Trust in the Information Systems Discipline

Ayten Öksüz, Nicolai Walter, Bettina Distel, Michael Räckers, and Jörg Becker

Abstract The digitalization of today's world has greatly advanced during the last few years and affects nearly all areas of life. The research discipline Information Systems (IS) views digitalization from multiple perspectives. On the one hand, IS is concerned with the development and functionality of technological artifacts. On the other hand, researchers in this field also investigate questions of how users perceive and actually use technological innovations. This last point brings about the question of how users deal with perceptions of risks that are inevitably connected to the use of technology (e.g., data theft, abuse of personal data). Thereby, trust research found its way into IS research since trust is widely considered to be a key factor in dealing with risk perceptions. Trust relations are commonly described as the relation between two parties: the trustor (who trusts) and the trustee (who is trusted). So far, technology has mainly been viewed as a medium through which trust can be transmitted or developed. With the emergence of quasi humans (e.g., recommendation agents), this ascription becomes more and more difficult and raises the question of whether or not a technology can be trusted. This article gives an overview of perspectives on the relations between users' perceptions of risk, trust through and in technologies, and trust towards technology providers. We furthermore provide insights into the state of the art of trust research in the IS discipline.

Keywords Trust • Risk • Technology • Quasi humans • Digitization • Information Systems

1 Introduction

In the digitized world of today, more and more services are carried out online and people are more strongly connected to technology than ever before (van Eimeren and Frees 2014). While shopping for books on Amazon is an example of early times

A. Öksüz • N. Walter • B. Distel • M. Räckers • J. Becker (✉)
University of Münster - ERCIS, Münster, Germany
e-mail: ayten.oeksuez@ercis.uni-muenster.de; nicolai.walter@ercis.uni-muenster.de; bettina.distel@ercis.uni-muenster.de; michael.raeckers@ercis.uni-muenster.de; joerg.becker@ercis.uni-muenster.de

B. Blöbaum (ed.), *Trust and Communication in a Digitized World*, Progress in IS,
DOI 10.1007/978-3-319-28059-2_12

of the World Wide Web, consumers and businesses currently think about online services such as mobile applications, the Internet of things, and cloud computing (Gartner 2013). Moreover, while computers originate from the domain of business, and it took a while for personal computers to succeed, nowadays many people own a smartphone and, thus, carry a supercomputer in their pocket. The use of technology offers several opportunities, such as mobile apps that enable fast access to online services like traffic information, or cloud computing, which is considered to increase the comfort of file management, flexibility of computing resources, and overall lower costs (Armbrust et al. 2010).

What all these trends have in common is that they include some aspect of information technology (IT). The Information Systems (IS) discipline follows two lines of research on IT (Hevner et al. 2004). On the one hand, the internet is an IT infrastructure accessed via software programs like 'apps' on hardware devices like smartphones. This entails many questions of how information systems and devices should be designed in order to function as intended. This perspective originates from the designers' view of information systems. On the other hand, the users and their behaviors highly influence how technology is used and what services are actually adopted (Benbasat 2010). This brings about the question of how users perceive information systems, for example, as useful and easy to use. While the focus of IS was originally limited to organizations, the discipline has evolved. Current research also deals with trust and IT in the context of e-government, as well as the personal sphere (social media).

However, the presence of IT does not offer only opportunities. On the downside of technology usage, many individuals and organizations have heightened perceptions of risk. When individuals carry out transactions on the internet, (personal) data may be recorded on servers that could be located anywhere. Individuals may, for example, post personal information on Facebook, buy on eBay, or take out an insurance policy on a web portal. Furthermore, the relationship between online providers and their (potential) customers is characterized by information asymmetry and social distance between the parties (Ba and Pavlou 2002; Gefen and Straub 2003; Pavlou et al. 2007). This means that individuals interacting with an online provider often do not exactly know how their personal data is used and processed by the provider (McKnight et al. 2002a). Third parties also pose a threat to individuals and organizations by gaining unauthorized access to sensitive data stored on the servers of a provider (Bélanger et al. 2002). Furthermore, online environments or interactions are considered to be more anonymous and impersonal than offline interactions (Wang and Emurian 2005) and, thus, lack human contact and warmth (Gefen and Straub 2003). Risk perceptions associated with the threats in online environments and the related lack of trust in online providers and e-commerce shops often lead to individuals' and organizations' reluctance to use certain new technologies or online services (Garrison et al. 2012; Hoffman et al. 1999). As a consequence, trust is suggested to be a key factor for the diffusion of innovations and adoption of new technologies or online services (e.g., Gefen et al. 2003). Research on how to improve IT security is fundamental for trust building in the digitized world.

