Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

Adoption of Biometric Technology: Information Privacy in TAM

Wafa Elgarah
Al Akhawayn University, w.elgarah@aui.ma

Natalia Falaleeva
Loyola College in Maryland, nfalaleeva@loyola.edu

Adoption of Biometric Technology: Information Privacy and TAM

Wafa Elgarah
Al Akhawayn University
w.elgarah@aui.ma

Natalia Falaleeva
Loyola College in Maryland
nfalaleeva@loyola.edu

ABSTRACT

This paper (work in progress) investigates how the individual's concern for information privacy affects the adoption of biometric technologies. Biometrics refers to the automated authentication of an individual based on his/her distinguishing characteristics (Bolle et al. 2004). Given the very personal nature of biometric technologies, their adoption may be inhibited by individual's concern for information privacy. This research develops a model of biometrics adoption that integrates information privacy and TAM. This model aims to assist researchers and practitioners in understanding the factors that affect biometrics adoption. To examine the effects of TAM and privacy on intentions to use biometric technology, a pretested instrument will be administered to medical personnel who use finger scanning equipment to retrieve drugs in a hospital.

Keywords

Concern for information privacy, TAM, Biometrics.

INTRODUCTION

International Biometrics group estimates the total revenues in the biometrics market to reach 5 billion U.S. dollars by 2008. The market has been growing rapidly with biometric technologies being deployed in transportation, healthcare, law enforcement, financial and government sectors. With the increasing proliferation of biometric technologies, the issue of personal information privacy has gained increasing importance. This paper investigates the role of individual's concern for information privacy (CFIP) in the acceptance and use of biometric technologies. Understanding how CFIP impacts intention to use biometric technology will certainly help both researchers and practitioners to direct their efforts in successful development and implementation of biometrics.

Biometrics involves the automated authentication of an individual based on his or her distinguishing physical characteristics (Bolle, Connell, Pankanti, Ratha and Senior, 2004). Biometric system can use any personal physical or psychological trait that can be measured, recorded, quantified and stored in its digital representation. Based on the original enrollment authentications, the recorded trait is used to determine with a degree of certainty that an individual is the same person during the subsequent biometric authentication (Reid, 2004).

Depending on the implementation of the system, biometrics is argued to either threaten or enhance individual's information privacy (Albrecht, 2003; Reid, 2004; Tomko, 1998). On one hand, biometrics is viewed as privacy and security enhancing. The proponents of biometrics argue that authentication that is available with biometrics ensures that only the authorized individual gets access to a particular service or product. Biometrics, thus, can be used to prevent identity theft and enhance security. While biometrics does not eliminate the possibility of security breach, it helps to ensure that the systems are difficult to compromise and as a result ensures the privacy of the information (Fulcher, 2004). On the other hand, biometric data, even if it is only stored for the purposes of authentication, can also be used for identification, and as such can inhibit individual privacy. Storing biometric data either on a chip or data server raises concerns of possible misuse of such data, access to it by unauthorized individuals and tracking of individuals using their uniquely identifiable traits. As a result, there is an increasing concern with information privacy associated with the adoption of biometrics.

Information privacy describes the individual's ability to control the release and possible subsequent dissemination of information about him or her (Stone and Stone, 1990). Individual's concern for information privacy involves several dimensions. The first one deals with the collection of personal information, and pertains to the individual's concern about the quantities of personal data being collected. The second dimension, unauthorized secondary use, addresses individual's concerns about the use of collected personal data for purposes other than the ones originally stated. The third dimension relates to improper access and whether or not unauthorized individuals or organizations may have access to the data. Finally,

the fourth dimension pertains to presence of accidental or deliberate errors in the collected data and how such erroneous information may affect the individual (Smith, Milberg and Burke, 1996).

RESEARCH MODEL

Given the increased adoption of biometric technologies in various sectors of economy and government, it's interesting to examine the role of the concern for information privacy in the use of biometric technologies. This study develops and tests a user acceptance model of biometric technologies (Figure 1). The research model suggests that user acceptance of biometric technologies is affected by individual's concern for privacy, perceived usefulness and perceived ease of use. Next, the constructs and the hypotheses related to the relationship between the constructs are discussed.

