Chapter XIV

The Impact of Privacy Risk Harm (RH) and Risk Likelihood (RL) on IT Acceptance: An Examination of a Student Information System

Joseph A. Cazier
Appalachian State University, USA

E. Vance Wilson
Arizona State University, USA

B. Dawn Medlin
Appalachian State University, USA

ABSTRACT

In today’s networked world, privacy risk is becoming a major concern for individuals using information technology. Every time someone visits a website or provides information online they have exposed themselves to possible harm. The information collected can be sold to third parties or kept by the site owners themselves for use in creating a profile of users’ preferences and tastes. To gain insight into the role risk plays in the adoption process of technology, the authors studied the use of information systems in relation to a student registration and schedule management system at a major United States university. Further, they extended the Technology Acceptance Model (TAM) to include perceptual measures of privacy risk harm (RH) and privacy risk likelihood (RL) which apply to the extended model and predict students’ intentions to use technology. Their finding indicated the growing importance of privacy risk in the use of information technology.
INTRODUCTION

The past few decades have seen the proliferation of information technology (IT) into virtually every aspect of the personal and professional lives of Americans. As a nation, we regularly employ information technologies to file taxes, conduct banking and financial transactions, order pizzas, and even search for a mate. The general trend has been to consider IT in terms of the benefits that can accrue to individuals or organizations. However, information technology is “morally neutral” in that it can be employed for either positive or negative uses (Conca, Medlin, & Dave, 2005, p. 167). As an example, e-mail can be a highly useful form of communication in routine work situations or for sharing information among friends or family. However, email can also be used for the dissemination of malicious computer code and viruses such as the case with the Email-Worm.Win32.NetSky. in 2008 that spread using the Internet as an attachment to infected messages. It is also able to propagate via P2P networks and accessible http and ftp directories (VirusList.com, 2008).

Privacy concerns are among some of the largest fears that Americans have identified when using information technologies (Garfinkel, Gopal and Goes, 2002), and privacy practices appear as a key determinant of trust for websites (Bart, Shankar, Sultan and Urban, 2005). In response to negative occurrences, many Americans have discontinued activities formerly done online - for example, a recent IBM study finds 18% of participants have stopped paying bills online and that most Americans believe they are more likely to be a victim of a cyber attack than a physical crime (IBM, 2006).

Where in the past security was mainly the responsibility of the consumer, most of the privacy risks today are controlled by others, such as third party vendors or e-commerce organizations. As individuals lose control of their information and incidents occur such as identity theft, anxiety and stress will likely increase, making it even more important to study privacy risk today than in the past (Schneier, 2005). Certainly, as more individuals have given up control of their information, opportunities for abuse have escalated. Consumers must balance the cost of supplying information with the benefits received from providing it (Ng-Kruelle, Swatman, Rebne, Hampe, 2002). This balancing act is often a difficult one, as consumers begin to rely on more online services.

In the future, privacy risk will likely be even more important as mobile commerce introduces new security and privacy risks above and beyond those of simple online e-commerce activities (Gosh and Swaminatha, 2001). This transition requires that privacy become an even more important issue to understand as we currently prepare to adopt this new type commerce and the technologies that it incorporates.

We propose that it is becoming increasingly important to evaluate individuals’ risk perceptions in understanding the adoption and use of IT. This paper presents an exploratory study of the role of users’ perceived privacy risk (PPR) as measured by its components risk harm (RH) and risk likelihood (RL) in forming behavioral intentions toward continued use of IT. In the following sections we briefly review the IT acceptance literature and then define the elements of risk relating to privacy of individuals and organizations.

THEORETICAL DEVELOPMENT

We frame this paper as an extension of the Technology Acceptance Model (TAM) (Davis, Bagozzi, & Warshaw 1989). TAM is a derivation of the theory of reasoned action (TRA) (Ajzen & Fishbein, 1980) that is customized for prediction of IT adoption and use. TRA and TAM represent a rational decision-making approach to the prediction of behaviors in which individual beliefs are mediated by attitude and behavioral intentions leading to subsequent use or non-use of technologies. For example, TAM posits that