2018

Technology humanness, trust and e-government adoption

Lemuria Carter
The University of New South Wales, lecarter@vt.edu

Dapeng Liu
Virginia Commonwealth University, liud22@mymail.vcu.edu

Technology humanness, trust and e-government adoption

Lemuria Carter
School of Information Systems & Technology Management
University of New South Wales
Sydney, New South Wales, Australia
Email: Lemuria.Carter@unsw.edu.au

Dapeng Liu
School of Business
Virginia Commonwealth University
VA, United States
Email: liud22@vcu.edu

Abstract

With regards to technology adoption, users may be influenced by trust in two forms – human-like trust (e.g., benevolence, integrity, and ability) and system-like trust (e.g., helpfulness, reliability, and functionality). While the literature interestingly differentiates the use of these two types of trust, insufficient efforts have been devoted to examine and explain which type of trust should be used in the context of e-government. Additionally, when government agencies increasingly experience security breaches, insufficient literature examines how human-like trust and system-like trust may be influenced by such important antecedents as security threats and citizens' security concerns in e-government settings. We propose a conceptual model to address this gap in the literature.

Keywords: e-government, human-like trust, technology-like trust, system adoption, security concerns

1 Introduction

Information systems (IS) studies have been manifesting increasingly individuals trust in information technologies. Extant literature shows users' trust can crucially influence their intention of technology adoption. A large portion of IS researchers conceptualized trust in technology as if the technology were a human, utilizing and measuring the human-like trust constructs of integrity, ability/competence, and benevolence (Lankton, McKnight, & Tripp, 2015). In contrast, other IS scholars use system-like trust constructs to measure trust, such as reliability, functionality, and helpfulness (Mcknight, Carter, Thatcher, & Clay, 2011).

e-Government utilizes information and communication technology (ICT) to provide open and secure online services that can enhance the process of public service, administration and participation (Janowski, 2015). Trust beliefs are important in fostering e-government adoption. While IS literature interestingly differentiates the human-like trust and system-like trust (Lankton et al., 2015) and suggests that trust beliefs may not be invariant across various settings (e.g., cultures and contexts) (Jarvenpaa, Tractinsky, & Saarinen, 1999), insufficient studies exist to examine and explain which type of trust should be used in the settings of e-government service. Additionally, no e-government literature demonstrates how human-like trust and system-like trust are affected by such important antecedents as security threats and citizens' security concerns when government agencies are increasingly falling victims to cyber-attacks.

Given that current research is limited in its exploration of human-like trust and system-like trust in e-government settings, our study addresses this gap in the literature by exploring the following research question: how does human-like trust and system-like trust impact e-government service adoption? To explore this question, we present a conceptual model to examine human-like trust or system-like trust and their antecedents in e-government adoption. In particular, we adapt Lankton et al. (2015) to an e-government context. Given the potential impact of security concerns on trust in the digital environment, we extend the model to incorporate security breach concern. The proposed model provides a parsimonious approach to exploring the role of trust and security concerns in e-government.

2 Relevant Concepts and Theoretical Background

2.1 Trust – System-like Trust and Human-like Trust in Technology

Trusting in information technology proves to be reasonable —editors can trust office processing software to process text and web users can trust the Internet to transfer data (Lankton et al., 2015).

Interpersonal trust is often measured in three dimensions of human-like beliefs: integrity, competence, and benevolence (Lankton et al., 2015; McKnight, Choudhury, & Kacmar, 2002) (Figure 1). IS studies have used these human-like trust to study technology because people tend to ascribe human characteristics to information technology (Nowak & Rauh, 2005). Integrity is the belief that a trustee "adheres to an acceptable set of principles" (Lankton et al., 2015). Ability/competence is the belief that a trustee has the ability, skills or competencies to implement a task or to be influential in a specific domain. Benevolence is the belief that a trustee "wants to do good to the trustor aside" (Lankton et al., 2015). These human-like trust has been examined to be significantly influential towards system adoption (Lankton et al., 2015; Wang & Benbasat, 2005).

While human-like trust in technology assume that technology "have volition (the power to choose)", other studies have developed alternative trust measurements that do not assume technologies have volition, such as utility, reliability, and predictiveness (Lippert & Swiercz, 2005) and reliability, functionality, and helpfulness (Lankton et al. (2015). This study will use Lankton et al. (2015)'s conceptualization of system-like trust in a technology (reliability, functionality, and helpfulness) for two-fold reasons: on the one hand, this study is a follow-up study of Lankton et al. (2015), empirical examining whether and how system-like trust and human-like trust differentially performs in e-government adoption; on the other hand, the attributes of system-like trust from Lankton et al. (2015) were conceptually congruent with those in human-like trust.