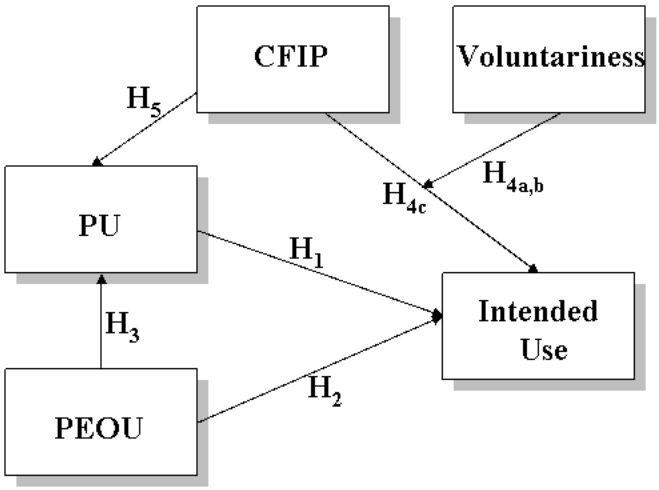

Figure 1. Research Model

TAM and Biometrics

Biometrics is an information technology (IT) innovation, and hence, its user acceptance can be explained using the Technology Acceptance Model (TAM). TAM has been used in multiple research studies to explain IT user acceptance (Davis, Bagozzi and Warshaw, 1989; Gefen and Straub, 2000; Gefen, Karahanna and Straub, 2003; Mathieson, 1991). Empirical results demonstrated that it is a robust and parsimonious model compared to other user acceptance models (Geffen and Straub, 2000; Taylor and Todd, 1995). According to TAM, there are two main constructs that affect the user behavior al intention to accept a new innovation: (1) perceived usefulness (PU) and (2) perceived ease of use (PEOU). PEOU is defined as "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989, p.320). PU is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p.320). Considerable TAM research have examined user acceptance in organizational settings (Davis, Bagozzi, et al., 1989; Gefen and Straub, 2000; Mathieson, 1991;). We hypothesize that PU, PEOU and User acceptance relationships will still apply in the case of biometrics technology.

H_1. PU will positively affect intended use of biometrics.

H_2. PEOU will positively affect intended use of biometrics.

H_3. PEOU will positively affect PU of biometrics.

CFIP, Voluntariness and Intended Use

The fact that biometric technologies are based on unique physical and physiological characteristics (finger print, iris scan, etc) poses a threat to individual's privacy. Additionally, individuals fear that these distinctive identifiers can then be used to link disparate databases and information, and eventually track everyone. Possible use or misuse of this information creates a concern for information privacy on the part of individual. These concerns will certainly affect the way people perceive biometric technology, and hence, their intention to use it. Biometric technology may be introduced voluntarily or the user

may be required to use it to perform their job duties. In many organizations the use of biometric equipment is mandatory. As part of their job employees have to use biometric technology for authentication and access to resources, data or certain locations. When biometric authentication is mandated by the employer user's CFIP can not prevent them from using the system. However, in the situations where biometrics is voluntary, users that are more concerned about their privacy are less likely to use the system. Several studies have investigated the role of perceived voluntariness in technology acceptance (Agarwal and Prasad, 1997, Moore and Benbasat 1991, Venkatesh and Davis 2000). Voluntariness refers to the extent to which potential users of biometrics perceive use of such system as non-mandatory (Moore and Benbasat, 1991). Voluntariness has been empirically proven to be significant in explaining current usage (Agarwal and Prasad, 1997). In our case, we hypothesize that voluntariness will moderate the relationship between concern for information privacy and intention to use biometrics.

H4a. CFIP will have no significant effect on intention to use when system use is perceived to be mandatory.

H4b. CFIP will have a negative effect on intentions to use when the system use is voluntary.

H4c. Voluntariness will moderate the effect of CFIP on intentions to use.

CFIP and PU

Biometrics is regarded as the highest level of security, it provides the most secured form of authentication and verification than the current authentication technologies can offer. Advocates of this technology posit that benefits of biometric methods include the fact that they cannot be stolen like password or PINs, and that one does not need to remember different passwords for different applications. Despite these benefits, biometrics have been shunned by privacy advocates (Albrecht 2003; Reid 2004; Tomko 1998). The ultimate threat to privacy comes from the uniqueness of identifiers and the possible convergence of huge data warehouses from different databases. This lack of control over how personal biometric information will be used increases the significance of this privacy threat. Increase in the importance of privacy is exemplified in the many new laws and regulations around the globe dealing with this issue. As a result, the concern for information privacy is expected to decrease certain aspects of perceived usefulness of biometrics. We hypothesized that CFIP will negatively affect perceived usefulness of biometrics.

