Individual Trust and the Internet

Lisa van der Werff[*]

DCU Business School, Dublin City University, Ireland

lisa.vanderwerff@dcu.ie

Colette Real

DCU Business School, Dublin City University, Ireland

colette.real@dcu.ie

Theodore G. Lynn

Irish Centre for Cloud Computing and Commerce, DCU Business School, Dublin City University, Ireland

theo.lynn@dcu.ie

*Corresponding Author

Please cite this work as:

van der Werff, L., Real, C., & Lynn, T. (2018). Individual trust and the internet. In R. Searle, A. Nienaber, & S. Sitkin (eds.), *Trust*. Oxford, UK: Routledge.

INTRODUCTION

The emergence of Web 2.0 technologies and associated services heralded a second generation of the Internet emphasising collaboration and sharing amongst users. This resulted in a seismic shift in the relationship between individual consumers and firms but also between individual consumers and the Internet as a system. Consumers, not firms, became an emerging locus of value production and through the ability to publish and connect with known and unknown others, an emerging locus of power (Berthon, Pitt, Plangger, & Shapiro, 2012). Powered by broadband telecommunications and device connectivity, the intensity of these changes was further deepened by being freed from the desktop to the mobile web. We are more connected now than ever before. The high levels of societal interconnectedness encouraged by the internet have made trust an even more vital ingredient in today's society (Hardin, 2006). The more recent development of Web 3.0 technology emphasises ubiquitous connectivity and a machine-facilitated understanding of information that may once more change the locus of activity, value production and control. In order to keep pace with the issues of contemporary society, trust researchers must consider the how trust relationships and perceptions operate and are influenced by the online environment.

This chapter will discuss how traditional trust concepts translate to the online context and will examine empirical literature on online trust at three different levels. Interpersonal trust between individuals using the internet as a medium for communication is particularly relevant in a world where personal and professional relationships are increasingly mediated by technology. We will also discuss the role of the internet in relationships between individuals and organisations with particular attention to the provision of e-services. Finally, we discuss trust in the system of the internet itself as a distributed connected infrastructure made up of indirect system service providers which are often nameless or in the background.

Our focus in the chapter is on individual trust in other individuals, organisations and the system of the internet itself. Trust from the perspective of the organisation may also be of interest to trust scholars. This includes issues relating to organisational trust in individuals, inter-organisational trust, and organisational trust in the system of the Internet itself however these topics are outside of the scope of this chapter (see Perks & Halliday, 2003; Ratnasingam, 2005).

TRADITIONAL TRUST THEORY IN AN INTERNET CONTEXT

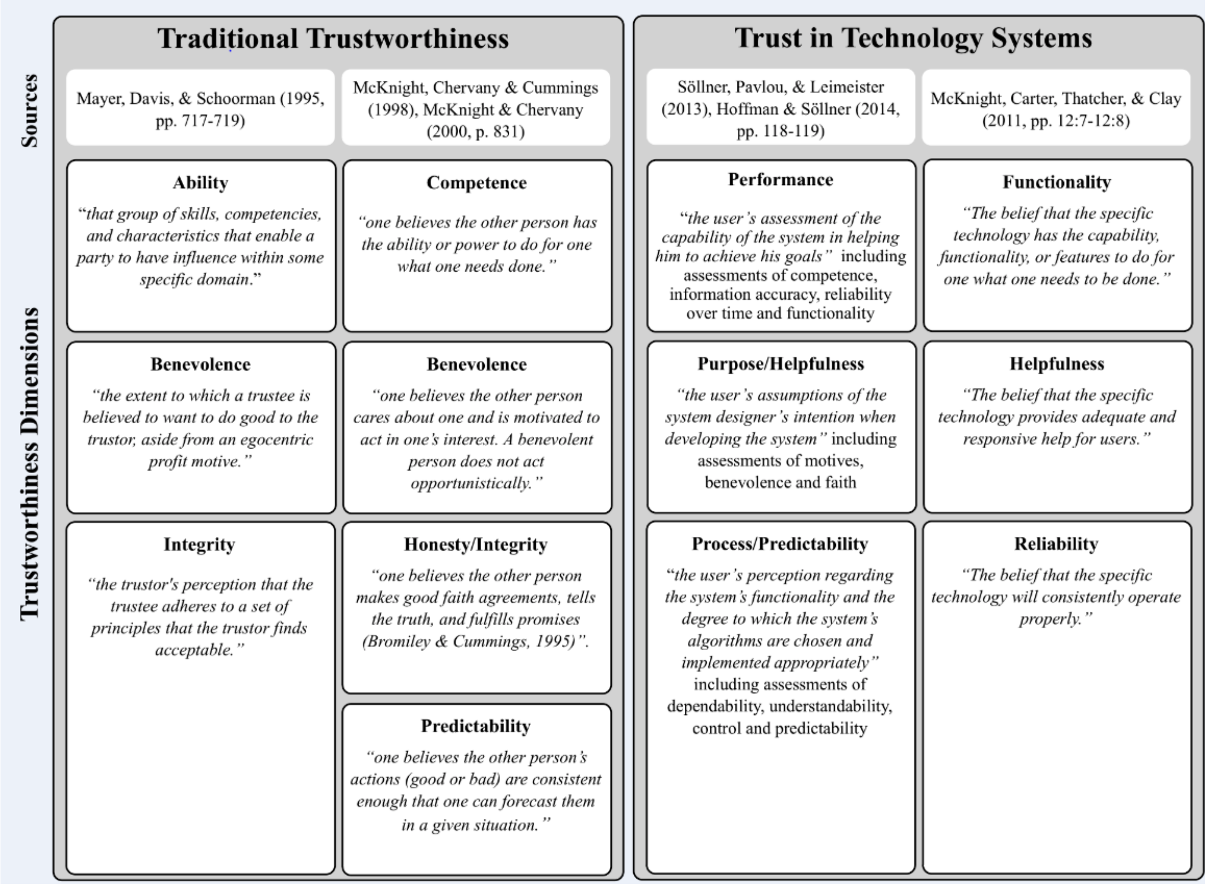
As can be seen from previous chapters, the topic of trust has attracted scholarly attention across a range of disciplines. This research attention has led to an overabundance of possible definitions for the construct. However, irrespective of the discipline, two key components are common to the majority of trust definitions: a willingness to be vulnerable and a perception of the intentions of the other party (Lewicki & Brinsfield, 2012). Reflecting these commonalities, Rousseau and colleagues (1998) propose a cross disciplinary definition of trust as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" (Rousseau, Sitkin, Burt, & Camerer, 1998, p.395). This is the perspective from which we will approach the discussion of trust in the internet context.

