Assessing the Impact of Concern for Privacy and Innovation Characteristics in the Adoption of Biometric Technologies

Aakash Taneja

University of Texas at Arlington
Department of Information Systems & Operations Management; Arlington, TX 76019
Phone: (817) 272-3707 Fax: (817) 272-5801
E-mail: aakash@uta.edu

Ailing Wang

University of Texas at Arlington
Department of Information Systems & Operations Management; Arlington, TX 76019
Phone: (817) 272-3537 Fax: (817) 272-5801
E-mail: awang@uta.edu

M. K. Raja
University of Texas at Arlington
Department of Information Systems & Operations Management; Arlington, TX 76019
Phone: (817) 272-3540 Fax: (817) 272-5801
E-mail: raja@uta.edu

ABSTRACT

The introduction of biometric techniques into the workplace is both a source of anxiety and excitement. While biometric techniques are easier to use, fears and concerns relating to an individual's privacy influence their intention to adopt such techniques. To assess this influence, in this study, we endeavor to propose a model of Biometric Technology Adoption in organizations by building upon Roger's Perceived Characteristics of Innovation (PCI) Model. A set of testable hypotheses is also provided in order to empirically validate the model.

INTRODUCTION

With the growing concerns for security, various technologies are being developed and deployed to safeguard and mitigate the concerns of organizations and users. Some examples of these technologies include: Password protected accounts, Anti-virus software, Biometrics, Firewalls, Intrusion Detection / Prevention Systems, and Smart cards, to name a few. Although organizations are investing resources for computers and information systems security, people are the weakest link in the information security (Mitnick and Simon 2002; Mitnick 2003; Whitman and Mattord 2003; Wade 2004).

Systems are designed in such a way that the users needs to authenticate and verify self in the form of passwords in order to access the resources. However, employees are found to knowingly share their password with fellow employees. They are also many times duped into disclosing their password (Social Engineering). Difficulty in remembering dissimilar passwords discourages people to have different passwords for various accounts. Again, strict complexities and rules involved while creating a password and a requirement to change the password after

certain period of time also causes lot of inconvenience to the users. There is no doubt that all these efforts are aimed to better protect the data and information, but they are also moving technology away from the people in terms of "Ease of use" of the operations. Thus, there is a need to integrate "Ease of use" and required functionality of authentication and control to safeguard the data and information. Biometric Technology is one such innovation that is being claimed to achieve the same.

Literature suggests that there is a difference in adoption of technologies by various users (Rogers 1995). Some users readily adopt or reject new technologies while others take time for the same (Rogers 1995). New technology that is developed to solve existing problems is also many times perceived by the users as an originator of new concerns. While there are positive factors influencing the use of Biometric Technology (in terms of safety and security), there are also some perceived potential negative factors (e.g.: privacy, inconvenience, etc.) that are causing concerns to users in terms of their acceptance of these technologies. This study will attempt to assess these factors related to adoption of the Biometric Technology.

The main contributions of this study are the following: This paper builds upon theoretical perspectives to offer a rich model of Biometric Technology Adoption in organizations and provide a set of testable propositions to empirically validate this model. It also extends the applicability of Perceived Characteristics of Innovation (PCI) model (Moore and Benbasat 1991) by adding a characteristic related to the concern for privacy that is unique to innovations such as Biometric Technology. We surmise the need of such a construct in the PCI model because of the inherent characteristics of these types of new technologies. Based on the existing IS and psychology literature, this paper develops a conceptual model of how the privacy concerns of the users along with other innovation characteristics influence their intention to adopt Biometric Technology.

The structure of the paper is as follows: In the first section, we describe Biometric Technology and review the related research concerning benefits and weakness of the use of this technology. Next, we present the theoretical background for this study followed by an integrated model and testable propositions derived from this model. Finally, we conclude by discussing the contributions of this study.

BIOMETRIC TECHNOLOGY

Biometrics can be defined as the measurable physical / personal characteristics of an individual that can be compared for identification purposes. According to Boole et al (2004), it involves the authentication of an individual based on some distinctive characteristics of that individual. In order to serve as a biometric characteristic, an attribute must possess the conditions shown in Table 1.

