Southern University College of Business E-Journal

Volume 16 | Issue 1 Article 3

2022

The Role of Institution Based Trust in IoT Environment: A Theoretical Model

Anupam K. Nath
George Gwinnett College, anath@ggc.edu

The Role of Institution Based Trust in IoT Environment: A Theoretical Model

Anupam K Nath, Ph.D.

Assistant Professor

office: 404-938-3378
cell: 404-938-3378
email: anath@ggc.edu

Georgia Gwinnett College

School of Business
W3127
1000 University Center Lane
Lawrenceville, GA 30043
www.ggc.edu

ABSTRACT

Internet of Things (IoT) is rapidly gaining popularity at the industrial as well as personal level. This rapid adoption of IoT has created privacy, security, and other relevant concerns. In this paper, we develop a theoretical model based on the Trust-based model that can help us understand a user's adoption of an IoT device.

INTRODUCTION

The current trend to interconnect all kinds of devices and systems has produced the increasingly popular paradigm of the "Internet of Things (IoT)." IoT has brought in several benefits to users through increased control, remote management, and volume of available usage information (Atzori & Morabito, 2010). Homes are being converted to "smart" through the integration of IoT technology in various home activities. With numerous benefits due to increased information and control, the technology also introduced various vulnerabilities to allow remote management and communication between devices (Wendzel et al. 2014). These vulnerabilities have raised privacy, security, and overall trust concerns (Menard & Bott, 2018). This is a similar scenario that occurred with the emergence of e-Commerce a few decades ago, and then for M-commerce (Giovannini et al., 2015). Institution-based trust played an important role in understanding users' perceived trust in the E-commerce environment (McKnight et al., 1998). Institution-based trust helps individuals operate within an impersonal and unfamiliar environment (Zucker, 1986). Hence, in this research, we develop a theoretical model to understand the role of Institution-based Trust in IoT Environment. Extant research has identified two dimensions of institution-based trust: structural assurance and situational normality (McKnight et al., 1998). Based on that, in our proposed model, we identify Perceived IoT device quality, Perceived IoT device effectiveness, and Perceived Trustworthiness of IoT device host as the basis of Institution-based Trust in

the context of IoT. This theoretical model serves as a basis for understanding the role of trust in the IoT environment.

LITERATURE REVIEW

Trust can be described as one's willingness to place oneself in a vulnerable position (Mayer et al. 1995), and the expectation that others one chooses to trust will not behave opportunistically by taking advantage of the situation (Gefen et al. 2003). Historically, whenever a new technology arrived where a person has to share information, it created security and privacy issues. In the extant literature, trust played a crucial role in addressing those concerns (Giovannini et al., 2015). Similarly, researchers have also started studying the role of trust in the IoT environment. However, so far, almost all the research works have looked at "Trust" from a technical point of view, not from the consumer's point of view. Aldossari & Sidorova (2018) is one of the very few papers that have studied trust from a consumer's perspective. The paper draws upon the unified theory of acceptance and use of technology and found that trust and security risk play a vital role in accepting IoT. Lee (2019) studied the trust's role in users' perceived security risk in the IoT environment. Esmaeilpour et al. (2020) developed a model for examining the role of the IoT in the development of e-business which includes trust as an important factor. All these show the importance of studying trust in the IoT environment. However, very little effort has been made to study the role of trust in the IoT environment from the consumers' point of view.

THEORY DEVELOPMENT

Trust

Trust has been examined across many disciplines, including but not limited to management, psychology, sociology (Beldad et al., 2010; Butler, 1991; Corazzini, 1977; Lewis and Weigert, 1985; McKnight et al. 2002; McKnight and Chervany, 2000; Muir, 1994). Based on the offline expectation-based trust as a starting point, researchers have elaborated upon one another's definitions and emphasized online environments' specific characteristics to form online trust definitions.

Trust plays a vital role in IoT for reliable data fusion and mining, qualified services with context-awareness, and enhanced user privacy and information security (Accenture, 2015a). Trust becomes even more critical when users share their personal information with their service providers. Home IoT service providers, through the myriad of IoT devices, can collect and store personal information in the real world, and they can access to detailed behaviors of the user (Accenture,2015b)

Efforts have been made to provide consistent measures for trust in the online context that builds upon a solid and theoretical foundation and that have been validated through empirical analysis (McKnight et al., 2002; Pavlou and Gefen, 2004). From E-commerce to Trust has been extended to the M-commerce domain (Giovannini et al., 2015). As the next logical progression, we theoretically develop the Trust concept to the domain of a relatively newer phenomenon- IoT.

