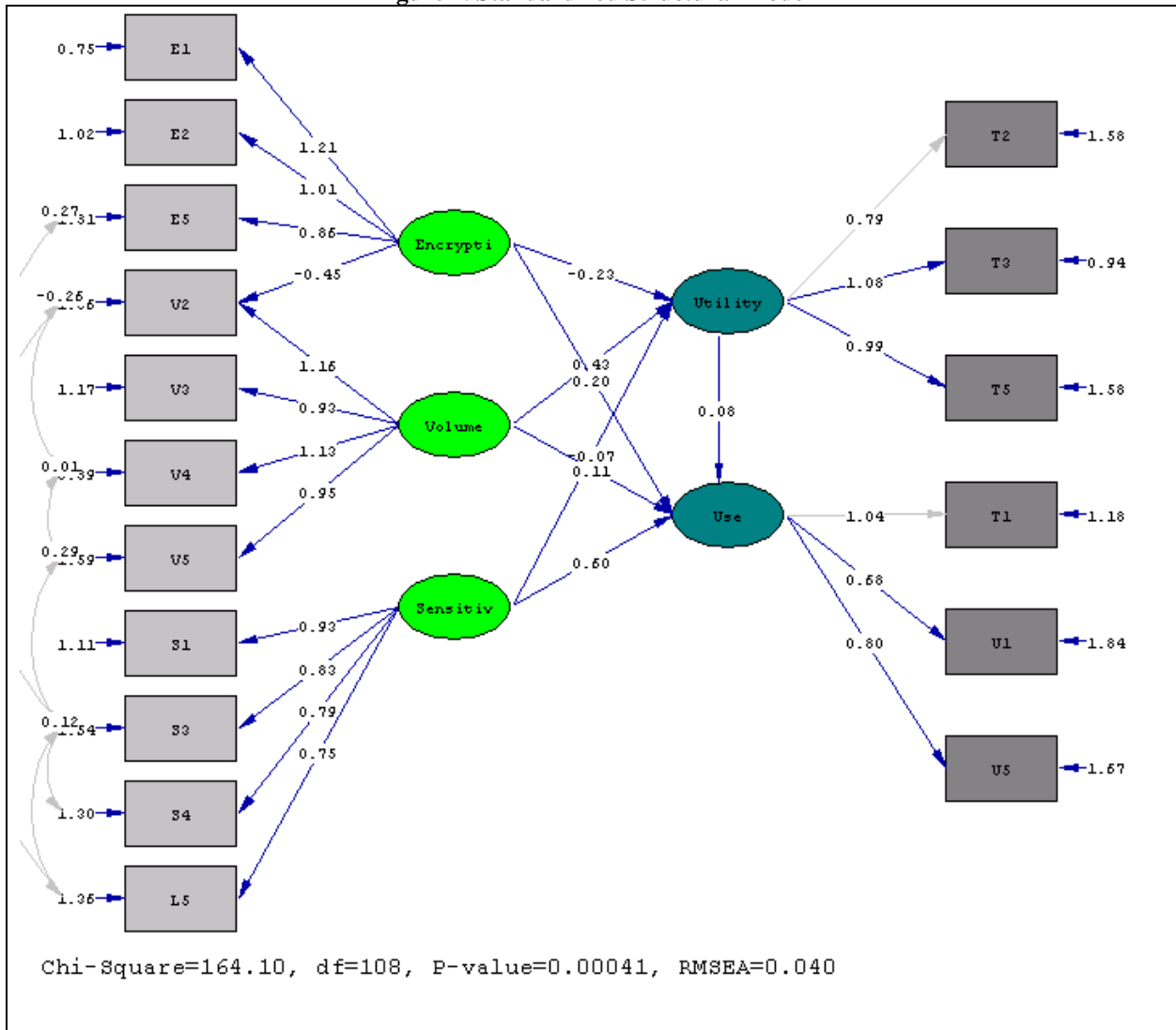
Table 6. Correlation, Variance/Covariance/Cronbach's Table

| | Path | Hypotheses | Estimate | t-value |
|-------------------------------|---------------|------------|----------|---------|
| Test of Hypotheses: | | | | |
| Sensitivity to Utility | γ_{13} | 1a | -0.07 | -.55 |
| Sensitivity to Use | γ_{23} | 1b | 0.6 | 5.05* |
| Encryption to Utility | γ_{11} | 2a | -0.23 | -2.23* |
| Encryption to Use | γ_{21} | 2b | 0.2 | 2.03* |
| Location to Utility | γ_{14} | 3a | - | - |
| Location to Use | γ_{24} | 3b | - | - |
| Volume to Utility | γ_{12} | 4a | 0.43 | 3.98* |
| Volume to Use | γ_{22} | 4b | 0.11 | 1.04 |
| Utility to Use | β_{21} | 5 | 0.08 | .89 |
| Global Model Fit Diagnostics: | | | | |
| Chi-squared | | 164.1 | | |
| Degrees of Freedom | | 108 | | |
| P-value | | 0.000 | | |
| GFI | | 0.940 | | |
| AGFI | | 0.920 | | |
| RMSR | | 0.120 | | |
| Bentler & Bonett's NFI | | 0.930 | | |
| Bentler's CFI | | 0.970 | | |

