2016

Rethinking Trust in E-Commerce in a Context-aware, Mobile World

Ayodele A. Barrett
University of Pretoria, ayodele.barrett@gmail.com

Machdel Matthee
University of Pretoria, machdel.matthee@up.ac.za

56. Rethinking Trust in E-Commerce in a Context-aware, Mobile World

Ayodele A. Barrett
University of Pretoria
ayodele.barrett@gmail.com

Machdel Matthee
University of Pretoria
machdel.matthee@up.ac.za

Abstract

Privacy invasion, surveillance and profiling are some identified vulnerabilities as a consequence of trusting context-aware technologies such as smart-phones. With PC-enabled e-commerce transactions, the technological ecosystem was smaller with a corresponding simpler chain of trust. Context-aware technologies such as smart-phones are increasingly being used in initiating and completing commercial transactions. It is argued that newer and richer understanding of the issue of trust informed by mobile commerce is important. Research is needed to understand the nature of trust in context-aware technologies. This might lead on the one hand to valuable insights into the effect of the awareness of risks on user behavior and on the other hand, to suggestions on what can or should be done from the retailer or provider's side to enhance the communication of risks and privacy issues to users.

Keywords

Trust, e-Commerce, m-Commerce, Context-Aware Technologies (CATs), Smart-phones, Retail apps

1. Introduction

Context-aware technologies (CATs), such as smart-phones, are increasingly being used in carrying out m-commerce transactions. Smart-phones frequently use apps and an abundance of sensors to achieve personalised solutions by garnering personal information of users and their environment. The amassed data, often done unobtrusively, sometimes is disclosed to untrusted parties (Treiblmaier & Chong, 2011; Christin *et al.*, 2011). Furthermore, in an effort to abstract the functionality of modern technologies, ostensibly to improve user experiences, the systems are becoming more and more opaque leading to a loss of control on the part of the user (Söllner & Leimeister, 2013). Additionally, users often lack the opportunity to know or interact with the creators of these artefacts via traditional means of interaction such as face-to-face contact (Kim *et al.*, 2009; Bevan, 2011). Thus, the conventional sense of community or shared values that foster trust between engaging parties is absent (Belanger & Carter, 2008).

Information systems (IS) research identifies trust's important role in helping users overcome perceptions of risk, uncertainty and vulnerabilities in the use and acceptance of technology (McKnight *et al.*, 2011). As modern society becomes more complex with the development, and use, of complex digital technologies, trust is seen as one means of navigating and reducing complex situations (Li *et al.*, 2008). The subject of trust continues to be an important issue and has a significant bearing on the continued use of technologies. Where trust specifically with the use of CATs and pervasive computing has been researched, the approach has primarily been

examined computationally (e.g. Marsh, 1994; Al-Karkhi et al, 2012), with trust being said often to be confused with security solutions (Stark, 2014).

There has been extensive research demonstrating the important role of trust in e-commerce. Given the prevalence of smart-phones and their burgeoning ecosystem (including an ever-increasing number of retail apps), a consideration of user-centered trust is required. It is argued that a newer and richer understanding of the issue of trust informed by mobile commerce is important. This article reviews extant studies of trust in e-commerce literature and seeks to find out their relevance in m-commerce, specifically via the use of retail apps. To do so, the discussions in the article begin with an introduction to trust and existing research on trust and technology. Following this are reflections on e-commerce, Context-Aware Technologies (CATs) & smart-phones, and apps. Prior to the conclusion are considerations on what possible bearing CATs may have on trust as well as and illustration of the increased risk associated with m-commerce.

2. Trust and Technology

With the accepted importance of trust comes a number of problems. Primarily, there is concern in literature regarding the lack of a common definition of trust (Seigneur & Jensen, 2004; Taddeo, 2009). The multiplicity of definitions has been attributed by some, to the fact that trust has been studied from different fields (Dasgupta, 2000; Das & Teng, 2004), such that there is a proliferation of narrow intra-disciplinary definitions of trust (McKnight & Chervany, 2001). One such definition used in this paper, and according to Janson et al., (2013) by a vast majority of IS researchers, is by Mayer *et al.*, (1995, p. 712) ..."the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party".