Figure 1 provides a graphical depiction of our proposed theoretical model and demonstrates the relationships relevant to our study. The following sections provide a comprehensive overview of the theoretical model.

Institution-based Trust.

Institution-based trust helps individuals operate within an impersonal and unfamiliar environment (Zucker, 1986). Extant research has identified two dimensions of institution-based trust: structural assurance and situational normality (McKnight et al., 1998).

Structural assurance posits that the presence of institutions such as rules and regulations that promote safety and security will increase trust in an environment wherein people are unknown to one another. Situational normality suggests that an environment that is in proper order is conducive to trust, and therefore, successful interaction is possible within that kind of environment.
Due to the importance of trust in the Internet's impersonal environment, structural assurance, and situational normality in institution-based trust have been adapted toward investigations of trust within the e-commerce context. McKnight and Chervany (2002) describe institution-based trust as a key component of successful e-commerce transactions and posit that the consumer's assumptions of legal and regulatory protections are integral to trust formation. Ratnasingam and Pavlou (2002) describe structural institution-based trust in the context of B2B e-commerce as technology trust, which encompasses trust engendered via the presence of technical standards, security, and other protective mechanisms. Keen et al. (2000) and Leonard and Riemenschneider (2008) suggest that the Internet's structural characteristics, such as technical and safety mechanisms, will positively influence trusting