Universal	Each person should have the concerned characteristic.
Unique	Any two persons should be different in terms of the characteristic.
Permanent	Needs to be sufficiently invariant over a period of time.
Quantifiable	Needs to be measurable.

Table 1: Biometric Characteristic

Biometric Technologies utilize a pattern-recognition system that is capable to recognize a person based on some unique characteristics of that person. It is used to automate the measurement and comparison of these distinctive characteristics in order to identify the individuals during subsequent biometric authentication (Reid 2004). Fingerprints, Facial Recognition, Hand Geometry, Retinal Scan, Iris Scan, Vascular Pattern, and Voice Dynamics biometric are some examples of this technology.

Uses

Traditionally, users employ passwords to authenticate their identity and gain access to the system resources. They set common and easy to remember passwords consisting of simple words and numbers for various applications. It is beyond any doubt that complex passwords consisting of random digits or numbers are secure, but on the other hand are also not relatively easy to remember. Users are frustrated when they cannot access the system because of the forgotten passwords. It also leads to a need of increase in support (technical or human) in order to gain access to the resources. Many times, users also share their passwords with their peers, hereby permitting unauthorized users to access the system. However, this behavior is not encouraged as it makes the system prone to vulnerability, hereby not in the interest of an organization.

Commercial	Government	Forensics
Computer Network Logins Credit Cards E-Commerce Electronic Data Security Internet Access Medical Records Management Physical Access Control	Anti-Terrorism National Id Cards Border Control Driver's Licenses	Corpse Identification Criminal Investigation Missing Children. Terrorist Identification

Table 2: Biometric Technology Applications
(Adopted from Prabhakar et al. 2003)

The main advantage of Biometric Technologies is the convenience to the user. Users no longer need to remember the long and difficult passwords. Since the biometric characteristics can not be shared by anyone else, the individual himself needs to be present at the time of authentication. This is beneficial to organization as its resources can not be accessed by any unauthorized users. These technologies are useful in regulating access and control and are increasingly being used in diverse areas like database access, electronic commerce, financial sector, government, health care, law enforcement, travel and transportation, to name a few. Some typical applications of Biometric Technologies are listed in Table 2. The advancements in technology have also made biometrics affordable to small organizations. According to the CSI-FBI survey (2005), the use of Biometric Technology has increased to 15% as compared to being used by 8% of the

respondents in the year 2000. International Biometric Group (2004) predicts the total biometric revenue to grow to US$4.6 billion by 2008.

Privacy Concerns

Biometrics is considered to be capable of both threatening and increasing individual's information privacy (Woodward 1997; Reid 2004; Elgarah and Falaleeva 2005). While it is helpful in maintaining the security, users also perceive some negative outcomes that inhibit them from using these technologies. For example, since biometric characteristics of an individual present in different applications could be linked together, it is possible to aggregate his / her information stored in these applications without his knowledge. As a result, there is an increasing concern with information privacy associated with the adoption of this technology. This risk of an individual's probable breach of privacy is a unique characteristic of this newer form of technology that should be considered in the context of Technology Adoption and Diffusion.

THEORETICAL BACKGROUND

Adoption of innovation is an important issue among academics and practitioners across various disciplines. IT adoption has also witnessed lot of efforts to have a better understanding of the adoption behavior of various information systems. Davis's (1989) Technology Adoption Model (TAM) is one of the most widely applied model in IS literature. It assumes that beliefs about usefulness and ease of use are the primary determinants of the intention to use a system. However, in some instances, other variables besides ease of use and usefulness also play an important role to predict intentions (Mathieson 1991). Although parsimony is very important, the main reason for which TAM is generally preferred, an individual's intention to adopt the technology also depends on the context in which it has to be used (Plouffe et al. 2001). According to Plouffe (2001), an understanding of such a behavior requires a model that captures the richness of the adoption process across many different contexts.