The positive expectations identified in Rousseau's definition are thought to be based predominantly on perceptions of the other party's ability, benevolence and integrity collectively known as trustworthiness (Mayer, Davis, & Schoorman, 1995). A smaller body of literature points to either predictability (Dietz & Den Hartog, 2006; McKnight, Cummings, & Chervany, 1998) or value congruence as possible fourth sub dimensions of trustworthiness perceptions. However, the Mayer et al trustworthiness concept incorporates a moral conceptualisation of integrity that includes a value congruence between trustor and trustee as a necessary component (Tomlinson, Lewicki, & Ash, 2014). Evidence regarding these trustworthiness dimensions is collected to allow an individual to make a trust decision on the basis of which that individual may engage in trust behaviour (McEvily, Perrone, & Zaheer, 2003). The context of the internet has a number of important implications for these commonly accepted characteristics of the trust process. First, many decisions to trust online are likely to involve trust in a number of known and unknown referents. For instance, a decision to buy groceries online may be influenced by trust in the retailer (organisational trust), trust in the individuals who will select or deliver your groceries (interpersonal trust), trust in the online payment system and trust in the internet itself (system level trust).

Second, whether each of the trustworthiness dimensions is applicable to all possible referents in an online environment is the subject of debate. At an individual and organisational level, it could be expected that the components of trustworthiness perceptions would translate relatively neatly to the internet context, although the evidence on which these perceptions are based may be quite different (see McKnight & Chervany, 2001 for discussion). In essence, the internet in many situations acts a medium through which individuals and organisations can communicate and many of the same trust cues can be perceived. However, with regards to system level trust, such as trust in web based software applications or in the internet itself, the applicability of ability, benevolence, integrity and predictability is not unequivocal. Consider for example judging the trustworthiness of an IT application. It may be possible to make a competence or ability judgement or an evaluation of predictability but is it possible to make a benevolence or integrity judgement about another party that does not have agency? Some scholars have argued that these traditional trust concepts are not suitable for discussing trust in IT systems (Friedman, Khan, & Howe, 2000).

However, a number of scholars have endeavoured to apply traditional trust theory to the context of automated systems. Notable among these is the work of Harrison McKnight and colleagues along with that of Matthias Söllner. Drawing on Lee and See (2004), Söllner and colleagues propose a model of technology system trust antecedents that includes performance, purpose and process (Hoffman & Söllner, 2014; Söllner, Pavlou, & Leimeister, 2013). Within this model, performance is an indicator of ability like constructs such as competence, reliability and information accuracy. Purpose (sometimes referred to as helpfulness) represents an assessment of the motives and benevolence of developers, while process reflects user perceptions of the predictability, consistency, dependability and understandability of the system. In a similar vein, McKnight and colleagues put forward a model of attributes of information technology that contribute to trust in a technology system. Their subdimensions of functionality, helpfulness and reliability are proposed to map directly to the more traditional ability, benevolence and integrity and predictability characteristics. Thus far, the issue of value congruence remains largely unaddressed in the context of trustworthiness cues for technology systems. Table 1 displays how seminal models of trustworthiness have been translated in this context.

Third, in interpersonal trust relationships trust behaviour and behavioural intentions are often portrayed as cooperation (Deutsch, 1958) or reliance and disclosure intentions (Gillespie, 2003). A common critique of the trust literature is that there is a scarcity of theoretical and empirical research exploring actual trust behaviour, as opposed to trust intentions or cooperative behaviour in a laboratory setting. This criticism has been addressed to some extent in the online environment where a more specific context has allowed researchers to explore trust behaviours in more detail. Risk taking in a relationship has been operationalised in the online context as a variety of behaviours including purchasing behaviours (Lim, Sia, Lee, & Benbasat, 2006; Pavlou & Dimoka, 2006) and interaction with technology (McKnight et al., 2011).



	Traditional Trustworthiness		Trust in Technology Systems	
Sources	Mayer, Davis, & Schoorman (1995, pp. 717-719)	McKnight, Chervany & Cummings (1998), McKnight & Chervany (2000, p. 831)	Söllner, Pavlou, & Leimeister (2013), Hoffman & Söllner (2014, pp. 118-119)	McKnight, Carter, Thatcher, & Clay (2011, pp. 12:7-12:8)
Trustworthiness Dimensions	**Ability** *"that group of skills, competencies, and characteristics that enable a party to have influence within some specific domain."*	**Competence** *"one believes the other person has the ability or power to do for one what one needs done."*	**Performance** *"the user's assessment of the capability of the system in helping him to achieve his goals"* including assessments of competence, information accuracy, reliability over time and functionality	**Functionality** *"The belief that the specific technology has the capability, functionality, or features to do for one what one needs to be done."*
	Benevolence *"the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive."*	**Benevolence** *"one believes the other person cares about one and is motivated to act in one's interest. A benevolent person does not act opportunistically."*	**Purpose/Helpfulness** *"the user's assumptions of the system designer's intention when developing the system"* including assessments of motives, benevolence and faith	**Helpfulness** *"The belief that the specific technology provides adequate and responsive help for users."*
	Integrity *"the trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable."*	**Honesty/Integrity** *"one believes the other person makes good faith agreements, tells the truth, and fulfills promises (Bromiley & Cummings, 1995)".* **Predictability** *"one believes the other person's actions (good or bad) are consistent enough that one can forecast them in a given situation."*	**Process/Predictability** *"the user's perception regarding the system's functionality and the degree to which the system's algorithms are chosen and implemented appropriately"* including assessments of dependability, understandability, control and predictability	**Reliability** *"The belief that the specific technology will consistently operate properly."*

Figure 1. Comparing Models of Trustworthiness Across Contexts.

VULNERABILITY AND ASSURANCE ON THE INTERNET

Do perceptions of risk and vulnerability differ in an online context from those discussed in the traditional trust literature? What do individuals or organisations do to alleviate these concerns? While many similarities exist between online and offline trust relationships (Corritore, Kracher, & Wiedenbeck, 2003), significant differences are also apparent. In line with our discussion above, trust interactions with individuals or organisations online will generally be complicated by trust in the system of the internet itself and third party organisations that may be involved in supporting the technology (Beldad, de

Jong, & Steehouder, 2010). Many online trust interactions are also characterised by a lack of face to face interaction, an asymmetry in the information available to each party and privacy concerns.

A lack of face to face interaction in online relationships can impede trust development through the removal of physical cues such as gestures, eye contact and facial expressions (Jarvenpaa & Leidner, 1998). At an organisational level, research suggests that trust can transfer from offline to online if there is evidence that the organisation providing the web service also has physical premises (Stewart, 2003). Similarly, information asymmetry between parties interacting online is driven by physical separation between individuals and a relative lack of opportunity to monitor previous behaviour, which influences the quantity and quality of information shared between them. Typically, in ecommerce relationships, information asymmetry is thought to favour the vendor leaving the buyer with high levels of uncertainty (Pavlou, Liang, & Xue, 2007).

Online information privacy is a key concern for the digital consumer (for an overview see Grant & Waite, 2013). Information privacy describes issues relevant to access to personal information that is individually identifiable (Smith, Dinev, & Xu, 2011). Concerns regarding privacy violations can be categorised according to whether they relate to social, institutional (Brandtzaeg, Luders, & Havard Skjetne, 2010) or malicious third party privacy. Social privacy issues relate to the risks involved in other users sharing information you have disclosed to them, such as making private communications public. Institutional privacy refers to the unauthorised use of personal information by organisations you have disclosed information to, for instance, sharing customer data with third party organisations for marketing purposes. In contrast, concerns related to malicious third parties cover security and privacy threats from insider misbehaviour, and externally from malevolent third parties such as cybercriminals. Consideration of privacy and security related issues are important to understanding online trust as empirical research demonstrates that perceptions of privacy and security are key antecedents of trust in ecommerce transactions (Pavlou & Chellappa, 2001).