(*Significant at the .05 level)

Table 7. Structural Model Fit Statistics and Hypotheses Results

Figure 2. Standardized Structural Model



Results

The hypothesis about the negative relationship between sensitivity of information and perceived utility of a device was not supported. The relationship was negative but was not statistically significant at the .05 level. The hypothesis about the influence of sensitivity of information stored on a device on a person’s intention to use a portable device was also not supported, though the relationship was significant. This is interesting because it indicates that people feel that the more sensitive the information on a portable device, the greater their intention to use it, however, there is no relationship between perceived utility and sensitivity of information. This suggests an apparent disparity between perceived utility and use, at least with this sample.

The hypothesis about the relationship between encryption and perceived utility of portable devices was supported. The relationship was negative suggesting that perhaps users perceive encryption as something that decreases the utility of a device by making it more difficult to use. When considered in conjunction with the hypothesis about the relationship between encryption

and user's intention to use a mobile device which was also supported, it becomes clear that even though users perceive that encryption makes a portable device more difficult to use, they are actually more likely to use a portable device that utilizes encryption technologies. This suggests that users perceive encryption as a tolerable trade-off in spite of its negative impact on the utility of a portable device.

H3a and H3b were not tested because the Location construct was not incorporated into the model. The hypothesis about the positive effect of the volume of communication on a user's perceived utility of a portable device was supported. Users feel that the longer or more often a device is used, the more utility that device has. Interestingly, the volume of communication is not related to user's intention to use a portable device. Another interesting finding was that the utility of a portable device did not impact the use of that device. Perhaps, portable device use is influenced by other factors, not included in this study, such as mandated use or the desire of some users to project an image of early adopters of new technology.

Limitations

Additional research is needed to boost confidence in the external validity of the present study's findings. One external validity concern centers on the possibility of a selection of the sample used in the study. Specifically, it might be argued that students would use portable devices differently than would employees in organizations. In addition, it might be argued that the external validity of the present study is questionable because the types of portable devices that students use may not have been comparable to those used by the general population. Note, however, that the types of portable devices considered in the present study were taken from those that appear in several commonly and widely used portable devices (e.g., PDAs, laptops, toll tags). This fact should reduce concerns about external validity.

While increasing perceived utility by making encryption techniques more user friendly and promoting a device's capability to communicate large amounts of data, the lack of a relationship between utility and use indicate that such efforts may prove fruitless in the world of portable devices. This lack of relationship between utility and use of portable devices may indicate that users are utilizing these devices for entertainment rather than work or task-related purposes. Another possibility may be that users are required to utilize these devices in their daily activities. The use of a toll pass may not be perceived to provide utility, but rather a necessity in order to be able to commute.

Future research on portable devices needs to examine the impact of location on the perceived utility and use of a portable device. Standard practices of locating sensitive information as far away from prying eyes as functionally possible suggests that location is indeed an important factor. However, empirical support of this relationship was not found in this study. Additionally, the Utility and Intention to Use constructs could be refined to strengthen the instrument. The absence of a relationship between these two constructs as measured in the proposed model suggests a measurement error or something unique to the use of portable devices that has not been explained by the model. One possible reason is whether or not use of such devices is required or optional. Whether or not the use of a portable device is optional or mandatory may impact how a user perceives the utility of that device.

Conclusion

This research is relevant for researchers and practitioners alike. For researchers, it draws attention to possible relative differences in the security of portable devices and how they are influenced differently than more traditional fixed devices. For practitioners, it allows organizations to understand what end users think is important with respect to the security of portable devices. For example, since perceived utility does not lead to intention to use, building in extra features may be seen as both a waste of time and money. Because manufacturers ultimately are more interested in intention to use a device than they are in perceived utility, efforts should focus on explaining the ability of a device to store information locally and encrypt sensitive information in order to increase user's likelihood of using such devices.

Finally, the study can be replicated using a different population to determine if differences, such as age or culture, influence user feelings about the security of portable devices and their perceived utility and use. While students were an appropriate population for purposes of this study, such differences may influence the strength and directionality of the relationships proposed in the current study. Age has been shown to be negatively related to the adoption technology (Morris and Venkatesh 2000). The use and securing of private information as it applies to portable devices can be tested among different age groups to determine whether the findings by Morris and Venkatesh (2000) hold for portable devices specifically. Portable devices are becoming ubiquitous to the point that their use goes unnoticed. This study enhances our understanding of some of the more important factors involved when users attempt to evaluate the security of portable devices and when making a decision of whether or not to use such a device.