Notwithstanding the lack of a common definition, there is general consensus on the necessary conditions without which trust would not be required. The first of these is that there needs to be an element of reliance on one party by another. Prior to deciding to trust, a trustor (the reliant party) has a need of some type that cannot be met without the assistance of a providing party, or trustee. Secondly, there is an element of risk or the possibility that expectations of the reliant party may not be met. Trust would not be required if actions could be taken with absolute certainty. Lastly, there is the view that trust is a reductionist strategy to dealing with complexities (Li *et al.*, 2008; Gulati & Sytch, 2008). Vulnerabilities which could arise from the use of modern IS include privacy violations and unauthorised use of private data gathered from consumers of IS products.

IS-based research on trust has drawn heavily from traditional disciplines (e.g. psychology, sociology and economics). Areas of research in trust and IS-use include e-health (Bansal *et al.*, 2010), e-governance (Abu-Shanab 2014), online information (Lucassen, 2013), ubiquitous/pervasive computing (Bevan, 2011) and mobile applications (Janson et al., 2013). There have been debates on if it can be said that human beings can trust an inanimate entity (e.g. a smart-phone. Chopra & Wallace (2003) believe that trust is a construct applicable to humans. Söllner *et al.*, (2012) found, however, that it is possible for technological artefacts to be viewed directly as a trustee, rather than merely as a communications medium between humans or an

enabler in helping users accomplish their tasks. This view is relevant for autonomous systems that do not require direct human intervention in completing their tasks (Janson *et al.*, 2013).

In measuring technological trust, some researchers utilise human-oriented attributes. Examples are benevolence (a belief that a trustee would act in the best interest of the trustor), integrity (a belief that a trustee possesses moral soundness and adheres to principles acceptable to the trustor) and competence (a belief that a trustee possesses suitable skills to accomplish that which the trustor requires) (Vance *et al.*, 2008). McKnight *et al.* (2011) submit that technological artefacts lack volition, the capacity to act and choose independently, thus the use of human-oriented attributes are inappropriate. As alternatives, the authors proffer, technologically-oriented attributes *viz*., helpfulness (a belief that the artefact provides adequate help for it users), reliability (a belief that the artefact will work properly) and functionality (a belief that the technology has the appropriate features required to accomplish tasks). Lankton *et al.*, (2015) believe, however, that both sets of attributes could be appropriate as technologies differ in perceived humanness. As such, people will develop trust in each technology in different ways.

3. Trust & e-Commerce

Electronic commerce is the buying and selling of goods and services leveraging the power of the Internet. Typically e-commerce is assumed to be accessed via fixed infrastructure (e.g. the use of a browser on a PC accessing the Internet via phone lines or Local Area Networks (LANs)). There are various types of e-commerce of which perhaps the most common is business-to-consumer or B2C (trade conducted between corporations and individuals). Other categories include business-to-business or B2B (business conducted between corporations) and consumer-to-consumer or C2C (transactions conducted directly between individuals).

In contrast to traditional commerce, e-commerce is said to be more impersonal due to its facelessness, fewer sensory cues, less instant gratification and information asymmetry. Furthermore, the distance between the seller and the purchaser magnifies risks and uncertainties. More importantly, perhaps, is the increased possibilities for unprincipled behaviours by trustees (Head & Hassanein, 2012; Bansal & Zahedi, 2014). Thus the role of trust is elevated in e-commerce, due to the fact that there is a higher degree of uncertainty present in online transactions (Pavlou, 2003).

Users are required to provide personal and financial information for the successful completion of a transaction, which could be subject to abuse (Du *et al.*, 2010). Although the disclosure of information by users on the internet is primarily voluntary, they are often unaware of the fact that additional information could be garnered, who is able to access their data and how their data can potentially be used (Zheleva & Getoor, 2011). Two most common approaches to ensuring the privacy of online users is either via legislation (protected by law), or by using technological means (Seigneur & Jensen, 2004).