In the face of these risks and vulnerabilities, there are a number of system level cues which may be important to building trust at individual and organisational levels by providing a sense of security and a reduction in feelings of uncertainty. In their seminal paper on initial trust, McKnight et al. (1998) posit that institution or system based trust is composed of structural assurances and perceptions of situational normality. Structural assurance refers to the safeguards and regulations inherent in the context that are likely to govern or restrict certain behaviours. In the internet environment, cues for such structural assurances may include affiliations with a third party, seals of approval, policy or guarantee statements, firewalls, encryption mechanisms and contact details for representatives of an overseeing organisation (Gefen, Karahanna, & Straub, 2003; Pavlou, 2003). Structural assurances such as these have been reported to significantly reduce system related uncertainty and build trust (Kim & Prabhakar, 2002). In light of this many government and industry level organisations introduce regulations and monitoring mechanisms to govern conduct around compliance to a set of minimum standards across industries and organisations as well as mandatory rules on disclosure. However, outside of the online context, the influence of control mechanisms on trust has been the focus of a long history of debate. Empirical research has shown that control mechanisms are seldom flawless (Sitkin & Roth, 1993) and may even undermine cooperation (Fehr & Gächter, 2002).

Situational normality describes the extent to which the setting is perceived as normal, customary and in proper order (McKnight et al., 1998). In the context of the internet, feelings of familiarity are reported to be an important predictor of trust in online organisations

(Bhattacherjee, 2002; Gefen, 2000). Situational normality influences trust both directly and indirectly via perceptions of how easy a technology is to use (Gefen et al., 2003). Furthermore when experience with a technology matches expectations, users report positive attitudes towards that technology while unmet expectations lead to negative consequences (Lankton, McKnight, & Thatcher, 2014). The concept of situational normality has been applied repeatedly in the design of IT applications. For instance, many cloud based storage services (e.g. Dropbox, Office365, Apple iCloud) offer folder solutions that are designed to integrate and look very similar to those provided by the user's chosen operating system.

EMPIRICAL RESEARCH ON TRUST AND THE INTERNET

Research examining trust in an online context has been conducted across a range of disciplines including human-computer interaction, organisational behaviour, economics, and marketing and management information systems. This section of the chapter will draw together some of the research from these areas to explore the issues of individual trust in individuals, organisations and technology systems in the context of the internet.

Interpersonal Trust Online

Online interaction between individuals is increasing for professional and personal purposes alongside the globalisation and virtualisation of work and the popularity of social networks and cross platform mobile messaging applications. Using the internet as a medium for communication, we interact with known and unknown others through channels such as email, social media, instant messaging and online video conferencing.

As a critical ingredient of positive social interaction, trust is regularly cited as a potential hurdle for effective online communication (Naquin & Paulson, 2003). Early theoretical work from Green and Gillespie (2014) suggests that online interactions are experienced as increasingly distant and abstract, and thus more difficult for trust building, depending on the extent to which they are temporally, spatially and geographically separate. Communication methods such as online teleconferencing are affected only by geographic separation while text-based, online communication is also characterised by spatial separation as no physical or non-verbal cues are available. In addition, text-based communications can also be temporally separated depending on whether the interaction happens in real time (e.g. live chat) or has potential to be time lagged (e.g. email). Effective communication in such scenarios is impacted by the challenge of communicating affective and relational information through text-based online communication (Walther, 1995). This is a problem which has arisen through an emphasis on work effectiveness and neglect of socioemotional communication in designing computer-mediated communication technology (Redfern & Naughton, 2002). Naquin and colleagues argue that psychological distance triggers different norms for appropriate behaviour and increases the likelihood of deceptive behaviour (Naquin, Kurtzberg, & Belkin, 2010). Interestingly in online avatar interactions, where visual cues are reembedded into the online context, alterations to avatar appearance influence trust in the party represented by that avatar (Peña & Yoo, 2014). In fact, some research suggests that avatar mediated student communications show no significant differences from video conferencing in terms of affective trust or perceptions of social closeness (Bente, Ruggenberg, Kramer, & Eschenburg, 2008).

While the majority of personal and workplace relationships now include some degree of virtual interaction, a large body of research has been dedicated to the study of virtual work including virtual teams and virtual leadership (for a full discussion see Gilson, Maynard, Young, Vartianen, & Hakonen, 2015). Virtual teams are characterised by geographical dispersion and a reliance on information technology as their primary means of coordinating work (Hertel, Geister, & Konradt, 2005). Approximately 66% of multinational organisations use virtual teams to organise their workforce (Society for Human Resource Management, 2012) and this number continues to rise (Gilson et al., 2015). The importance of trust for collaboration is widely acknowledged, and virtual team researchers argue that trust is even more vital for collaboration in virtual work where individuals experience a high level of self-direction and self-control (Robert, Dennis, & Hung, 2009). Robert et al. (2009) demonstrate that higher perceptions of the risk involved in interacting via the internet decreases as virtual teams gather more information about each other. Henttonen and Blomqvist (2005) argue that trust can be built in virtual teams through positive communication behaviours such as timely responding, provision of feedback and openness. For leaders of virtual teams and organisations, typically referred to as e-leaders (see Avolio, Kahai, & Dodge, 2000), appearing available and engaging in informal personal communication is important to building follower trust (Savolainen, 2014). Overtime, computer-mediated teams can develop levels of trust comparable to traditional face-to-face teams, but trust starts out at a lower level and takes longer to develop in computer mediated teams, influenced by the more limited communication medium (Wilson, Straus, & McEvily, 2006).

Outside of the work environment, individuals use the internet to establish and maintain a host of personal relationships. Social media platforms are designed to allow users to create and share information with others creating a conflict between sociability, social capital and heightened visibility for shared content on one side and privacy on the other (Brandtzaeg et al., 2010). Many of these platforms present the opportunity for interaction with individuals or groups of individuals who are largely unknown and often likely to remain unknown to the user. For instance, social media platforms like Twitter involve communicating information to a wide network of followers with the potential for that information to be shared far beyond one's own social network. These new media offer interesting avenues for the study of interpersonal interaction and trust at an individual level.

In particular, the internet offers individuals increased control over self-presentation and impression management (Ellison, Heino, & Gibbs, 2006) and identity misrepresentation which may have important implications for trust. Unfortunately, much of the research on trust in this context has focused on the social media platform itself as the referent rather than other users.