Human-like trust and system-like trust portray users' trust in e-service from two different perspectives. This differentiation applies in the practice of building e-government services which aims at providing enhanced system friendliness and accordingly increasing user satisfaction. In this sense, e-government services are increasingly subject to more humanness (or human-like characteristics). Social cognitive theories posit that people categorize subjects into humans, animals, or objects (Nowak & Rauh, 2005). While a technology has historically been categorized as an object (i.e., not human), IS/IT can "display certain human characteristics that make them seem quite human-like" (Cassell & Bickmore, 2000). We

are motivated to test how human-like trust performs versus system-like trust in the specific setting of e-government.

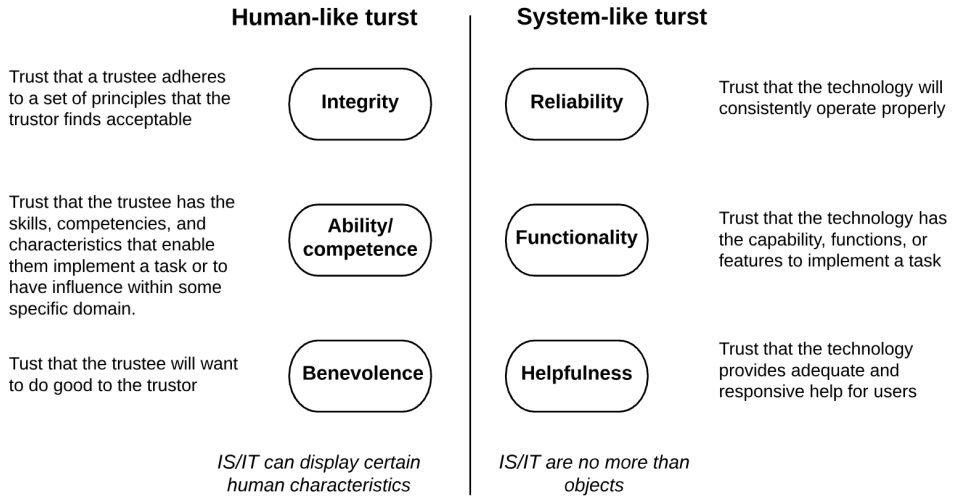

Figure 1. Trust in Technology Adapted from Lankton et al. (2015)

2.2 Security threats and concerns

Security in e-government settings is of crucial importance to citizens, businesses, and government agencies. Security breaches of e-government transactions and databases will harm citizens' confidential information (e.g., social security number, address, and password) and can result in identity theft (Featherman, Miyazaki, & Sprott, 2010).

In reality, security breaches are occurring at a growing rate. In recent years, government agencies continue to lose citizens' confidential information. In 2016, government agencies reported 30,899 data breach incidents, 16 of which are deemed as major incidents. For example, in the Internal Revenue Service (IRS) breach covering September 2016 to March 2017, approximately information of 100,000 taxpayer may have been compromised (Ng, 2017).

Among internet users' concerns, system security breaches ranked at the top (Miyazaki & Fernandez, 2001). System users report that security concerns adversely affect their behaviour towards adoption (Featherman et al., 2010). While an investigation of security concerns surrounding the adoption of e-government services is necessary, IS literature manifest limited efforts.

Acknowledging insufficient efforts have been devoted to the examination of security threats and security concerns in e-government setting, this study will fill this gap by examining their effects towards trust in terms of system-like trust and human-like trust.

3 Hypothesis Development

3.1 Security Threat, Security Breach Concern and Trust

In the IS context, system security threats can be visualized in terms of the individual assessment of the severity of potential security threats and the probability of exposure to substantial security threats (Herath & Rao, 2009, p. 111). According to the Protection Motivation Theory (PMT), security threats may arouse security concerns which can be defined as "the level to which an employee believes that her/his organizational information assets are threatened" (Herath & Rao, 2009, p. 111). In the e-government context, if citizens perceive that a security threat can impose notable damages or losses, they are more likely to be concerned. Conversely, if citizens do not perceive severe security threats, they will give no or less concern. In other words, security breach severity and probability arouse in system users the security concerns, potentially offsetting the trust in e-government and the convenience afforded to citizens.