A lack of trust has also been cited as a main reason for some online users not participating in e-commerce in greater numbers or not completing a transaction (Awad & Ragowsky, 2008). When users trust e-vendors, however, they are more likely to share information, which in turn can be used by the vendor to offer tailored services (Reichheld & Schefter, 2000). Research has raised the point that with a cheap enough price, customers would engage in e-commerce even if

they do not entirely trust the vendors, a view not shared by (Reichheld & Schefter, 2000, p. 107) who argue that "price does not rule the web, trust does".

Trust in e-commerce research has been undertaken from various perspectives including differences across cultures and nationalities (e.g. Cyr, 2008), gender differences (e.g. Slyke, et al., 2010) and religion (e.g. Muhammad, et al. 2013). Additionally, studies have shown that technological factors enhance user trust in e-commerce. These include usability of the website usability, quality and information quality (Kim *et al.*, 2009; Patton & Jøsang, 2004), perceived trustworthiness of product vendor (Thaw *et al.*, 2009), use of 3rd party seals (Head & Hassanein, 2002), electronic word-of-mouth (eWOM)/recommendations (Awad & Ragowsky, 2008).

4. Trust & m-Commerce

The increased suffusion of smart-phones has seen users increasingly accessing the internet via their phones. The move to conducting e-commerce via mobile phones and wireless communications, has given rise to the term m-commerce (or mobile commerce). M-commerce, described as a subset of e-commerce, refers to financial transactions initiated, authorised and confirmed by means of a mobile telecommunications device such as a smart-phone (Cao *et al*., 2015, Jahanshahi *et al.*, 2010). Retailers provide multiple, retail mobile channels ranging from Unstructured Supplementary Service Data (USSD), Short Message Service (SMS), e-commerce sites (optimised for smaller screens), mobile apps or a combination thereof.

With PC-enabled e-commerce transactions, the technological ecosystem was smaller with a corresponding simpler chain of trust. Context-aware technologies, however, have a larger ecosystem that is inherently less secure.

Statistics vary but globally, almost 40% of all electronic retail is completed via mobile devices. Increasing too is the use of retail apps, as opposed to accessing an e-commerce site via a mobile device. South Korea records a staggering 99% of e-commerce sales from smart-phones (Criteo, 2015). Although prior research suggest a lack of mobile devices (Juniper, 2012). In emerging economies, the uptake is less. A lack of trust being cited for the low numbers (Joubert & van Belle, 2013; Rind *et al*., 2015). Prior to highlighting features of apps that may have a bearing on trust, a brief definition of the underlying technologies is presented in the next section.

4.1 Context-Aware Technologies (CATs) & Smart-Phones

Context-Aware Technologies (CATs) are equipped with the ability dynamically to detect and analyse data related to the consumer, the device itself and from the environment in which both the consumer and the device are situated (Dey & Abowd, 1999). Academic research and commercial interest in CATs is driven by the desire to transfer the onus of initiating interaction, between a consumer and a technological device, to the device. This move to creating greater device autonomy has been described as untethering the consumer from devices. The list of contextual data capable of being gathered is ever increasing, with the broadening attributed to the increase in the number of sensors being included in the devices. Based on gathered and analysed data, a CAT-enabled device can thus adapt its functionality and provide useful information, behaviour or services relevant to the task at hand (Schilit et al., 1994; Gediminas & Tuzhilin, 2011).

Context-awareness is perceived as both a building block and an enabler for the development of new paradigms that assist in the fulfilment of a future of pervasive computing. Pervasive computing is a vision identified by researchers in which technologies are transparent to users, interwoven into people's daily lives and distributed across the environment to such an extent that the usage of technologies fade into a user's subconsciousness (Weiser, 2002). Many forms of CATs are now commonplace, particularly *smart-phones*, with others such as *wearable computing* (body-borne computers) and the *Internet of Things* (IoT) gaining in popularity. Smart-phones have been described as communications Swiss Army knives, capable of doing a little bit of everything (Livingston, 2004). They consist of hardware (with sensors), processing capabilities, network connectivity and software (preinstalled or 3rd-party).