Individual Trust in Online Organisations

Consumer trust relationships with organisations in the context of the internet resemble offline trust interactions with organisations in that they involve conditions of risk and vulnerability for the consumer as a result of reliance on an organisation. However as discussed above, the context of the internet brings some unique aspects of the trust relationship into consideration. For organisations providing services over the internet, consumer trust in web-based services is critical to enable three risk-taking behaviours: following advice from the website organisation; sharing personal information with the organisation via the website; and making purchases from the organisation via the website (McKnight, Choudhury, & Kacmar, 2002). Much of the research carried out in this area has been in the context of e-commerce, with limited attention focused on other types of e-services such as e-health and e-government. This section draws on several review papers (Beldad et al., 2010; Wang & Emurian, 2005; Grabner-Krauter & Kalusha, 2003) in discussing the empirical research on trust in online organisations. For the purposes of this section, we have organised our discussion into three categories: website characteristics, organisational characteristics and the external environment.

Website Characteristics. The impression, content and interactive experience of a website can influence consumer trust perceptions of the organisation it represents, in a similar manner to the influence of the physical premises of an organisation and interaction with its agents. For instance, website visual design factors such as colour and graphics can influence trust beliefs. Cool pastel colour tones, symmetrical colour balance, low brightness and use of 3D dynamic graphic effects have been shown to bring about feelings of trustworthiness (Kim & Moon, 1998). However, preferences for visual factors have been found to vary across culture (Cyr, Head, & Larios, 2010) and gender (Tuch, Bargas-Avila, & Opwis, 2010), limiting the usefulness of website aesthetics to elicit trust in a universal context. Research suggests that individuals are also influenced by less aesthetic factors such as perceived ease of use and information quality. Perceived ease of use in the context of the internet consists of easy website navigation enabled by the overall structure, organisation and accessibility of information, and has a key impact on the formation of trust in e-commerce (Bart, Shankar, Sultan & Urban, 2005; Flavian, Guinaliu, & Gurrea, 2006; Koufaris & Hampton-Sosa, 2004). Furthermore, quality of website information (accuracy, currency, clarity, completeness) is critical for online trust in e-organisations (Bart et al., 2005; Kim, Song, Braynov, & Rao, 2005; Liao, Palvia, & Lin, 2006).

Although, both aesthetic and practical website features are important cues for trusting an organization, researchers have yet to agree how these factors interact. Evidence suggests that a balance is needed between good web-site design to attract a consumer, and good web-site content to retain a consumer. Consumers may never reach a stage of information quality assessment if they reject the site early on because of poor website design, but once the design is acceptable to them, quality of information becomes key to building trust (Sillence, Briggs, Harris, & Fishwick, 2007). Other researchers (e.g. Li & Yeh, 2010) have suggested that the impact of design aesthetics on trust is mediated by perceptions of usefulness and ease of use. In contrast, Seckler and colleagues suggest that website design issues are more likely to influence perceptions of distrust, whereas trust is based on social factors such as reviews or recommendations by friends (Seckler, Heinz, Forde, Tuch, & Opwis, 2015).

Another theme in the website trust literature is the influence of social and relational factors on online trust. Social presence cues, such as socially rich text content, personalized greetings, human photos, audios or videos, live chats and online user numbers, can make impersonal online interactions more personal thereby increasing levels of trust (Cyr, Hassanein, Head, & Ivanov, 2007; Hassanein & Head, 2007) especially the benevolence aspects of trust (Gefen & Straub, 2004). However, reactions to the use of photographs on websites can be mixed, ranging from enthusiasm to suspicion, and they can be considered as superfluous to functionality or even manipulative (Riegelsberger & Sasse 2002, Riegelsberger, Sasse, & McCarthy, 2003), suggesting care is needed in this aspect of trust elicitation. Similarly, customisation -tailoring websites, products and services to target users- and personalisation -the inclusion of personal information- can improve levels of trust (Beldad et al., 2010; Koufaris & Hampton-Sosa, 2004). However, concerns for privacy in these instances can undermine trust particularly if information is collected covertly (Aguirre, Dominik, Mahr, Grewal, de Ruyter, & Wetzels, 2015).

Finally, consumer perceptions of website security and privacy are vital for online trust (Kim, Ferrin, & Rao, 2008). The inclusion of strong privacy policy declarations on the website can improve levels of trust (Lauer & Deng, 2007). Indeed, the mere existence of a privacy policy may serve to build trust, regardless of the content, as many consumers ignore the actual policy and assume it is similar to others (Pan & Zinkhan, 2006). Organisations often try to communicate security and privacy through the use of independent third party certification evidenced by the presence of seals of approval on a website. These seals communicate that the organisation adheres to the seal programme’s standards and principles, and can be successful trust-building mechanisms in e-commerce (Aiken & Bousch, 2006; Chang, Cheung, & Tang, 2013; Hu, Wu, Wu, & Zhang, 2010), although research findings in this area are mixed (e.g. Kim, Ferrin, & Rao, 2008). Trust seals can be classified into three categories: security seals, privacy seals and business identity seals (Hu et al., 2010, Ozpolat & Jank, 2015). Security seals (e.g. VeriSign, McAfee, GoDaddy) certify that data transmission is secure through SSL technologies and that the website is protected against malware. Privacy seals (e.g. TRUSTe, VeraSafe) certify that the website retailer has a privacy policy regarding consumer data confidentiality. Business identity seals (e.g. BBB, buySAFE) certify that the website retailer is a real, trustworthy business. Trust seals have been shown to be more effective for small online retailers and new shoppers, compensating for both shopper experience and seller sales volume (Ozpolat & Jank, 2015). Trust seals have been shown to have a greater effect on perceived trustworthiness than either objective third-party reviews or declarations of advertising investment by a retailer (Aiken & Boush, 2006). However, the presence of too many seals can lower the likelihood of purchase completion (Ozpolat & Jank, 2015), and combined multiple function seals are not necessarily more effective than single function seals (Hu et al., 2010).

Organisation Characteristics. In addition to characteristics of the website, consumer trust in an organisation is also influenced by more direct perceptions of the organisation itself. A number of organisational characteristics have been reported to impact individual trust in online organisations. Specifically, satisfaction with previous online transactions with a particular company allows organisations to build a more long-term trusting relationship with their consumers (Casalo, Flavian, & Guinaliu, 2007; Pavlou, 2003). An offline presence has also been shown to enhance online trust (Kuan & Bock, 2007), although not when the offline and online channels are poorly integrated (Teo & Liu, 2007). Similarly, perceived size of an e-service organisation may have an impact on trust, although research results in this area are mixed (Jarvenpaa, Tractinsky, & Vitale, 2000; Teo & Liu, 2007).