REFERENCES

Anderson, J. C., & Gerbing, D. W. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin*, 103(3), 411.

Awad, N. F., & Krishnan, M. D. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *Management Information Systems Quarterly*, 30(1), 13-28.

Berghel, H., & Uecker, J. (2004). Wireless infidelity II. *Association for Computing Machinery. Communications of the ACM*, 47(12), 15.

Caronni, G. (1999). *Dynamic Security in Communication Systems*. Swiss Federal Institute of Technology Zurich, Zurich.

Cate, F. H. (2002). Principles for Protecting Privacy. *Cato Journal*, 22(1), 33-57.

Chan, S. S., & Fang, X. (2001). *Usability Issues in Mobile Commerce*. Paper presented at the Proceedings of the Seventh Americas Conference on Information Systems, Atlanta, Georgia.

Comrey, A. L. (1973). *A First Course in Factor Analysis*. New York: Academic Press.

Cook, T. D., & Campbell, D. T. (1979). *Quasi-Experimentation: Design and Analysis Issues for Field Settings*. Boston: Houghton Mifflin Company.

Cronbach, L. J. (1951). Coefficient Alpha and the internal Structure of Tests. *Psychometrika*, 16(3), 297-337.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy Calculus Model in E-commerce - a Study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389-402.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transaction. *Information Systems Research*, 14(1), 61-80.

Duan, Y., & Canny, J. *Designing for Privacy in Ubiquitous Computing Environments*. Unpublished manuscript.

Fabbi, J. L., Watson, S. D., Marks, K. E., & Sylvis, Z. (2005). UNLV Libraries and the digital identification frontier. *Library Hi Tech*, 23(3), 313.

Gardner, D. (2004). *Rfid Chips Implanted in Mexican Law-Enforcement Workers*. Retrieved 6-28-2005, 2005, from <http://www.informationweek.com/story/showArticle.jhtml?articleID=23901004&tid=1369>

- Gow, G. A. (2005). *Privacy and Ubiquitous Network Societies* (ITU Strategy and Policy Unit). Geneva: International Telecommunication Union.
- Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis* (5th ed.). Dehli: Pearson Education.
- Joreskog K. & Sorbom D. (1993). *LISREL 8: User's reference manual*. Chicago: Scientific Software, Inc.
- Katz J.E. & Tassone A.R. (1990). Public opinion trends: Privacy and information technology. *Public Opinion Quarterly*, 54, 125-143.
- Kelly, E. P., & Erickson, G. S. (2005). RFID tags: commercial applications v. privacy rights. *Industrial Management + Data Systems*, 105(5/6), 703.
- Lallmahamood, M. (2007). An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce*, 12(3), 1.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355.
- Moores, T. T., & Dhillon, G. (2003). Do Privacy Seals in E-Commerce Really Work? *Communications of the ACM*, 46(12), 265-271.
- Morgan, R. (2001). *Privacy and Business 2001*. Retrieved 12-8-2005, 2005, from <http://www.privacy.gov.au/publications/rbusiness.html>
- Morris, M. G., & Venkatesh, V. (2000). Age Differences in Technology Adoption Decisions: Implications for a Changing Workforce. *Personnel Psychology* (53), 375-403.
- Ng-Kruelle, G., Rebne, D. S., Swatman, P. A., & Hampe, J. F. (2002). *Interfaces in Adoption of an Evolving Innovation: An Activity-Theoretical Perspective and the Price of Convenience*. Paper presented at the Eleventh European Conference on Information Systems, Naples, Italy.
- Patzer, G. L. (1996). *Experimental-Research Methodology in Marketing: Types and Applications*: Quorum Books.
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1), 27-41.
- Rensel, A. D., Abbas, J. M., & Rao, H. R. (2006). Private Transactions in Public Places: An Exploration of the Impact of the Computer Environment on Public Transactional Web Site Use. *Journal of the Association for Information Systems*, 7(1), 19-51.

Sarkar, D. (2005). *California Lawmakers Soften RFID Stance*. Retrieved 7-7-2005, 2005, from <http://www.fcw.com/article89425-06-29-05-Web>

Stone, E. F., Gardner, D. G., Gueutal, H. G., & McClure, S. A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 68(3), 459.

Stone E.F. & Stone D.L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management*, 8, 349-411.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

Wilton, P. C., & Myers, J. G. Task, Expectancy, and Information Assessment Effects in Information Utilization Processes. *Journal of Consumer Research*, 12(4), 469