Previous research and surveys (e.g. Juniper, 2012) show that CATs users do not trust these technologies. Yet smart-phones, with their increasingly sophisticated data gathering capabilities, are quickly becoming the preferred communications and technological device. Trends show a decrease in PC sales and an increase in smart-phone sales. Predictions are that desktops are being done away with, and most people will rely solely on their smart-phones as their primary computing devices (Bonnington, 2015). For many in developing countries, particularly in Africa, a smart-phone is often a first computer and only Internet-connected device used (Pew Research, 2014).

4.2 Retail Apps

Initially retail apps merely duplicated an e-commerce site but offered less functionality. As technology evolves there has been an increase in the functionality and usability of retail apps. There has a move, by some retailers, to discontinue with their websites and transition completely to retail mobile apps (Velayanikal, 2015). Proponents of retail apps reason that as apps can access native phone functionality, this results in increased speed leading to better user experience. Also, payments could be better streamlined as retail apps could interact with other payment or financial apps. Furthermore, by being able to track their customers, retailers can better understand their behaviours and offer personalised solutions, such as a voucher sent when a user is close in vicinity to a retail store (Saurav, 2015). It is, perhaps, this ability of tracking customers that highlights the importance of conducting further research.

As there are increased risks with the use of smart-mobile technologies, the issue of consumer trust becomes more critical. Using retail apps provide greater insight into the daily activities of users. This in addition to the fact that a typical smart-phone holds a lot of personal and financial data, leading to possibly greater potential for fraud and abuse. There is a disparity between perception of security and the reality. In a survey, 86% of users believed that their apps were secure. The reality, however, is that 90% of Android apps and 35% of iOS apps had been compromised (Arxan, 2016).

Prior to installing apps on phones, users may be required to accept End-User License Agreements (EULAs) and permission lists. EULAs are contracts between software developers and users. It has been shown that users do not read EULA statements and accept them in less time than is possible to read the entire notice. Thus preventing the very notion of informed consent that the dialogs are meant to promote (Böhme & Köpsell, 2010).

Research has shown too that permissions lists fare little better in informing users. Permissions lists are used to alert smart-phone users of privacy and security invasive applications. Often shown only during installation, all the resources that will be used by the app are listed. While official app stores require all apps to display the permissions list prior to installation, apps from unofficial stores are not compelled to do so. Still, users pay scant attention to permissions or if they do, fail to comprehend their consequences (Felt *et al.*, 2012). Analysis of apps show too that many apps access more permissions than are needed to accomplish their tasks. The most common permissions include accessing a user's location (both approximate and precise), camera, microphone, and the user's contact details (Lin et al., 2014).

Table 1 contains a synopsis of mechanisms and solutions proffered as trust-enhancements in e-commerce which should be reconsidered with the use of smart-phones.

	E-commerce recommendations	**Limitations of smart-phones**
Security Solutions	A common approach to ensuring the privacy of online users is protection using technological means (Seigneur & Jensen, 2004).	Security Solutions (if available) are resource-intensive. Smart-phones are yet to possess the processing power and battery resources to efficiently execute such programs (Pawar *et al.*, 2014)
Security Awareness	The use of 3rd-party visual clues (such as security seals and icons) to increase perceptions on trustworthiness (Head & Hassanein, 2002)	The screen size is a limiting factor in displaying seals as a means of demonstrating trustworthiness (Li & Yeh, 2010)
Legislation	Protection by law to ensure privacy and increase trust (Seigneur & Jensen, 2004).	Laws may not protect users based on infringements arising from passively-sensed data; Laws are not adapting as quickly as the technologies (Ackerman *et al.*, 2001; Vasileiadis, 2014)
Policies	Privacy policies to improve consumer trust (Wu *et al.*, 2012)	Users pay little attention to permissions list or fail to grasp their consequences (Felt *et al.*, 2012)
Connectivity	Guarantee the integrity of communication channels (Tsiakis & Sthephanides, 2005)	Most smart-phone users prefer wireless Wi-Fi networks which are more susceptible to interception (Park *et al.*, 2014)
Anonymity	Use of privacy-enhancing software, prior to online purchase, that anonymises PII (Patton & Jøsang, 2004)	Diverse and powerful sensors, phone portability and ubiquity provide unprecedented opportunities for mining and identification of personal traits (Weiss & Lockhart, 2011)