Consumers who do not have previous experience with an online e-service vendor often rely on the reputation of that vendor when making a trust decision (e.g. Jarvenpaa, Tractinsky, & Saarinen, 1999; McKnight et al., 2002). Similar to offline transactions, trust can result from being well-known and well-respected (e.g. Kim, Ferrin, & Rao, 2003), and from word-of-mouth within a consumer's social network (Kuan & Bock, 2007). Uniquely, the nature and scale of the internet facilitates easy provision of feedback from a wider set of previous buyers in relation to their experience of specific products or sellers, via online feedback mechanisms (Dellarocas, 2003) and reputation systems (Josang, Ismail, & Boyd, 2007; Resnick, Zeckhauser, Friedman, & Kuwabara, 2000). Online feedback mechanisms are primarily informal and self-regulated (for example, Tripadvisor, Ebay), and usually there is no way of verifying the feedback with the assumption that false or biased information will be diluted by a larger amount of accurate feedback (Sabater & Sierra 2005). Research has shown that these mechanisms engender trust, not only in the reported reputable sellers (Koehn, 2003), but also in the wider community of sellers in an online marketplace such as Amazon (Pavlou & Gefen, 2004). Some scholars have argued that high usage of third party feedback mechanisms in supporting consumer transactions may, in fact, bring about so much certainty that conditions of risk and vulnerability are effectively eliminated (Gefen & Pavlou, 2012). In practice however, while strong institutional structures may reduce the role of trust in the economic aspect of internet transactions, trust may continue to play a vital role in the social aspect of internet transactions (Gefen & Pavlou, 2012). For example, the comments themselves in feedback mechanisms seem to play a role above and beyond the actual numerical feedback rating, building trust by addressing the credibility and benevolence of the seller, more on a social than an economic basis (Pavlou & Dimoka, 2006).

The Role of Context. The system level determinants of online trust in an organisation differ according to the function and context of the website in question (Bart et al., 2005; Bansal, Zahedi, & Gefen, 2016). Privacy and order fulfilment are the strongest determinants of trust where there is high information risk and high involvement, such as travel sites. In contrast, navigation is strongest for information-intensive sites, such as sports, portal, and community sites while brand strength is strongest for high-involvement categories, such as automobile and financial services sites (Bart et al., 2005). Personal safety is emerging as a key consideration for trust in newer peer-to-peer marketplaces such as private accommodation sharing (e.g. AIRBNB) and location based taxi hire and ridesharing services (e.g. Uber, Lyft, Hailo), where the service goes beyond buying a physical product or exchanging information, and enables the connection of strangers with each other for access based consumption. In this sharing economy, in addition to traditional reputation feedback mechanisms, marketplace intermediary companies are prioritising identity verification as part of their service, in order to promote trust. In fact, with the right screening and authentication mechanisms and safety policies, there is a case to be made that peer-to-peer marketplaces for access based consumption can be safer (for both service providers and consumers) than the traditional business model it replaces (such as hailing a cab on the street). Although, in many markets, there is greater or lesser regulation than traditional models. This unbalanced approach to regulation may create an uneven playing field for market participants.

The legal jurisdiction in which internet transactions are conducted is also critical for trust formation and maintenance. The inherently global nature of the internet, combined with the recent advent of cloud computing, has introduced issues of legal jurisdiction to many transactions. For example, the consumer could be in one country, the organisation in another, the server provider in another, and the data held in another, all with different national laws applicable. Relatedly, beliefs about government surveillance on the internet can impact privacy concerns and intentions to disclose personal information. While some trust scholars propose that controls and monitoring are likely to undermine trust (De Jong & Dirks, 2012), this may not always be the case, particularly where the monitoring is expected and considered appropriate (Ferrin, Bligh, & Kohles, 2007). A perceived need for the government to have greater access to personal information and to monitor personal activities in order to increase security procedures and to ensure safe and reliable internet transactions, can reduce privacy concerns and encourage disclosure of personal information. On the other hand, concerns about government intrusion regarding individual internet activity and account information increases privacy concerns (Dinev, Hart, & Mullen, 2008). As our use of, and reliance on, the internet as a means for personal and professional interaction grows this is likely to become an issue of greater focus for scholars interested in trust in the internet context.

Finally, issues of temporal context play a role in which antecedents drive trust between individuals and online organisations. In new relationships with unfamiliar vendors website quality, vendor reputation and structural assurance strongly influence consumer trust (McKnight et al., 2002). Consumers interacting with a website for the first time make strong judgements about the unknown vendor from their initial experience on the website (including technical performance, visual appeal, ease of navigation, ease of access to information, contact details). In addition, second-hand information about the reputation of the vendor and structural assurance play a role in influencing initial web-based trust in vendors (McKnight et al., 2002). In more established relationships, familiarity and prior satisfaction with e-commerce in general, influence trust in specific web vendors (Yoon, 2002). For experienced, repeat online shoppers, trust has been shown to be fostered by a typical and easy to use web-site with built-in safety mechanisms (Gefen, Karahanna, & Straub, 2003).

In any ongoing relationship, trust has the potential to be violated. The extent to which a consumer information privacy violation leads to a reduction in trust in the organisation can depend on the attributed cause of the violation. General trust research has found that integrity-based violations have a greater impact on trust than competence-based violations (Kim, Dirks, Cooper, & Ferrin, 2006). Similarly, in an online context, unauthorised sharing of information by the website company (an integrity violation) may have a greater negative impact on trust than unauthorised access by external agents (a competence violation; Bansal & Zahedi, 2015). In line with offline trust violation research (Kim, Ferrin, Cooper, & Dirks, 2004), apology is an effective response in both situations (but more so for hacking), whereas denial is only effective for the externally attributed hacking violation (Bansal & Zahedi, 2015).

Individual Trust in Technology Systems

Trust in technology is an under-explored area of research (Lankton & McKnight, 2011). Most of the trust research in online environments examines trust in the humans who use the technology or trust in the organisations that provide the technology. Research that has focused on trust in the technology system itself has occurred primarily in the computer science and information systems literature. Unfortunately, conceptualisations of trust and related constructs in the field of computer science are considerably different to those found in the business literature. Trust is often portrayed as synonymous with security and vulnerability is associated with low levels of trust whereby trusted systems are those where all vulnerabilities have been eliminated (e.g. Abbadi & Alawneh, 2012; Takabi, Joshi, & Ahn, 2010). Contributions to understanding from the field of information studies have however begun to shed light on how trust, as a generalised and more specific psychological state, can be applied to understand the relationship between individuals and technology systems.

Generalised trust in information technology plays a role in shaping IT related beliefs and behaviour (McKnight, Carter, Thatcher, & Clay, 2011). This propensity to trust technology is a a form of general trust similar to dispositional trust, and distinguished from specific trust (in the merchant and the website).McKnight and colleagues (2011) differentiate between faith in general technology – a belief that IT is generally reliable, functional and helpful – and a technology trusting stance – a belief that interacting with technology is likely to lead to positive outcomes. In an internet context, Thatcher, Carter, Li, & Rong (2013) examine general trust in the internet as an IT infrastructure and report that trust in the internet (trusting beliefs in three technical attributes—capability, reliability and security) significantly influences trust in the website, but does not influence trust in the online merchant. They suggest that trust in IT infrastructure is a foundational belief for online behaviour, and that the evolving nature of the internet environment makes this a dynamic factor in trust interactions online. Empirical evidence demonstrates the impact of a lack of trust in internet technology on outcomes such as anxiety about internet use (Thatcher, Loughry, Lim, & McKnight, 2007).