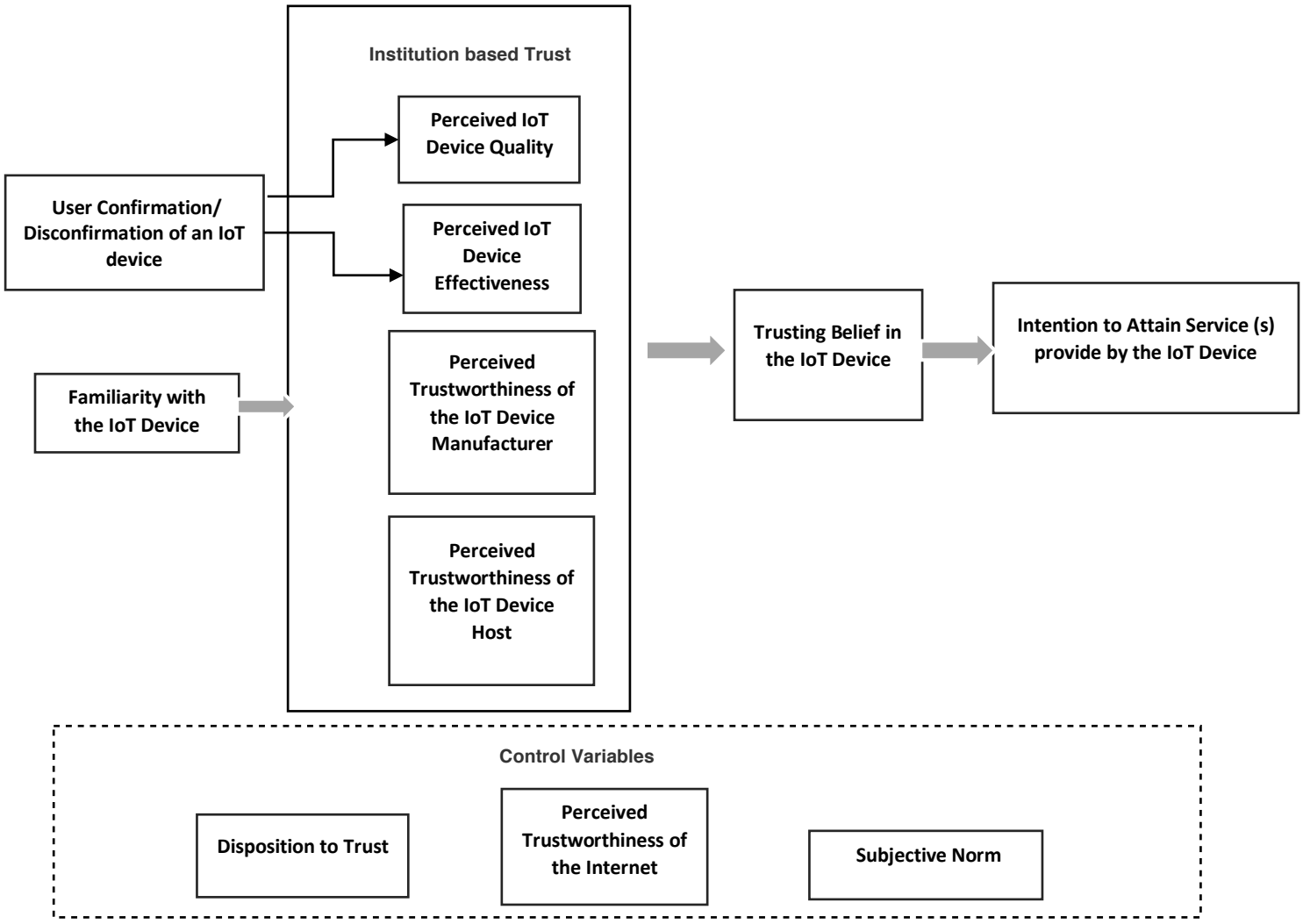

Figure1: Proposed Theoretical Model

beliefs in the online context. In applying the concept of situational normality to the Internet environment, McKnight et al. (2002) suggest that situational normality is high when the consumer perceives the Internet environment as in good order, and vendors in the environment are competent, benevolent, and have integrity. Here competent means is possessing the capability to do a task or fulfill a responsibility, benevolent means morally sound, and have integrity means having truthfulness and honesty.

Following Pavlou (2002,2003), who suggests there is a need to design institution-based trust in specific contexts, we have incorporated four specific components of institution-based trust in the context of IoT environment: Perceived IoT Device Quality, Perceived IoT device Effectiveness, Perceived Trustworthiness of the IoT Device Manufacturer, and Perceived Trustworthiness of IoT Device Host.

User Confirmation/Disconfirmation of an IoT Device.

Expectation Confirmation Theory (ECT) posits that satisfaction depends on the extent to which consumers perceive their initial expectations of a service to be confirmed or disconfirmed during actual use (Oliver, 1980), and has been validated across information systems use behaviors (Bhattacharjee, 2001). In the e-commerce context, ECT expectations refer to consumers' beliefs about the potential utility that can be derived from an e-commerce-based service.

Expectation forms the baseline against which users will form judgments about an IoT device. In the context of institution-based trust in the current study, a user will have expectations of the IoT device's effectiveness and quality that will be confirmed or disconfirmed during actual use. Thus, in the context of this study, we propose that user confirmation/disconfirmation of an IoT device will positively influence his or her perceptions regarding system quality and effectiveness.

Hypothesis 1a (H1a). A user's confirmation/disconfirmation of an IoT device positively influences perceived IoT device quality.

Hypothesis 1b (H1b). A user's confirmation/disconfirmation of an IoT device positively influences perceived IoT device effectiveness.

Familiarity with an IoT Device

A user who is familiar with a particular website has clearer and better understanding of the content, organization, and browsing procedures of the website than individuals who are unfamiliar with the site (Agarwal and Venkatesh, 2002). Such “situational normality” (McKnight et. al., 2002) can be extended toward IoT device s. The underlying assumption is that in general, familiarity with IoT devices will positively influence a person’s trust towards IoT devices, as the person will perceive interaction with IoT devices to be proper and normal. We can apply the theoretical aspect of Task Complexity, which suggests that familiarity with IoT devices is a factor that will positively influence institution-based trust. Studies using task complexity theory, (e.g., Agarwal and Venkatesh, 2002; Cox and Cox, 2002) have

supported the conclusion that the user who is familiar with a particular website has clearer and better understanding of the content, organization, and browsing procedures of the website than individuals who are unfamiliar with the web. Accordingly, a consumer who is comfortable with the Web situation is likely to have high trusting beliefs in a specific vendor in general (McKnight et al., 2002). Our research model suggests that familiarity with *IoT devices* will have a direct and positive relationship with institution-based trust and therefore, indirectly influence trusting beliefs as mediated by each of the components that make up Institution-based Trust in our theoretical model.

Hypothesis 2a (H2a). *A user's familiarity with an IoT device positively influences perceived IoT device quality.*

Hypothesis 2b (H2b). *A user's familiarity with an IoT device positively influences perceived IoT device effectiveness.*

Hypothesis 2c (H2c). *A user's familiarity with an IoT device positively influences perceived Trustworthiness IoT device Host.*

Hypothesis 2d (H2c). *A user's familiarity with an IoT device positively influences perceived Trustworthiness IoT device Host.*

Perceived IoT device Quality

McKnight et al. (2002) suggest that people make trust-related assumptions based upon their perceptions. We hypothesize that the user's perception of IoT device quality will impact his or her perceptions about the service provided by the system; thus, a user will be more likely to view service as trustworthy if it derives from an IoT device that is perceived to be of high quality.
Therefore, we hypothesize that the users' perception of IoT device quality will positively impact their trusting belief in IoT device(s).