Table 1: Comparison of trust-enhancing mechanisms for e-commerce and limitations for m-commerce

5. Discussion

Lankton *et al.*, (2015) provide evidence that trust occurs differently for differing IT artefacts. Technologies may vary in humanness (the ability to mimic human traits and afford a two-way interaction) and in turn, users develop trust in a different manner based on the perceived humanness of the technologies. Whereas online, e-commerce websites have been described as cold, impersonal and lacking in humanness, smart-phones in contrast are seen as extensions to one's self, with some describing being without their phone as being naked (Kwom *et al.*, 2013). This altered relation to technology as well as the increased vulnerabilities discussed in Section 4.2 point towards a need to reconsider research on trust related to CATs and all the functionalities (e.g. m-commerce) they provide.

CATs, specifically smart-phones, undoubtedly present many situational and immediate benefits to their users, and as a consequence, improving their user experiences. There is, however, a sense of inevitability associated with the CATs. Inevitability regarding their use in society and, particularly, inevitability with accepting vulnerabilities and unintended consequences associated with their use. As an example in 1999 the then CEO of Sun Microsystems, Scott McNealy, was quoted as declaring infamously that consumers of technology "have zero privacy. Get over it" (Sprenger, 1999). Other key figures in the technology arena have shared similar sentiments over the years.

Some have attributed the trusting stance, acceptance of the status quo, and sense of inevitability by consumers to being unaware of the real value of their information and having no understanding of how widespread the seeming indiscriminate collection, use and storage of their data. Others still have attributed the acceptance to consumers being tricked, by utterances and communication from the technology providers, that privacy, as an example, does not matter (Aimeur *et al*., 2016; Eastin *et al*., 2016). This despite the fact that it has been argued that practices such as widespread personal data collection and storage are not unanticipated, but rather engineered deliberately into the technologies (Warnier *et al*., 2015).

Future research should explore the potential moderating role that awareness plays in this model. Accordingly, one such area being investigated by the authors is the influence of communicative practices as antecedents of trust. Communication plays a crucial role in the decisions made in our social lives, including decisions on whether or not to trust. Despite perceived risks and vulnerabilities associated with smart-phones, they continue to be the ICT device of choice (with double-digit growth sales, particularly in Africa). Questions that need to be asked include: are there any misrepresentations of the capabilities of CATs? How do discussions around the use of CATs succeed in supporting the manifestation of trust? Can trust be established through communicative acts? These questions will be answered in upcoming research.

6. Conclusions

Consumer trust is considered to be important in influencing the use of technologies, as trust aids in situations of uncertainty and in which consumers have not control of. While CATs are ever increasing in their suffusion in society, there are still perceptions of risks associated with conducting m-commerce on these devices. Many studies have addressed the issue of trust in e-commerce. The article strives to highlight differences between e-commerce, in which access

was traditionally from fixed location, and m-commerce in which access is from wireless channels and its attendant risks. There is a belief in some quarters that retail apps could gain greater prominence than websites as they offer greater versatility. Apps present better opportunities for personalised communication between the retailer and the customer. While there are attendant risks associated with the use of e-commerce sites, these are amplified by using smart-phones. This article creates an awareness of the necessity of research on trust and CAT. Further research, particularly complemented with empirical findings from typical users of retail apps will be required.

References

Abu-Shanab, E. (2014). Antecedents of Trust in e-Government Services: An Empirical Test in Jordan. Transforming Government: People, Process and Policy, 8(4), pp 480-499.

Ackerman, M., Darrell, T. & Weitzner, D. J. (2001). Privacy in Context. Human-Computer Interaction, 16(2), pp 167-176.

Aïmeur, E., Lawani, O. & Dalkir, K. (2016). When Changing the Look of Privacy Policies Affects User Trust: An Experimental Study. Computers in Human Behavior, 58, pp 368-379.

Al-Karkhi, A., Al-Yasiri, A. & Linge, N. (2012). Privacy, Trust and Identity in Pervasive Computing: A Review of Technical Challenges and Future Research Direction. International Journal of Distributed and Parallel Systems (IJDPS), 3(3), pp 197-218.