Researchers have also examined trust in specific technology systems. However, as discussed above, considerable debate exists around whether trust as a psychological state can be experienced in a relationship with another party that does not possess consciousness or agency. One perspective on this maintains that trust in technology reflects beliefs about the technology’s characteristics rather than its will or motives (McKnight, Carter, Thatcher, & Clay, 2011). From this perspective, uncertainty and vulnerability in trusting technology systems arises predominantly from the potential of unanticipated technical problems or lack of knowledge on the part of the trustor (Paravastu, Gefen, & Creason, 2014). However, with the increasing automation of technology systems and the advent of ubiquitous information systems, it can be argued that the systems themselves can possess attributes such as benevolence and integrity.

Much of the research in this area has thus far focused on technologies that have fewer human-like characteristics and more technology-like characteristics e.g. software. However, in many online interactions with technology, the distinction between human and technology characteristics is not all that clear. In a study of trust in relation to online recommendation agents (intelligent virtual assistant software), Wang and Benbasat (2005) found that in addition to a rational process governed by assessments of perceived usefulness and perceived ease of use (technology acceptance model; Davis, 1989), consumers treat online recommendation agents as social actors and form social relationships with them that involve trust. Similar to models of interpersonal trust (Mayer et al., 1995; McKnight et al., 2002), they contend that consumers assess the competence of the recommendation software to accurately understand their needs, its benevolence demonstrated by prioritisation of the needs of the consumer over those of the e-service provider, and its integrity demonstrated by the provision of unbiased recommendations. In another study of online recommendation agents, Komiak and Benbasat (2006) suggest that trust in technology consists of emotional trust as well as cognitive trust, and is influenced by the perceived personalisation of the IT artefact. Similarly, in a study of social networking, Lankton & McKnight (2011) discovered that users trust Facebook as both a technology and as a quasi-person, proposing an integrated trustworthiness assessment model covering both interpersonal and technology factors (competence/functionality, integrity/reliability, benevolence/helpfulness). However, it seems that human-like trust only applies to particular internet technologies, and may depend on the characteristics of the individual technology such as intelligence and personalisation (Wang & Benbasat, 2005).

Recent advances in cognitive neuroscience show promise for new insights into whether or not trust in technology is similar or different to interpersonal trust. Riedl, Mohr, Kenning, Davis and Heekeren (2014) demonstrate that people are better at making trustworthiness assessments of humans than of human-like avatars, and neurobiological analysis shows that trustworthiness assessments activate the medial frontal cortex of the brain more strongly where the trustee is a human rather than an avatar. In the context of ecommerce, Dimoka (2010) finds support for different constructs of trust and distrust, which activate different brain areas. There appears to be considerable potential for using cognitive neuroscience theories and functional brain imaging tools to enhance the understanding of trust in the broad environment of the Internet.

FUTURE DEVELOPMENTS AND POTENTIAL AVENUES FOR RESEARCH

While a considerable body of literature has been devoted to examining online trust, the fast pace of change in the technology realm means that methods of online interaction are continually updated and new trust related issues will continue to arise. As it stands there are a number of key issues which deserve further attention.

The conceptualisation of trustworthiness in relation to a technology system requires further consideration both theoretically and empirically. For instance, it may be that certain dimensions of trustworthiness are more applicable in particular online circumstances such as those which involve more vulnerability on behalf of the trustor or more autonomy and intelligence on behalf of the technology. Similarly, privacy debates and the extent to which our lives are now accessible online are likely to highlight the more motivational and value laden aspects of trustworthiness in interacting online with individuals and organisations. As we continue to grapple with the appropriateness of the traditional ABI (ability, benevolence and integrity) model for the internet context, the concepts of predictability and value congruence may gain additional significance in this regard. Once we have gained further conceptual clarity around the components of trustworthiness in the online context, further research into how these characteristics are best communicated at the individual, organisational and system levels will provide an interesting avenue for researchers.

The internet context also offers a fruitful avenue for further research into the debate around trust and control. As organisations and governments strive to keep pace with technological advances and their influence on society and business, the focus has been predominantly on the introduction of control mechanisms such as regulation and contracts or service level agreements to provide a foundation for interaction. Although often considered a costly overhead with negative trust impacts, the benefits of legal remedies as a support for trust have also been highlighted (e.g. Sitkin, 1995). However, the complexity of the impact of these mechanisms on trust requires further research. For example, in a general context, contracts are proposed to have both positive and negative influences on interorganisational trust through different control and coordination mechanisms (Lumineau, in press). The application of trust and control theory to the context of the Internet offers significant potential for further theoretical development and empirical research.

One relevant issue that is gaining increasing attention in terms of media debate is online privacy. As the internet has evolved and content becomes increasingly user generated, it is not merely that corporations and governments can engage in surveillance, but that private citizens themselves will directly engage in sousveillance of their own lives and of those that they encounter on a day-to-day basis. This can be seen already with the use of social media to tag the location and activities of contacts or ubiquitous technology in the form of wearable devices such as glasses. This data and its metadata may be stored, accessed and combined with other data sources along the chain of service provision inherent in the Future Internet potentially in unintended ways and for unintended purposes. As a result, the number of unknown referents involved in any online trust relationship is likely to grow and theory and empirical work regarding trust in unknown individuals and systems becomes increasingly relevant. Another aspect of online privacy with relevance for trust scholars is the increased prevalence of data privacy breaches and the effectiveness of trust breach responses. In the context of many trust referents within the internet service supply chain, a deeper examination of responses maybe appropriate, including not only apologies and denials, but potentially other responses such as reticence (Bansal & Zahedi, 2015), social accounts or explanations (Sitkin & Bies, 1993).

The emergence, maturation and integration of new technologies such as cloud computing, social media, big data, sensor and mobile computing technologies is rapidly redefining what the Internet is and might be in the future. Unsurprisingly, the “Future Internet” or the “Internet of Everything” remains definitionally ambiguous although encompasses a number of common features and themes. At the core of the Future Internet, is the increasing pervasiveness of highly distributed heterogeneous but interconnected technology infrastructures. The pervasiveness, interoperability and inter-dependency of these infrastructures extends how we conceive of the Internet beyond networks and people to the relationship between machines, virtual constructs or other entities (including networks and people) with greater or lesser degrees of autonomy and intelligence. Furthermore, as the technology underlying these infrastructures complexifies there are significant implications for an individual’s capacity to understand new technologies and make sense of their relationship with entities in the Future Internet. This raises questions for researchers around how trust can be developed in the face of high levels of uncertainty and a lack of prior experience. These contextual issues may increase the difficulty of forming systematic, logical trustworthiness judgements, leading to heuristic factors playing an increasing role in driving online trust. Such a process may also provide a central role for emotions as an important determinant of trust. Although they have been largely overlooked in the existing literature, emotions both negative (e.g. fear, anxiety, anger) and positive (e.g. enthusiasm, excitement) are likely to influence trust and risk related behaviors online. The debate on whether we can trust technology is not a new one but is an increasingly relevant one and will be for a long time to come.

REFERENCES

Abbadi, I. M., & Alawneh, M. (2012). A framework for establishing trust in the Cloud. *Computers & Electrical Engineering*, *38*(5), 1073-1087.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34-39.

Aiken, K. D., & Boush, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: investigating online trust and the context-specific nature of internet signals. *Journal of the Academy of Marketing Science*, *34*(3), 308-323.