Hypothesis 3(H3). A user's perception of an IoT device quality will positively influence trusting beliefs in an IoT device.

Perceived IoT device Effectiveness.

Pavlou and Gefen (2004) suggest that it is essential to evaluate the user's perception of institutional mechanisms' effectiveness. In the context of this study, we can describe effectiveness based on two aspects. First, as the degree to which the user perceives that the IoT device's mechanisms are capable of providing reliable, useful, and dependable service. Second, the degree to which a user believes that enforceable, cost-effective mechanisms are in place that provides recourse to the user in disputes or problems. Therefore, the users' perception of an IoT device's effectiveness will impact their perceptions about the device's service. Hence, we hypothesize that as users' perception of an IoT device's effectiveness increases, so will their trusting beliefs about that IoT device.

Hypothesis 4 (H4). A user's perception of an IoT device's effectiveness will positively influence trusting beliefs in an IoT device.

Perceived Trustworthiness of IoT device Host.

Extant research found that trust transference can occur intra-channel, when trust is transferred from an entity to another in the same channel (Ballester & Espallardo, 2008; Stewart, 2003, 2006). It can also happen inter-channel when trust is transferred from one context to another (Hahn & Kim, 2009; Kuan & Bock, 2007; Lin et al., 2011). For example, Lin et al. (2011) found that trust in online brokerage services directly affects initial trust in mobile brokerage services. Therefore, we infer that the trust a user has in a company's current web-based and mobile-based services will transfer to the IoT environment when they serve as IoT hosts. Pavlou and Gefen (2004) and McKnight and Chervany (2000) suggest that unknown parties often draw trust in the online context through their association with a trusted entity.

Therefore, we hypothesize that users will draw trust-related conclusions about an IoT device because they trust the IoT device host.

Hypothesis 5 (H5). A user's perception of an IoT device host's trustworthiness will positively influence trusting beliefs in an IoT device.

Trusting Beliefs in the IoT Device.

Kim and Benbasat (2006) have identified trusting belief as an important mediator leading to trusting intentions in studies of trust in e-transactions. McKnight and Chervany (2002) have broadly defined trusting beliefs as meaning that "one believes that the other party has one or more characteristics beneficial to oneself" (p. 46). In general, trusting beliefs can be defined as the trustor's perception that the trustee shows attributes such as those beneficial to the trustor. McKnight et al. (2002) have described trusting belief as competence, benevolence, and integrity in the context of e-commerce and a web vendor.

Competence addresses the consumer's perception of the vendor's ability to complete the transaction. Benevolence refers to the consumer's belief that the vendor cares about its customers and will act in their best interests. Integrity refers to the consumer's belief in the vendor's honesty in keeping commitments. These characteristics have been defined and applied in a very generic way across several studies of e-commerce (e.g., Kim and Benbasat, 2006; Lim et al., 2006; Stewart, 2006). Hence, we can extend and apply them towards trusting beliefs in IoT devices. We hypothesize that increased Trusting Beliefs in IoT devices' services will lead to increased Intention to Attain service (s) provided by the IoT device. We hypothesize that increased Trusting Beliefs in a Reputation System will lead to increased Intention to Use Feedback from the reputation system.

Hypothesis 6 (H6): *A user's trusting beliefs in an IoT device positively influences intention to attain service from an IoT device.*

Intention to Use Service from an IoT Device

Based on the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1980), we can conjecture that trusting beliefs lead to trusting intentions. McKnight et al. (1998) recognized trusting intentions concerning consumer trust in terms of behavioral intention. McKnight et al. (2002) have extended subjective measures of trusting intention specifically for the e-commerce domain. These measures are yet to be tested in the context of Intention to Attain service (s) provide by the IoT Devices. We extend the measures for this relatively newer extension of e-commerce-IoT. The proposed measures are as follows: provide the IoT device personal information, engage in an interaction, and act on IoT provided service or information. `

Control Variables
Disposition to Trust.