Arxan. (2016). State of Application Security. https://www.arxan.com/resources/state-of-application-security/ Date accessed: January 2016.

Awad, N. F. & Ragowsky, A. (2008). Establishing Trust in Electronic Commerce through Online Word of Mouth: An Examination across Genders. Journal of Management Information Systems, 24(4), pp 101-121.

Bansal, G., Zahedi, F. & Gefen, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. Decision Support Systems, 49(1), pp 138-150.

Bevan, C. R. (2011). Human to Computer Trust in Urban Pervasive Computing. PhD thesis, University of Bath, England.

Böhme, R. & Köpsell, S. (2010). Trained to Accept? A Field Experiment on Consent Dialogs, In Proceedings of CHI 2010, Atlanta, Georgia, pp 2403-2406.

Bonnington, C. (2015). In Less than Two Years, A Smartphone could be Your Only Computer. http://www.wired.com/2015/02/smartphone-only-computer/ Date accessed: December 2015.

Brengman, M. & Karimov, F. P. (2012). The Effect of Web Communities on Consumers' Initial Trust in B2C e-Commerce Websites. Management Research Review, 35(9), pp 791-817.

Cao, Y., Lu, Y., Gupta, S. & Yang, S. (2015). The Effects of Differences between e-Commerce and m-Commerce on the Consumers' Usage Transfer from Online to Mobile Channel. International Journal of Mobile Communications, 13(1), pp 51-70.

Chopra, K. & Wallace, W. A. (2003). Trust in Electronic Environments. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, pp 10-19.

Christin, D., Reinhardtb, A., Kanherec, S.S. & Hollicka, M. (2011). A Survey on Privacy in Mobile Participatory Sensing Applications. Journal of Systems and Software, 84(11), pp

1928-
1946.
Criteo. 2015. State of Mobile Commerce – Growing like a Weed. http://www.criteo.com/media/1894/criteo-state-of-mobile-commerce-q1-2015-ppt.pdf Date accessed: January 2016.
Cyr, D. (2008). Modeling Web Site Design Across cultures: Relationships to Trust, Satisfaction, and E-Loyalty. Journal of Management Information Systems, 24(4), pp 47-72.
Das, T. K. & Teng, B. (2004). The Risk-Based View of Trust: A Conceptual Framework. Journal of Business and Psychology, 19(1), pp 85-116.
Dasgupta, P. (2000). Trust as a Commodity. In Trust: Making and Breaking Cooperative Relations, pp 49-72. University of Oxford.
Dey, A. K. & Abowd, G. D. (1999). Towards a Better Understanding of Context and Context-Awareness. In HUC 99: Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, pages 304-307.
Eastin, M. S., Brinson, N. H., Doorey, A. & Wilcox, G. (2016). Living in a Big Data World: Predicting Mobile Commerce Activity through Privacy Concerns. Computers in Human Behavior, 58, pp 214-220.
Gediminas, A. & Tuzhilin, A. (2011). Context-Aware Recommender Systems. Recommender Systems Handbook, 1(1), pp 217-253.
Gulati, R. & Sytch, M. (2008) Does Familiarity Breed Trust? Revisiting the Antecedents of Trust. Managerial and Decision Economics, 29:165-190.
Einav, L., Levin, J., Popov, I. & Sundaresan, N. (2014). Growth, Adoption, and Use of Mobile E-Commerce. American Economic Review: Papers & Proceedings, 104(5), pp 489-494.
Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. & Wagner, D. (2012). Android Permissions: User Attention, Comprehension and Behavior. In Symposium on Usable Privacy and Security
(SOUPS), Washington DC, USA.
Firdhous, M., Ghazali, O. & Hassan, S. (2012). Trust Management in Cloud Computing: A Critical Review. International Journal on Advances in ICT for Emerging Regions, 4(2), 24-36.
Head, M. M. & Hassanein, K. (2002). Trust in e-Commerce: Evaluating the Impact of Third-Party Seals. Quarterly Journal of Electronic Commerce, 3(1), pp 307-325.
Janson, A., Hoffmann, A., Hoffman, H., & Leimeister, J. M. (2013). How Customers Trust Mobile Marketing Applications. In Proceedings of the 34th International Conference on Information Systems, Milan.
Joubert, J. & van Belle, J. (2013). The Role of Trust and Risk in Mobile Commerce Adoption within South Africa. International Journal of Business, Humanities and Technology, 3(2), pp
27-38.
Juniper Network. (2012). Global Trusted Mobility Index. http://www.juniper.net/us/en/local/pdf/additional-resources/7100155-en.pdf Data accessed: November 2015.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2009). Trust and Satisfaction, Two Stepping Stones for Successful E-Commerce Relationships: A Longitudinal Exploration. Information Systems Research, 20(2), pp 237-257.