H1a *Perceived Probability of Security Breach will negatively affect Human-like Trust*
H1b *Perceived Probability of Security Breach will negatively affect System-like Trust*
H1c *Perceived Probability of Security Breach will positively affect Security Breach Concern*
H2a *Severity of Security Breach will negatively affect Human-like Trust*

H2b *Severity of Security Breach will negatively affect System-like Trust*
H2c *Severity of Security Breach will positively affect Security Breach Concern*

Literature highlights that individual concerns are an essential influential antecedent factor of trust (Bansal & Gefen, 2010; Bansal, Zahedi, & Gefen, 2016; Van Slyke, Shim, Johnson, & Jiang, 2006). Security breaches subject citizens' confidential information to loss or theft and may severely harm them financially or socially (Mothersbaugh, Foxx, Beatty, & Wang, 2012) and raise security concerns. Security breach concern, considered as a personal belief, may lower trust towards the e-government. In other words, a high level of security breach concern is likely to be associated with a low-level trust in e-government service in terms of the human-like trust or system-like trust. Therefore, we posit that security breach concerns negatively impact trust.
H3a *Security Breach Concern will negatively affect Human-like Trust*
H3b *Security Breach Concern will negatively affect System-like Trust*

3.2 Trust and Dependent Variable

Trust holds a crucial stance in influencing individual perceptions and behaviours (Schurr & Ozanne, 1985), especially in an uncertain environment (Chellappa & Pavlou, 2002). Hence, trust is crucial in online relationships between individual and organization where there often exists asymmetrical information (Moody, Lowry, & Galletta, 2017), context (Graebner, 2009) and expectations (Hann, Hui, Lee, & Png, 2007), manifesting system success (Bélanger & Carter, 2008; Gefen, Karahanna, & Straub, 2003; McKnight et al., 2002; Pavlou & Gefen, 2004).

3.2.1 Trust and Perceived Usefulness

In the setting of e-government, perceived usefulness is an important indicator portraying how a person believes that using the e-government system will enhance his/her performance or outcome. It is a well-documented belief that the users will be more likely to successfully accomplish their tasks with the supporting e-service which can be trusted. Trust builds the e-service credibility in "providing what has been promised" (Gefen et al., 2003). Conversely, working with an e-service which is not credible and cannot be trusted often result in detrimental consequences. E-government research also manifests trust being influential towards perceived usefulness (Horst, Kuttschreuter, & Gutteling, 2007). Therefore, we hypothesize trusting beliefs (human-like and system-like) into e-government would benefit citizens' perception of usefulness.
H4a *Human-like trust will positively affect perceived usefulness.*
H4b *System-like trust will positively affect perceived usefulness.*

3.2.2 Trust and Enjoyment

Enjoyment can be defined as the degree to which performing an activity is perceived as providing pleasure and joy in its own right, other than perceived performance consequences (e.g. perceived usefulness) (Igbaria, Schiffman, & Wieckowski, 1994). In the context of IS, enjoyment is often measured by the perceived fun pleasure of using a system or online service (Lankton et al., 2015). While enjoyment is a behavioral belief that represents pleasure-relevant motivation for e-government use, trusting beliefs may impact enjoyment in the way that the more individuals trust a technology and perceive that e-government has trustable features that may reduce uncertainty, the more they will feel comfortable (and, thus, enjoy) using e-government services. Literature has examined the relationship between trust and enjoyment and found that both human-like trusting beliefs and system-like trust significantly influence enjoyment in online payment systems (Lankton et al., 2015). Therefore, we synthesize that:
H5a *Human-like trust will positively affect Enjoyment.*
H5b *System-like trust will positively affect Enjoyment.*

3.2.3 Trust and Trusting Intention

Trusting beliefs are object-specific beliefs about characteristics of IT/IS system or relevant entities (Wixom & Todd, 2005). Trusting intention depicts an object-oriented attitude which results from trusting belief in these technology characteristics and reflects users' evaluative response to these characteristics (Benamati, Fuller, Serva, & Baroudi, 2010). In e-government setting, trusting beliefs should influence trusting intention because citizens who have high trusting beliefs will perceive that the trustee (e.g., e-government service) has desirable characteristics that enable trusters (e.g., citizens) to depend on it. Previous literature demonstrated that trust beliefs have significant influences on trust intentions (McKnight et al., 2002). Especially, researchers have found a relationship between both human-like (Benamati et al., 2010; Lankton et al., 2015) and system-like (Lankton et al., 2015) trusting beliefs and trusting intention.
H6a *Human-like trust will positively affect Trusting Intention.*