McKnight et al. (1998; 2002) suggest that *faith in humanity* (the general assumption that others are forthright and dependable) and *trusting stance* (the general assumption that if we treat others as if they are forthright and dependable, we will experience better outcomes) (Riker, 1971) are integral to Disposition to trust. The e-commerce literature identifies the Disposition to trust as particularly important in the online context (Gefen, 2000; McKnight et al. 2002; Salam et al., 2005). Some consumers have a greater Disposition to trust in general and are more likely to trust a Web vendor despite the impersonal Internet environment (Salam et al., 2005). In general, Disposition to trust refers to a person's propensity or tendency to believe in others' positive attributes. This personal trait is critical in any relationship's initial stages (Mayer et al., 1995; McKnight et al., 1998). However, it is based on personality, which explains why some tend to trust or not trust others (Mahad et al., 2015). Hence, our proposed research model considers Disposition to trust as a control variable.

Subjective Norm.

Ajzen and Fishbein (1973) describe subjective norm as "the actor's belief about the likelihood that members of a given reference group expect him to perform the behavior in question" (p. 43). The Subjective Norm construct has been utilized frequently in studies of information systems in general (Hartwick and Barki, 1994; Karahanna et al., 1999; Venkatesh et al., 2003) and in studies of online interactions in particular (Hansen, 2005; Song and Zahedi, 2005; Yoh et al., 2003). Furthermore, some studies have found Subjective Norm to be an essential predictor of intentions to use a system (Hu et al., 2003; Riemenschneider et al., 2003; Venkatesh and Morris, 2000). These findings indicate that users who have regular interactions with referent others who use reputation systems will be more receptive to the use of reputation systems themselves. Since IoT is a relatively newer phenomenon, the current study incorporates the Subjective Norm as defined by Ajzen and Fishbein (1973, 1980), as a control variable

Perceived Trustworthiness of the Internet.

IoT devices are mechanisms that exist within the Internet environment. Trust the user has in the Internet's structural and situational soundness (Keen et al., 1999; McKnight, 1998, 2002; Pavlou and Gefen, 2004) impact everything that uses the Internet. Hence, it is not exclusive or anything outstanding for the IoT. Therefore, we propose considering the Perceived Trustworthiness of the Internet as a control variable in our model.

CONCLUSION AND FUTURE WORK

Internet of Things (IoT) brings a new paradigm of `talking' sensors or objects with the help of the Internet. During this "talk," important data are shared, which makes a user uncomfortable. The model we proposed should help us understand the antecedents of Institution-based trust in IoT environment, which essentially leads to the adoption of an IoT device. In the future, we would like to test our proposed model and the hypotheses empirically. Through this, we believe, will address a critical void in the extant IoT literature.

REFERENCE

Accenture. (2015a). Digital trust in the IoT era. Retrieved August 15, 2019, from https://www.accenture.com/us-en/insight-digital-trust

Accenture. (2015b). The four keys to digital trust: Don't be left behind. Retrieved August 15, 2019, from https://www.accenture.com/us-en/ insight-accenture-four-keys-digital-trust

Agarwal, R., & Venkatesh, V. (2002). Assessing a Firm's Web Presence: A Heuristic Evaluation Procedure for the Measurement of Usability. Inf. Syst. Res., 13, 168-186.

Ajzen I, Fishbein M. (1973) Attitudinal and normative variables as predictors of specific behaviors. Journal of Personality and Social Psychology. 27:41–57

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Aldossari, M.Q., Sidorova, A. (2018). Consumer acceptance of Internet of Things (IoT): smart home context. Journal of Computer Information Systems 60 (6), 507-517

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787–2805.

Barney, J. B., & Hansen, M. H. (1994) Trustworthiness as a Source of Competitive Advantage. Strategic Management Journal (15), pp. 175-190

Beldad, A.; de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior, 26(5): 857-869

Cox, D., & Cox, A.D. (2002). Beyond first impressions: The effects of repeated exposure on consumer liking of visually complex and simple product designs. Journal of the Academy of Marketing Science, 30(2), 119–130.

Delgado-Ballester, E., & Hernández-Espallardo, M. (2008). Effect of Brand Associations on Consumer Reactions to Unknown On-Line Brands. International Journal of Electronic Commerce, 12(3), 81-113

Esmaeilpour Ghouchani, B., Jodaki, S., Joudaki, M., Balali, A., & Rajabion, L. (2020). A model for examining the role of the Internet of Things in the development of e-business. VINE: The Journal of Information & Knowledge Management Systems, 50(1), 20.