Kwon, M., Lee, J., Won, W., Park, J., Min, J., Hahn, C., Gu, X., Choi, J. & Kim, D. (2013). Development and Validation of a Smartphone Addiction Scale (SAS). PLOS ONE, 8(2)

Lankton, N. K., McKnight, D. H. & Tripp, J. (2015). Technology, Humanness, and Trust: Rethinking trust in Technology. Journal of the Association for Information Systems, 1610, pp 880-918.

Li, X., Hess, T. J. & Valacich, J. S. (2008). Why do We Trust New Technology? A Study of Initial Trust Formation with Organizational Information Systems. Journal of Strategic Information Systems, 17(1) pp 39-71.

Li, Y. & Yeh, Y. (2010). Increasing Trust in Mobile Commerce through Design Aesthetics. Computers in Human Behavior, 26(4), pp 673-684.

Lin, J., Liu, B., Sadeh, N. & Hong, J. I. (2014). Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permissions Settings. In 10th Symposium on Usable Privacy and Security (SOUPS), California, pp 199-212.

Livingston, A. (2004). Smartphones and Other Mobile Devices: The Swiss Army Knives of the 21st Century. Educause Quarterly, 27(2), pp 46-52.

Lucassen, T. (2013). Trust in Online Information. PhD thesis, Centre for Telematics and Information Technology, University of Twente, The Netherlands.

Magrath, V. & McCormick, H. (2012). Marketing Design Elements of Mobile Fashion Retail Apps. Journal of Fashion Marketing and Management: An International Journal, 17(1), pp 115-134.

Marsh, S. P. (1994). Formalising Trust as a Computational Concept. PhD thesis, University of Stirling, Scotland.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. Academy of Management Review, 20(3), pp 709-734, 1995.

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, 2(2), pp 1-25.

McKnight, D. H. & Chervany, N. L. (2001). Trust and Distrust Definitions: One Bite at a Time. In R. Falcone, M. Singh, and Y. Tan, editors, Trust in Cyber-Societies, volume 2246 of Lecture Notes in Computer Science, Springer Berlin, pp 27-54.

Muhammad, M., Muhammad, M. R., Suhaimi, M. A., Razi, M. J. M. & Abdullah, K. (2013). Building Trust in e-commerce from an Islamic Perspective: A Literature Review. American Academic & Scholarly Research Journal, 5(5), pp 161-168.

Patton, M. A. & Jøsang, A. (2004). Technologies for Trust in Electronic Commerce. Electronic Commerce Research, 4, pp 9–21.

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7(3), pp 69-103.

Pawar, K., Jagtap, V., Bedekar, M. & Mukhopadhyay, D. (2014). AFMEACI: A Framework for Mobile Execution Augmentation Using Cloud Infrastructure. Advanced Computing, Networking and Informatics, 2, pp 441-450.

Pew Research Center. (2014). Emerging Nations Embrace Internet, Mobile Technology. http://www.pewglobal.org/2014/02/13/emerging-nations-embrace-internet-mobile-