H6b *System-like trust will positively affect Trusting Intention.*

3.2.4 Trust and Continuance Intention

Trust strongly impacts technology adoption (Warkentin, Gefen, Pavlou, & Rose, 2002). Especially, citizens' trust in the government agencies' capability of providing secure e-services is vitally important for e-government adoption (Carter, Weerakkody, Phillips, & Dwivedi, 2016). Existent literature provides accumulated empirical evidences that trust in technology foster acceptance or continued acceptance of various technologies such as online banking service (Lin, 2011), supply chain information systems (Lippert, 2007), recommender system (Wang & Benbasat, 2005), e-commerce (Corbitt, Thanasankit, & Yi, 2003), and e-government services (Bélanger & Carter, 2008; Carter et al., 2016). More specifically, as trust in the form of human-like trust and system-like trust, portray user's wholistic belief in e-government service, we hypothesize that:
H7a *Human-like trust will positively affect Continuance Intention.*
H7b *System-like trust will positively affect Continuance Intention.*

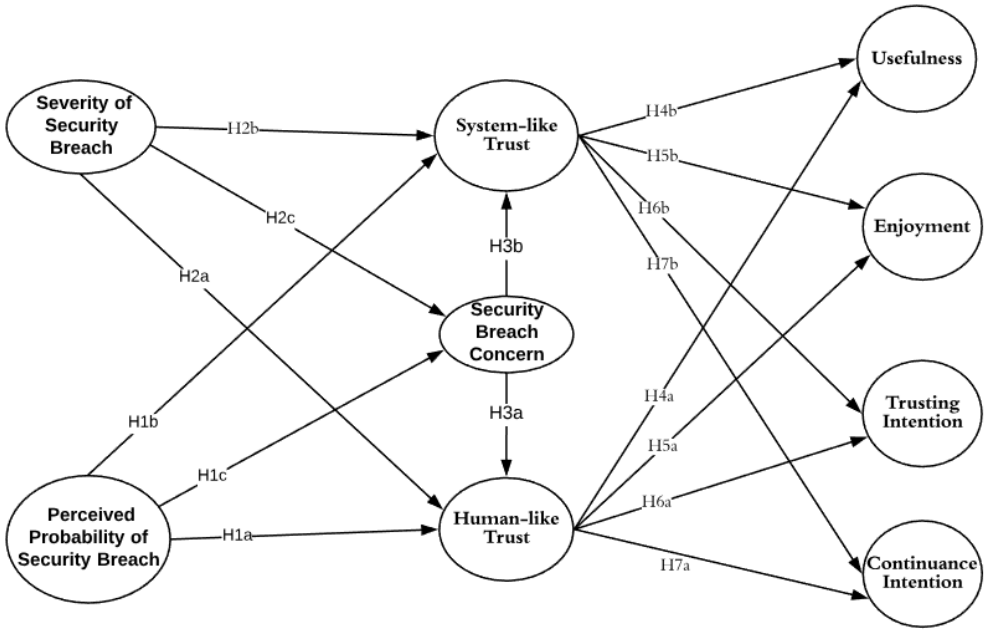

Figure 2. Conceptual Model

4 Research Model Conceptualization

Based on the aforementioned analysis, this research proposes the model (in Fig. 2). Seven groups of hypotheses derived from the model are summarized as H1-H7 mentioned above. As is shown in the research model in Figure 2, this conceptualization investigates the roles of security threat (severity of security breach and perceived probability of security breach), security concerns, and trust (system-like and human like) that leads to dependent variable of interest in e-government adoption.

5 Methodology

To test the proposed research model, we will administer a survey to e-government users in the United States. Empirically testing the proposed research model, which highlights security concerns, trust (system-like trust and human-like trust) and dependent variable listed in Lankton et al. (2015), will address an existing gap in the literature. The instruments to be used are listed in Table 1. All of the questions in the instruments are validated and tested questions in the cited studies, the use of which will reduce the problems with the reliability and validity of results (Straub, 1989). Each item in the instrument involved a 7-point Likert scale which indicate how a respondent agree with the statements.