Giovannini, C., Ferreira, Jorge B., Silva, J., & Ferreira, D. (2015). The effects of trust transference, mobile attributes and enjoyment on mobile trust. BAR - Brazilian Administration Review, 12(1), 88-108. https://doi.org/10.1590/1807-7692bar2015140052

Hahn, K. H., & Kim, J. (2009). The effect of offline brand trust and perceived internet confidence on online shopping intention in the integrated multi-channel context. International Journal of Retail and Distribution Management, 37(2): 126-141

Hansen, T. (2005) Consumer adoption of online grocery buying: a discriminant analysis.International Journal of Retail & Distribution Management, Vol. 33 No. 2, pp. 101-121.

Hartwick, J., and Barki, H. (1994) Explaining the Role of User Participation in Information System Use. Management Science. 40(4), pp. 440-465

Karahanna, E., Straub, D. W., and Chervany, N. L. (1999) Information Technology Adoption across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. MIS Quarterly 23(2), 1999, pp. 183-213

Keen, P., Ballance,C., Chan, S. and Schrimp, S. (2000),ElectronicCommerce Relationships– Trust by Design, Prentice-Hall, Englewood Cliffs, NJ

Kim, D., & Benbasat, I. (2006). The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's model of argumentation. Information Systems Research, 17(3), 286-300

Kuan, H-H., & Bock, G-W. (2007). Trust transference in brick and click retailers: an investigation of the before-online-visit phase. Information and Management, 44(2): 175-187

Lee, M. (2019) An Empirical Study of Home IoT Services in South Korea: The Moderating Effect of the Usage Experience. International Journal of Human-Computer Interaction. 2019, Vol. 35 Issue 7

Lim, K., Sia, C. L., Lee, M. K. O., and Benbasat, I. (2006) How Do I Trust You Online, and If So, Will I Buy? An Empirical Study on Designing Web Contents to Develop Online Trust. Journal of Management Information Systems (23:2), pp. 233-266

Lin, J.; Lu, Y.; Wang, B., & Wei, K. K. (2011). The role of inter-channel trust transfer in establishing mobile commerce trust. Electronic Commerce Research and Applications, 10(6): 615-625

Mayer, R. C., Davis, J. H. & Schoorman, F. D. "An Integrative Model of Organizational Trust," Academy of Management Review (20), 1995, pp. 709-734

McKnight, D.H., Cummings, L.L., Chervany, N.L., 1998. Initial trust formation in new organizational relationships. Academy of Management Review 23 (3), 473–490.

McKnight, D. H; Choudhury, V; and Kacmar, C. (2000) Trust in E-Commerce Vendors: A Two-Stage Model. ICIS 2000 Proceedings. 54.

McKnight, D. H. & Chervany, N (2000) What is Trust? A Conceptual Analysis and an Interdisciplinary Model. AMCIS 2000 Proceedings. Paper 382

Menard, P., & Bott, G. (2018). Investigating Privacy Concerns of Internet of Things (IoT) Users. AMCIS

Pavlou, P. A., & Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. Information Systems Research, 15(1), 37–59

Pavlou, P. A. (2002) Institutional trust in interorganizational exchange relationships: The role of electronic B2B marketplaces. J. Strategic Inform. Systems 11(3–4) 215–243.

Pavlou, P. A. (2003) Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. Internat. Journal. Electronic Commerce 7(3) 69–103

Riemenschneider, D., Harrison, D. and Mykytyn, P. (2003) Understanding IT adoption decisions in small

business: integrating current theories. Information Management, Vol.40, pp.269–285.

Ratnasingam, P., & Pavlou, P (2002). Technology trust: The next value creator in B2B electronic commerce. International Resource Management Association Conference: Seattle, Washington, May 21-23.

Salam, A.F., Iyer, L., Palvia, P. and Singh, R. (2005). Trust in e-commerce, Communications of the ACM, 48(2), 73-77

Song J., & Zahedi F. (2005) A theoretical approach to web design in e-commerce: a belief

reinforcement model, Management Science, 51(8) 1219-1235.

Stewart, K. J. (2003). Trust transfer on the World Wide Web. *Organization Science, 14*(1), 5–17.

Stewart, K. J. (2006) How Hypertext Links Influence Consumer Perceptions to Build and Degrade Trust Online, Journal of Management Information Systems, 23(1)

Venkatesh, V., Morris, M., Davis, G.B., and Davis, F.D. (2003) User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27(3) pp. 425-78.

Venkatesh, V., & Morris, M. (2000). Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior. MIS Quarterly, 24(1), 115-139.

Zucker, L.G. (1986) The Production of Trust: Institutional Sources of Economic Structure, 1840-1920. Research in Organizational Behavior, 8, 53-111