technology/
Date accessed: December 2015.
Reichheld, F. F. & Schefter, P. (2000). E-Loyalty: Your Secret Weapon on the Web. Havard Business Review", 78(4), pp 105-113.
Rind, M. M., Koondhar, M. Y., Chandio, F. & Shah, A. (2015). A Conceptual Framework for the Analysis of Determinants of M-Commerce Acceptance. In Proceedings of the 13th International Conference on Statistical Sciences, Pakistan, pp 433-446.
Saurav, K. (2015). E-Commerce Apps vs Mobile Sites: Which is Better? http://retail.economictimes.indiatimes.com/news/industry/e-commerce-apps-vs-mobile-sites-which-is-better/49797144 Date accessed: January 2016.
Seigneur, J. & Jensen, C. D. (2004). Trading Privacy for Trust. In Proceedings of the 2nd International Conference on Trust Management, pp 93-107.
Shankar, N. & Arbaugh, W. (2002). On Trust for Ubiquitous Computing. In Proceedings of the Workshop on Security in Ubiquitous Computing, UBICOMP, pp 44-54.
Sharif, M. S., Shao, B., Xiao, F. & Saif, M. K. (2014). The Impact of Psychological Factors on Consumers Trust in Adoption of M-Commerce. International Business Research, 7(5), pp 148-155.
Slyke, C. V., Bélanger, F., Johnson, R. D. & Hightower, R. (2010). Gender-Based Differences in Consumer E-Commerce Adoption. Communications of the Association for Information Systems, 26(2), pp
Söllner, M., Hoffmann, A., Hoffman, H., Wacker, A. & Leimeister, J. M. (2012). Understanding the Formation of Trust in IT Artifacts. In Proceedings of the 33rd International Conference on
Information Systems, Orlando.
Sprenger, P. (1999). Sun on Privacy: 'Get Over It'. http://archive.wired.com/politics/law/news/1999/01/17538 Date accessed: February 2016
Stark, J. E. (2012). Trust in Distributed Computing. MSc thesis, University of Guelph, Canada.
Taddeo, M. (2009). Defining Trust and E-Trust: From Old Theories to New Problems. International Journal of Technology and Human Interaction, 5(2), pp 23-35.
Taylor, P. (2015). Edward Snowden Interview: 'Smartphones can be taken over'. http://www.bbc.com/news/uk-34444233 Date accessed: December 2015.
Thaw, Y. Y., Mahmood, A. K. & Dominic, P. D. D. (2009). A Study on the Factors that Influence the Consumers' Trust on E-commerce Adoption. International Journal of Computer
Science and Information Security (IJCSIS), 4(1), pp 153-159.
Thorsteinsson, G. & Page, T. (2014). User Attachment to Smartphones and Design Guidelines. International Journal of Mobile Learning and Organisation, 8(3-4), pp 201-215.
Treiblmaier, H. & Chong, S. (2011). Trust and Perceived Risk of Personal Information as Antecedents of Online Information Disclosure: Results from Three Countries. Journal of Global Information Management, 19(4), pp 76-94.
Vance, A., Elie-Dit-Cosaque, C. & Straub, D. W. (2008). Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture. Journal of Management Information Systems, 24(4), pp 73–100.
Vasileiadis, A. (2014). Security Concerns and Trust in the Adoption of M-Commerce. Social Technologies, 4(1), pp 179-191.

Velayanikal, M. (2015). Flipkart Moves Close to Going App-only. http://www.business-standard.com/article/companies/flipkart-moves-closer-to-going-app-only-115092200292_1.html Date accessed: January 2016.

Warnier, M., Dechesne, F. & Brazier, F. (2015). Design for the Value of Privacy InJ. Van den Hoven, P. E. Vermaas, and I. van de Poel (eds.), Handbook of Ethics, Values, and Technological Design, pp 431-445. Springer.

Weiser, M. (2002). The Computer for the 21st Century. IEEE Pervasive Computing, 1(1), pp 19-25.

Weiss, G. M. & Lockhart, J. W. (2011). Identifying User Traits by Mining Smart Phone Accelerometer Data. Proceedings of the Fifth International Workshop on Knowledge Discovery from Sensor Data (KDD '11).

Wingreen, S. C. & Baglione, S. L. (2005). Untangling the Antecedents and Covariates of E-Commerce Trust: Institutional Trust vs. Knowledge-Based Trust. Electronic Markets, 15(3), pp 246-260.

Zheleva, E. & Getoor, L. (2011). Privacy in Social Networks: A Survey. Social Network Data Analytics, vol. 1, Database Management \& Information Retrieval, Springer US, pp 277-306.