Roger's (1995) theory of innovation is another commonly used model in the area of IT Adoption. The basic characteristics of an innovation considered by this model are: Relative advantage, Compatibility, Complexity, Trialability and Observability. Moore and Benbasat (1991) extended the set of characteristics proposed by Rogers (1995) and included seven perceived characteristics of an innovation as predictors of IT adoption behavior (Table 3).

Rogers (1995)	Relative advantage, Compatibility, Complexity, Trialability and Observability
Moore and Benbasat (1991)	Relative advantage, Compatibility, Ease of use, Trialability, Observability, Result Demonstrability, Visibility, Voluntariness, Image

Table 3: Innovation Characteristics

Earlier studies (Agarwal and Prasad 1998; Chin and Gopal 1995) have tested the full or a reduced set of the PCI characteristics and found that constructs other than usefulness and ease of use (TAM) are also significantly linked to the intention to adopt a technology. Others (For example, Chin and Gopal 1995) have also added additional constructs depending on the context.

Currently, there is a lot of concern for the security of the systems. New technologies meant to enhance the security mechanisms are being developed. However, these are also bringing new challenges concerning their adoption by the users. Plouffe et al. (2001) observed that many times there is a need to include a richer set of antecedents and sacrifice parsimony in order to predict adoption. Thus, we believe that testing for the perceived concern for privacy will give a better insight into the adoption behavior of these kinds of technologies.

RESEARCH MODEL

From a theoretical perspective, although the leading technology acceptance models (TAM, PCI, etc.) do provide insights into how adoption intentions are formed, the inclusion of concern for privacy will further enhance our understanding of this process. Based on this, we derive a model (Figure 1) and provide testable hypotheses from this model.

Perceived Usefullness

It refers to the degree to which an individual believes that using a system will enhance his or her performance (Davis 1989). Earlier studies have shown that perceived usefulness of a system is positively related to the perceived intention to use the system. As mentioned above, passwords have many problems associated with their uses, because of the difficulty in maintaining various passwords, adhering to policies to change passwords on a regular basis, and the expectation of maintaining different passwords for different applications. Moreover, users compromise the security by knowingly or unknowingly sharing their passwords with others. Biometric technology that uses Biometric traits will not allow someone other than the authorized user to use the resources. This will make it useful to the organization. Also, since traits are natural and unique to every individual, there will be no extra effort required by the users to remember and recall the same. The users who perceive Biometric Technology to be useful because of these unique characteristics will be likely to use this technology. Thus,

Hypothesis 1: Perceived usefulness is positively related to the perceived intention to use Biometric Technology