Avolio, B. J., Kahai, S., & Dodge, G. E. (2001). E-leadership: Implications for theory, research, and practice. *The Leadership Quarterly*, *11*(4), 615-668.

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62-77.

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

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, *69*(4), 133-152.

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.

Bente, G., Rüggenberg, S., Krämer, N. C., & Eschenburg, F. (2008). Avatar-mediated networking: Increasing social presence and interpersonal trust in net-based collaborations. *Human Communication Research*, *34*(2), 287-318.

Berthon, P. R., Pitt, L. F., Plangger, K., & Shapiro, D. (2012). Marketing meets Web 2.0, social media, and creative consumers: Implications for international marketing strategy. *Business Horizons*, 55(3), 261-271.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems*, *19*(1), 211-241.

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook “friends”? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human–Computer Interaction*, *26*(11-12), 1006-1030.

Briggs, P., Simpson, B., & De Angeli, A. (2004). Personalisation and trust: a reciprocal relationship?. In J. Karat (Ed.). *Designing Personalized user experiences in eCommerce* (pp. 39-55). Springer Netherlands.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The influence of satisfaction, perceived reputation and trust on a consumer's commitment to a website. *Journal of Marketing Communications*, *13*(1), 1-17.

Chang, M. K., Cheung, W., & Tang, M. (2013). Building trust online: Interactions among trust building mechanisms. *Information & Management*, *50*(7), 439-445.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737-758.

Cyr, D., Hassanein, K., Head, M., & Ivanov, A. (2007). The role of social presence in establishing loyalty in e-service environments. *Interacting with Computers*, *19*(1), 43-56.

Cyr, D., Head, M., & Larios, H. (2010). Colour appeal in website design within and across cultures: A multi-method evaluation. *International Journal of Human-Computer Studies*, *68*(1), 1-21.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

De Jong, B. A., & Dirks, K. T. (2012). Beyond shared perceptions of trust and monitoring in teams: implications of asymmetry and dissensus. *Journal of Applied Psychology*, *97*(2), 391-406.

Dellarocas, C. (2003). The digitization of word of mouth: Promise and challenges of online feedback mechanisms. *Management Science*, *49*(10), 1407-1424.

Deutsch, M. (1958). Trust and suspicion. *Journal of Conflict Resolution*, 265-279.

Dietz, G., & Hartog, D. N. D. (2006). Measuring trust inside organisations. *Personnel Review*, *35*(5), 557-588.

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly, 34*(2), 373-396.

Dimoka, A., Pavlou, P. A., & Davis, F. D. (2011). Research commentary on NeuroIS: The potential of cognitive neuroscience for information systems research. *Information Systems Research*, *22*(4), 687-702.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233.

Ellison, N., Heino, R., & Gibbs, J. (2006). Managing impressions online: Self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication*, *11*(2), 415-441.

Fehr, E., & Gachter. S. (2002). Do incentive contracts undermine voluntary cooperation. Working Paper No. 34, Institute for Empirical Research in Economics, University of Zurich.

Ferrin, D. L., Bligh, M. C., & Kohles, J. C. (2007). Can I trust you to trust me? A theory of trust, monitoring, and cooperation in interpersonal and intergroup relationships. *Group & Organization Management*, *32*(4), 465-499.

Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information & Management*, *43*(1), 1-14.

Friedman, B., Khan Jr, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34-40.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega*, *28*(6), 725-737.

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

Gefen, D., & Pavlou, P. A. (2012). The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Information Systems Research*, *23*(2), 940-959.

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega*, *32*(6), 407-424.

Gillespie, N. (2003). Measuring trust in work relationships: The Behavioural Trust Inventory. Paper presented at the annual meeting of the Academy of Management, Seattle, USA.

Gilson, L. L., Maynard, M. T., Young, N. C. J., Vartiainen, M., & Hakonen, M. (2015). Virtual teams research 10 years, 10 themes, and 10 opportunities. *Journal of Management*, *41*(5), 1313-1337.

Green, T., & Gillespie, N. (2014). Swift trust in virtual services: A construal-level perspective. Paper presented at the 8th First International Network on Trust Conference (FINT), Coventry University, United Kingdom.

Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: A review and critical assessment. *International Journal of Human-Computer Studies, 58*(6), 783-812.

Grant, I., & Waite, K. (2013). In R. W. Belk, & R. Llamas (Eds.). *The Routledge companion to digital consumption*. Routledge, 333-345.

Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies*, *65*(8), 689-708.

Henttonen, K., & Blomqvist, K. (2005). Managing distance in a global virtual team: the evolution of trust through technology-mediated relational communication. *Strategic Change*, *14*(2), 107-119.

Hertel, G., Geister, S., & Konradt, U. (2005). Managing virtual teams: A review of current empirical research. *Human Resource Management Review*, *15*(1), 69-95.

Hoffmann, H., & Söllner, M. (2014). Incorporating behavioral trust theory into system development for ubiquitous applications. *Personal and Ubiquitous Computing*, *18*(1), 117-128.

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems*, *48*(2), 407-418.

Jarvenpaa, S. L., & Leidner, D. E. (1998). Communication and trust in global virtual teams. *Journal of Computer‐Mediated Communication*, *3*(4).

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).

Jarvenpaa, S. L., Tractinsky, N., & Vitalec, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, *1*, 45-71.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*(2), 618-644.

Kim, P. H., Dirks, K. T., Cooper, C. D., & Ferrin, D. L. (2006). When more blame is better than less: The implications of internal vs. external attributions for the repair of trust after a competence-vs. integrity-based trust violation. *Organizational Behavior and Human Decision Processes*, *99*(1), 49-65.

Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the shadow of suspicion: the effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of Applied Psychology*, *89*(1), 104-118.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544-564.

Kim, D. J., Song, Y. I., Braynov, S. B., & Rao, H. R. (2005). A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. *Decision Support Systems*, *40*(2), 143-165.

Kim, J., & Moon, J. Y. (1998). Designing towards emotional usability in customer interfaces: Trustworthiness of cyber-banking system interfaces. *Interacting with computers*, *10*(1), 1-29.

Koehn, D. (2003). The nature of and conditions for online trust. *Journal of Business Ethics*, *43*(1-2), 3-19.

Komiak, S. Y., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly*, 941-960.

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management*, *41*(3), 377-397.

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

Lankton, N. K., & McKnight, D. H. (2011). What does it mean to trust Facebook?: examining technology and interpersonal trust beliefs. *ACM SIGMIS Database*, *42*(2), 32-54.

Lankton, N., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into Expectation Disconfirmation Theory. *The Journal of Strategic Information Systems*, *23*(2), 128-145.

Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, *6*(5), 323-331.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. Human Factors. *The Journal of the Human Factors and Ergonomics Society*, 46(1), 50-80.

Lewicki, R. J., & Brinsfield, C. (2012). Measuring trust beliefs and behaviours.In F. Lyon, G. Mollering, M.N.K. Saunders (Eds.). *Handbook of research methods on trust, 29-39.*

Li, Y. M., & Yeh, Y. S. (2010). Increasing trust in mobile commerce through design aesthetics. *Computers in Human Behavior*, *26*(4), 673-684.