Construct	Definition	Source
Severity of Security Breach	Seriousness or severity of breach events/incidents in e-government use	Herath and Rao (2009)

Perceived Probability of Security Breach	Perceived vulnerability, in terms of probability, to the thread of breach events/incidents in e-government use	Herath and Rao (2009)
Security Breach Concern	Concern over the e-government breach threat and the coping response efficacy	Herath and Rao (2009)
System-like Trust	System-like trusting beliefs regarding system integrity, ability and benevolence	Lankton et al. (2015)
Human-like Trust	Human-like trusting beliefs regarding system reliability, functionality and helpfulness	Lankton et al. (2015)
Usefulness	Perceived usefulness of e-government services regarding the performance, productivity and effectiveness etc.	Lankton et al. (2015); (Davis, 1989)
Enjoyment	Perceived enjoyment when using e-government services	Davis, Bagozzi, and Warshaw (1992); Lankton et al. (2015)
Trusting intention	Individual trusting intentions on e-government services-willingness to depend on e-government	Lankton et al. (2015); McKnight et al. (2002)
Continuance intention	Intended continued use of a system, which, in turn, will determine actual adoption of e-government services	Lankton et al. (2015);

Control variable: disposition to trust technology, experience, age and gender

Table 1. Constructs and Definitions

6 Discussion

In this paper, we utilize Lankton et al. (2015)'s model of trust to explore the role of human-like and system-like trust on e-government adoption. Given the potential impact of security concerns on trust in the digital environment, we extend the model to incorporate security breach concern. The proposed model provides a parsimonious approach to exploring the role of trust and security concerns in e-government. Implications for research and practice will be discussed at the conference.

7 References

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165-176.

Benamati, J., Fuller, M. A., Serva, M. A., & Baroudi, J. (2010). Clarifying the Integration of Trust and TAM in E-Commerce Environments: Implications for Systems Design and Management. *IEEE Transactions on Engineering Management, 57*(3), 380-393.

Carter, L., Weerakkody, V., Phillips, B., & Dwivedi, Y. K. (2016). Citizen adoption of e-government Services: Exploring citizen perceptions of online services in the United States and United Kingdom. *Information Systems Management, 33*(2), 124-140.

Cassell, J., & Bickmore, T. (2000). External manifestations of trustworthiness in the interface. *Communications of the ACM, 43*(12), 50-56.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358-368.

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: a study of consumer perceptions. *Electronic Commerce Research and Applications, 2*(3), 203-215.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace 1. *Journal of Applied Social Psychology, 22*(14), 1111-1132.

Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal of Services Marketing, 24*(3), 219-229.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90.

Graebner, M. E. (2009). Caveat venditor: Trust asymmetries in acquisitions of entrepreneurial firms. *Academy of Management Journal, 52*(3), 435-472.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13-42.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Horst, M., Kuttschreuter, M., & Gutteling, J. M. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Computers in Human Behavior, 23*(4), 1838-1852.

Igbaria, M., Schiffman, S. J., & Wieckowski, T. J. (1994). The respective roles of perceived usefulness and perceived fun in the acceptance of microcomputer technology. *Behaviour & Information Technology, 13*(6), 349-361.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), JCMC526.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems, 16*(10), 880-918.

Lin, H. F. (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. *International Journal of Information Management, 31*(3), 252-260.

Lippert, S. K. (2007). Investigating postadoption utilization: an examination into the role of interorganizational and technology trust. *IEEE Transactions on Engineering Management, 54*(3), 468-483.

Lippert, S. K., & Swiercz, P. (2005). Human resource information systems (HRIS) and technology trust. *Journal of Information Science, 31*(5), 340-353.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS), 2*(2), 12.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs, 35*(1), 27-44.

Moody, G. D., Lowry, P. B., & Galletta, D. F. (2017). It's complicated: explaining the relationship between trust, distrust, and ambivalence in online transaction relationships using polynomial regression analysis and response surface analysis. *European Journal of Information Systems, 26*(4), 379-413.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: the role of sensitivity of information. *Journal of Service Research, 15*(1), 76-98.

Ng, A. (2017). Hackers Use College Student Loans Tools to Steal $30 million. Retrieved from https://www.cnet.com/news/hackers-used-college-student-loans-tool-to-steal-30-million/

Nowak, K. L., & Rauh, C. (2005). The influence of the avatar on online perceptions of anthropomorphism, androgyny, credibility, homophily, and attraction. *Journal of Computer-Mediated Communication, 11*(1), 153-178.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37-59.

Schurr, P. H., & Ozanne, J. L. (1985). Influences on exchange processes: Buyers' preconceptions of a seller's trustworthiness and bargaining toughness. *Journal of Consumer Research, 11*(4), 939-953.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147-169.

Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(1), 415-444.

Wang, W., & Benbasat, I. (2005). Trust in and adoption of online recommendation agents. *Journal of the Association for Information Systems, 6*(3), 72-101.

Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets, 12*(3), 157-162.

Wixom, B. H., & Todd, P. A. (2005). A theoretical integration of user satisfaction and technology acceptance. *Information Systems Research, 16*(1), 85-102.