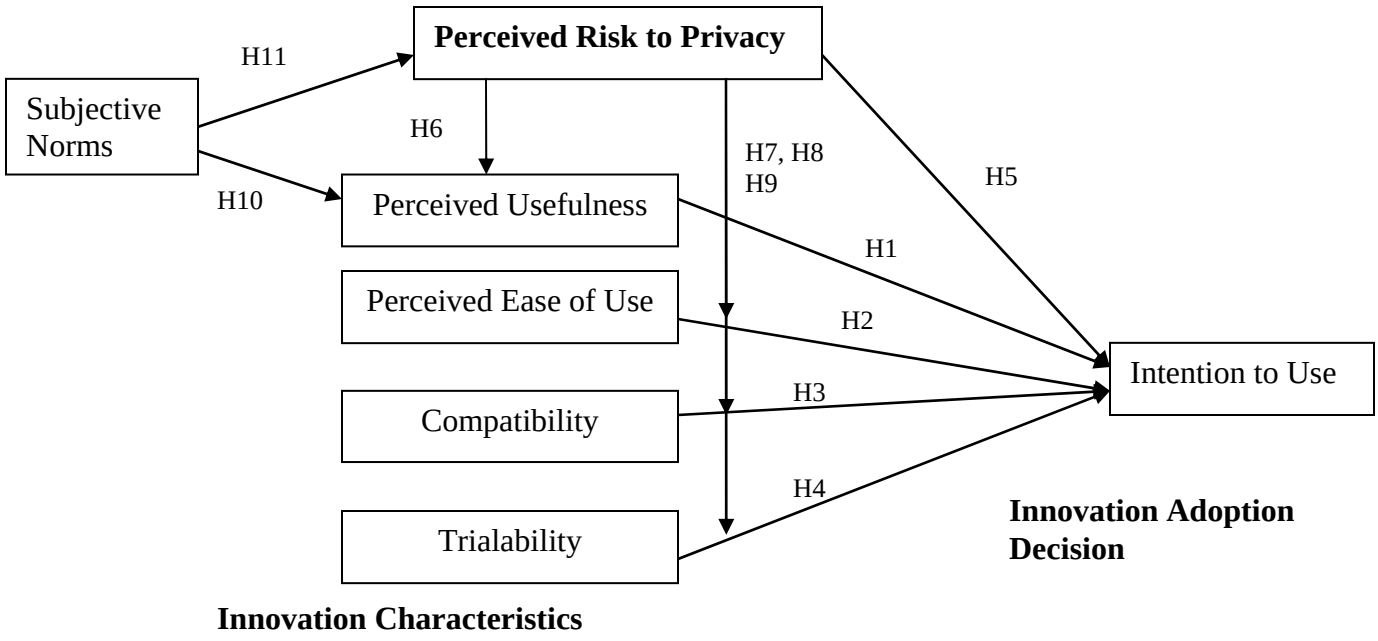

Figure 1: Research Model

Perceived Ease of Use

It refers to the degree to which an individual believes a system to be easy to use (Davis 1989). The ease of data collection has a major impact on the client in terms of accepting the Biometric Technology. For example, Retinal Scan in general faces maximum negative reaction compared to all other biometric techniques because of the difficulty to accomplish precise alignment during the scan. Biometric Technology must be easy to use during both the enrollment and verification (Prabhakar et al. 2003) phases. Thus, the ease of the process and the time required to enroll, verify, or identify a person is of critical importance to the acceptance and applicability of the system. The users who perceive Biometric Technology to be easy to use will be likely to use this technology. Thus,

> ***Hypothesis 2: Perceived ease of use is positively related to the perceived intention to use Biometric Technology.***

Compatibility

Biometric Technology needs the users to change the way they work. Compatibility measures the degree to which the use of Biometric Technology is compatible with, or requires changes in the way an individual performs the task. The more users perceive that they have to change; the less likely they are to use the technology. Thus,

> ***Hypothesis 3: Perceived compatibility is positively related to the perceived intention to use Biometric Technology.***

Trialability

It measures the extent to which the users perceive that they have an opportunity to experiment with the technology prior to committing to use the same. Depending on the type of Biometric Technology in use, the users will take different approaches to experiment and understand the technology. The more they perceive that they can experiment with the technology and personally explore the same, more likely are they to use the technology. Thus,

> ***Hypothesis 4: Perceived trialability is positively related to the perceived intention to use Biometric Technology.***

Perceived Risk to Privacy

Privacy is related to the accessibility of personal information that an individual is ready to provide to others. This is particularly relevant in an individual's adoption decision concerning Biometric Technology. Currently, people are not concerned about the cameras installed at various locations. But when organizations keep a record of facial data for authentication purpose, there is a great chance of user getting wary as the two data sources can be linked together to get some personal / private information about the person. Since Biometric Technologies are based on unique characteristics, the possibility of misusing this information may be perceived as a risk to the privacy of an individual (Elgarah and Falaleeva 2005). The more the users perceive this risk, less likely are they to use the technology. Thus,

> ***Hypothesis 5: Perceived risk to privacy is negatively related to the perceived intention to use Biometric Technology.***

Users are supposed to be rational in performing any task. According to rational choice theory, they tend to weigh cost and benefit before doing any task. The concerns of privacy will outweigh the benefits users receive in terms of using the technology and will perceive the technology of not being useful. Thus,

> ***Hypothesis 6: Perceived risk to privacy is negatively related to the perceived usefulness of the Biometric Technology.***

The technology may be perceived to be easy to use, be perceived to be compatible with the work user needs to do, or perceived to be available to try before committing for the same. However, if the users perceive some risk associated with the trial of the technology, they will not be inclined to use it, hereby lowering their intention to use the technology. In other words, the perceived risk to privacy will moderate the relationship between perceived ease of use, and / or perceived trialability, and / or compatibility and intention to adapt the technology. Thus,

> ***Hypothesis 7: Perceived risk to privacy will moderate the impact of perceived ease of use and the perceived intention to use Biometric Technology.***

Hypothesis 8: Perceived risk to privacy will moderate the impact of perceived compatibility and the perceived intention to use Biometric Technology.