Liao, C., Palvia, P., & Lin, H. N. (2006). The roles of habit and web site quality in e-commerce. *International Journal of Information Management*, *26*(6), 469-483.

Lim, K. H., Sia, C. L., Lee, M. K., & Benbasat, I. (2006). Do I trust you online, and if so, will I buy? An empirical study of two trust-building strategies. Journal of Management Information Systems, 23(2), 233-266.

Lumineau, F. (in press). How contracts influence trust and distrust. *Journal of Management, Forthcoming.*

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709-734.

McEvily, B., Perrone, V., & Zaheer, A. (2003). Trust as an organizing principle. *Organization science*, *14*(1), 91-103.

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., & Chervany, N. L. (2000). What is trust? A conceptual analysis and an interdisciplinary model. AMCIS 2000 Proceedings, 382.

McKnight, D. H., & Chervany, N.L. (2001). What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6*(2), 35-59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *The Journal of Strategic Information Systems*, *11*(3), 297-323.

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.

Naquin, C. E., Kurtzberg, T. R., & Belkin, L. Y. (2010). The finer points of lying online: E-mail versus pen and paper. *Journal of Applied Psychology, 95*(2), 387.

Naquin, C. E., & Paulson, G. D. (2003). Online bargaining and interpersonal trust. *Journal of Applied Psychology, 88*(1), 113-120.

Özpolat, K., & Jank, W. (2015). Getting the most out of third party trust seals: An empirical analysis. *Decision Support Systems*, *73*, 47-56.

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331-338.

Paravastu, N., Gefen, D., & Creason, S. B. (2014). Understanding trust in IT artifacts: An evaluation of the impact of trustworthiness and trust on satisfaction with antiviral software. *ACM SIGMIS Database*, *45*(4), 30-50.

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), 101-134.

Pavlou, P. A., & Chellappa, R. K. (2001). The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions. Working paper *Marshall School of Business, USC, Los Angeles*.

Pavlou, P. A., & Dimoka, A. (2006). The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation. *Information Systems Research*, *17*(4), 392-414

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

Pavlou, P. A., Liang, H., & Xue, Y. (2006). Understanding and mitigating uncertainty in online environments: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105-136.

Peña, J., & Yoo, S. C. (2014). The effects of avatar stereotypes and cognitive load on virtual interpersonal attraction mediation effects of perceived trust and reversed perceptions under cognitive load. *Communication Research*, 1-23.

Perks, H., & Halliday, S. V. (2003). Sources, signs and signalling for fast trust creation in organisational relationships. *European Management Journal*, 21(3), 338-350.

Ratnasingam, P. (2005). Trust in inter-organizational exchanges: A case study in business to business electronic commerce. *Decision Support Systems*, 39(3), 525-544.

Redfern, S., & Naughton, N. (2002). Collaborative virtual environments to support communication and community in internet-based distance education. *Journal of Information Technology Education*, 1(3), 210-220.

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM*, *43*(12), 45-48.

Riedl, R., Mohr, P. N., Kenning, P. H., Davis, F. D., & Heekeren, H. R. (2014). Trusting humans and avatars: a brain imaging study based on evolution theory. *Journal of Management Information Systems*, *30*(4), 83-114.

Riegelsberger, J., & Sasse, M. A. (2002, April). Face it-photos don't make a web site trustworthy. In *CHI'02 Extended Abstracts on Human Factors in Computing Systems* (pp. 742-743). ACM.

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2003). Shiny happy people building trust?: photos on e-commerce websites and consumer trust. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 121-128). ACM.

Robert, L. P., Denis, A. R., & Hung, Y. T. C. (2009). Individual swift trust and knowledge-based trust in face-to-face and virtual team members. *Journal of Management Information Systems*, *26*(2), 241-279.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393-404.

Sabater, J., & Sierra, C. (2005). Review on computational trust and reputation models. *Artificial Intelligence Review*, *24*(1), 33-60.

Savolainen, T. (2014). Trust-building in e-leadership: A case study of leaders' challenges and skills in technology-mediated interaction. *Journal of Global Business Issues*, *8*(2), 45.

Seckler, M., Heinz, S., Forde, S., Tuch, A. N., & Opwis, K. (2015). Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior, 45,* 39-50.

Sillence, E., Briggs, P., Harris, P. R., & Fishwick, L. (2007). How do patients evaluate and make use of online health information?. *Social Science & Medicine*, *64*(9), 1853-1862.

Sitkin, S. B. (1995). On the positive effects of legalization on trust. t. In R. J. Bies, R. J. Lewicki, & B. H. Sheppard (Eds.), *Research on negotiation in organizations*, Vol. 5 (pp. 185-217). Greenwich, CT: JAI Press.

Sitkin, S. B., & Bies, R. J. (1993). Social accounts in conflict situations: Using explanations to manage conflict. *Human Relations*, *46*(3), 349-370.

Sitkin, S. B., & Roth, N. L. (1993). Explaining the limited effectiveness of legalistic “remedies” for trust/distrust. *Organization Science, 4*(3), 367-392.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1016.

Söllner, M., Pavlou, P. A., & Leimeister, J. M. (2013). Understanding Trust in IT Artifacts–A New Conceptual Approach. Paper presented at the annual meeting of the Academy of Management, Florida, USA.

Stewart, K. J. (2003). Trust transfer on the world wide web. *Organization Science*, *14*(1), 5-17.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, (6), 24-31.

Teo, T. S., & Liu, J. (2007). Consumer trust in e-commerce in the United States, Singapore and China. *Omega*, *35*(1), 22-38.

Thatcher, J. B., Carter, M., Li, X., & Rong, G. (2013). A classification and investigation of trustees in B-to-C E-commerce: General vs. specific trust. *Communications of the Association for Information Systems*, *32*(1), 107-134.

Thatcher, J. B., Loughry, M. L., Lim, J., & McKnight, D. H. (2007). Internet anxiety: An empirical study of the effects of personality, beliefs, and social support. *Information & Management*, *44*(4), 353-363.

Tomlinson, E. C., Lewicki, R. J., & Ash, S. R. (2014). Disentangling the moral integrity construct: Values congruence as a moderator of the behavioral integrity–citizenship relationship. *Group & Organization Management*, 39(6), 720-743.

Tuch, A. N., Bargas-Avila, J. A., & Opwis, K. (2010). Symmetry and aesthetics in website design: It’s a man’s business. *Computers in Human Behavior*, *26*(6), 1831-1837.

Walther, J. B. (1995). Relational aspects of computer-mediated communication: Experimental observations over time. *Organization Science*, *6*(2), 186-203.

Wang, W., & Benbasat, I. (2005). Trust in and adoption of online recommendation agents. *Journal of the Association for Information Systems*, *6*(3), 4.

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior, 21*(1), 105-125.

Wilson, J. M., Straus, S. G., & McEvily, B. (2006). All in due time: The development of trust in computer-mediated and face-to-face teams. *Organizational Behavior and Human Decision Processes*, *99*(1), 16-33.

Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, *16*(2), 47-63.