H_5. CFIP will negatively affect PU.

METHODOLOGY

Data will be collected from hospitals in Florida that have adopted biometric technology to retrieve certain drugs and narcotics from the medicine storage. An online survey will be administered to the medical personnel that uses finger scanning equipment. In order to measure CFIP the 15-item, 4 scale survey instrument developed by Smith, Milberg and Burke (1996) is used. This instrument was tested for validity and reliability on multiple US samples (students, professionals, consumers). To operationalize PU and PEOU, we adapted the standard TAM scales developed by Davis (1989). To measure voluntariness, we used the three-item scale developed by Moore and Benbasat (1991). All items are reworded to reflect the context of biometrics. To ensure the appropriateness of the adapted items to the biometrics context the questionnaire is reviewed by 5 individuals (two IS academics and three users of biometric equipment in the hospital settings).

IMPLICATIONS

The use of biometric technology is growing across various industries and government sector. Identifiable physiological features of individuals stored in databases and later used for authentication. In some cases the use of biometric equipment is voluntary, e.g. finger scan to purchase groceries in the store or finger scan to enter the gym. In other cases it is mandated by either the employer or even government (e.g. all non US citizens have to submit to finger scanning and facial recognition when entering the US). Among individuals there is an increasing concern for information privacy and the way the unique biometric data is stored and used. Understanding the influence of the concern for information privacy on intention to use biometrics can provide insights into the implementation of various biometric technologies. Such a concern may hinder user acceptance of biometrics in voluntary settings, and cause dissatisfaction in mandatory environment.

REFERENCES

1. Agarwal, R. & Prasad, J. (1997) The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies, *Decision Science*, 28, 3, 557-582.
2. Albrecht, A. (2003) Privacy Best Practices, *Biometric Technology Today*, 11, 11, 8-9.
3. Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N., and Senior, A.W. (2004) Guide to Biometrics, New York.

4. Davis, F. D. (1989) Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology, *MIS Quarterly*, 13, 3, 319-340.
5. Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989) User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, *Management Science*, 35, 8, 982-1003.
6. Fulcher, J. (2004) The Use of Patient Biometrics in Accessing Electronic Health Records, *International Journal of HealthCare Technology and Management*, 6, 1, 20-31.
7. Hoffman, D. L., Novak, T. P., and Peralta, M. (1999) Information privacy in the marketspace: Implications for the commercial uses of anonymity on the web, *Information Society*, 15, 4, 129-139.
8. Gefen, D., and Straub, D. W. (2000) The Relative Importance of Perceived Ease-of-Use in IS Adoption: A Study of E-Commerce Adoption, *Journal of the Association for Information Systems*, 1, 8, 1-30.
9. Gefen, D., Karahanna, E. and Straub, D. W. (2003) Trust and TAM in Online Shopping: An Integrated Model, *MIS Quarterly*, 27, 1, 51-90.
10. Mathieson, K. (1991) Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior, *Information Systems Research*, 2, 3, 173-191.
11. Mason, R. O. (1986) Four ethical issues of the information age, *MIS Quarterly*, 10, 1, 4–12.
12. Moore, G, C. and Benbasat, I. (1991) Development of an instrument to measure the perceptions of adopting an information technology innovation, *Information Systems Research*, 2, 192-222.
13. Reid, P. (2004) Biometrics for Network Security, Prentice Hall PTR, Upper Saddle River, NJ.
14. Smith, H.J., Milberg, S.J., and Burke, S.J. (1996) Information Privacy: Measuring Individuals' Concerns About Organizational Practicies, *MIS Quarterly*, 20, 2, 167-196.
15. Stone, E.F., and Stone, D.L. (1990) Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms, in: *Research in Personnel and Human Resources Management*, G.R. Ferris and K.M. Rowland (eds.), JAI Press Inc, Greenwich, CT, 349-411.
16. Taylor, S., and Todd, P. A. (1995) Understanding Information Technology Usage: A Test of Competing Models, *Information Systems Research*, 6, 2, 144-176.
17. Tomko, G. (1998) Biometrics as a Privacy-Enhancing Technology: Friend or For of Privacy, *Privacy Laws & Business 9th Privacy Commissioners'/Data Protection Authorities Workshop*, Santiago de Compostela, Spain.
18. Venkatesh, V. and Davis, F. D. (2000) A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, *Management Science*, 46, 2, 186-204