Hypothesis 9: Perceived risk to privacy will moderate the impact of perceived trialability and the perceived intention to use Biometric Technology.

Subjective Norms

Subjective norm is defined as a "person's perception that most people who are important to him think he should or should not perform the behavior in question" (Fishbein and Ajzen 1975). In the present context, a co-worker or manager's expectation of using Biometric Technology may make an individual believe that using a system will enhance his or her performance, hereby increasing the perceived usefulness of the technology. Thus,

Hypothesis 10: Perceived subjective norm is positively related to the perceived usefulness of Biometric Technology.

Also, if the subjective norm suggests that there is not much concern for privacy in the use of Biometric Technology, it may actually reduce the concern of privacy as perceived by the user. This, in turn, will lead to form an intention to use it. Thus,

Hypothesis 11: Perceived subjective norm is negatively related to the perceived risk to privacy.

CONCLUSION

A successful implementation of Biometric Technology is dependent on users' perception and acceptance of this technology. Understanding the antecedents that are the determinants of users' intention to use such technology is crucial for the practitioners. Using a richer model based on (Moore and Benbasat (1991), this study addresses the issue of the relation between risk to privacy and the innovation characteristics along with their combined effect on the use of Biometric Technologies. The study will use survey methodology to empirically test the research model shown in Figure 1. The survey instrument is ready for the pilot test in an organization that is using fingerprinting in a voluntary setting to give controlled access to the users.

REFERENCES

Agarwal, R. and J. Prasad (1998). "A conceptual and operational definition of personal innovativeness in the domain of information technology." Information Systems Research.

Bolle, R. M., J. H. Connell, et al. (2004). Guide to Biometrics, Springer.

Chin, W. W. and A. Gopal (1995). "Adoption intention in GSS: relative importance of beliefs." Database Advances 26(2&3).

CSI/FBI (2005). "2005 CSI/FBI Computer crime and Security Survey."

Davis, F. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." MIS Quarterly 13: 319-340.

Elgarah, W. and N. Falaleeva (2005). Adoption of Biometric Technology: Information Privacy and TAM. Proceedings of the Eleventh Americas Conference on Information Systems.

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

International Biometric Group (2004). Biometrics Market and Industry Report 2004-2008, http://www.biometricgroup.com/reports/public/market_report.html.

Mathieson, K. (1991). "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior." Information Systems Research 2(3): 173-191.

Mitnick, K. D. (2003). "Are You the Weak Link?" Harvard Business Review 81(4): 18-20.

Mitnick, K. D. and W. L. Simon (2002). The art of deception: Controlling the human element of security, Indianapolis, Ind.: Wiley.

Moore, G. C. and I. Benbasat (1991). "Development of an instrument to measure the perceptions of adopting an information technology innovation." Information Systems Research 2(3): 173-191.

Plouffe, C. R., J. S. Hulland, et al. (2001). "Research Report: Richness versus Parsimony in Modeling Technology Adoption Decisions--Understanding Merchant Adoption of a Smart Card-Based Payment System.

Prabhakar, S., S. Pankanti, et al. (2003). "Biometric Recognition: Security and Privacy Concerns." IEEE SECURITY & PRIVACY March.

Reid, P. (2004). Biometrics for Network Security,

Rogers, E. M. (1995). Diffusion of Innovation, Free Press.

Wade, J. (2004). "The Weak Link in IT Security." Risk Management 51(7): 32-36.

Whitman, M. E. and H. J. Mattord (2003). Principles of Information Security, Thompson Course Technology.

Woodward, J. D. (1997). "Biometrics: Privacy’s Foe or Privacy’s Friend?" PROCEEDINGS OF THE IEEE 85(9).