As a first reaction, the development and implementation of new security measures shall contribute to an improved security of online transactions. However, besides the technical safety, dealing with individuals' and organizations' risk perceptions and trust building is also a question of communication (Khan and Malluhi 2010; Öksüz 2014). Trust can be built only when providers adequately communicate the implemented measures to ensure the security of data (Khan and Malluhi 2010; Öksüz 2014).

The omnipresence of technology in our daily lives has raised a high need for trust. While in computer science trust is understood as security in terms of technical safety, IS emphasizes the socio-emotional perspective (Recker 2013). In this sense, the IS discipline considers trust as an individual's perception of another party as being competent, benevolent, and as having integrity (Li et al. 2008; Mayer et al. 1995). As the nature of the IS discipline always involves an IT artifact, not only the IT artifacts themselves are diverse, but so are the relationships between trust and the IT artifacts. Trust research in IS ranges from dealing with the question of trusting another party interacted with in a computer-mediated setting (e.g., collaboration between virtual team members carried out via technology-mediated communication), to the question of trusting the IT artifact itself (McKnight et al. 2011). With regard to trust in IT, one of the most prominent examples is the area of e-commerce. When dealing with online providers, the provider's website is the primary and often sole source of information (Wang and Emurian 2005). Online providers mainly depend on their websites to represent themselves to consumers (Wang and Emurian 2005). As a result, many consumers tend to focus on the website design when assessing its or the online provider's trustworthiness (such as easy navigation and use of the website) (Karimov et al. 2011). This also shows that it is not always clear who the trustee is in a specific online trust relationship: the e-commerce website or the online provider the website represents. In this context, the question of whether or not the website can be trusted at all arises. Furthermore, websites sometimes include some contact opportunities, such as live chats. However, these chats may fully or partly be operated by software scripts, such as chat bots. There are even virtual agents that are software programs embedded into the website with which the user can interact (e.g., Qiu and Benbasat 2009). This leads to the question of whether or not algorithms, software, and technology can be trusted from a socio-emotional perspective.

Thus, the IS discipline distinguishes between three notions of trust: trust in individuals through technology, trust in quasi-humans (such as recommendation agents), and trust in a technology itself (cf. Fig. 1). This discussion paper includes all of these trust issues and presents approaches that try to structure the different streams of trust, as well as insights into studies that show the role and effects of trust in the IS discipline. The remainder of this article is structured as follows. First, we deal with trust when IT or an IT artifact is a mediator among humans or between humans and organizations. Second, we elaborate on the role of quasi-humans, such as virtual agents, for trust building. Third, the technology itself comes into focus and we discuss the role of trust in IT. Finally, we conclude with an outlook on trust research in the Information Systems discipline.

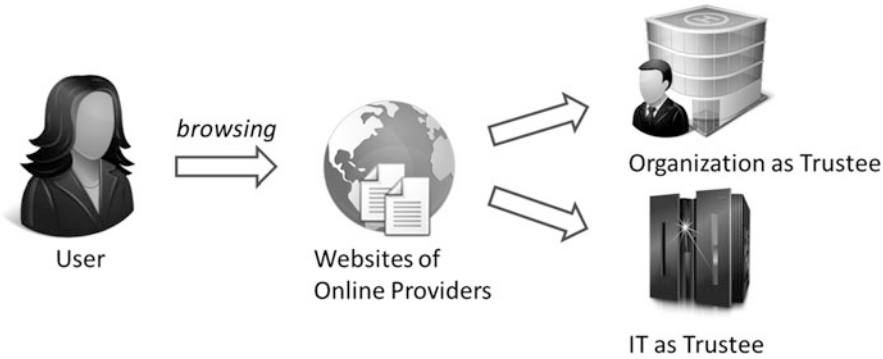

Fig. 1 Different trustees in the digitized world (images are kindly provided for commercial use by www.icons-land.com, www.creativefreedom.co.uk, and www.designcontest.com)

2 Trust in Individuals Through Technology

Trust research in the IS discipline can either focus on trust in the IT artifact itself or on trust in a service provider or another human (Söllner et al. 2012). In the latter case, the IT artifact functions as a mediator between two or more users. Based on an IT-artifact, such as websites, users may interact with individuals (e.g., on social network sites (SNS) or through social media (SM)), an organization (e.g., on e-commerce websites), or an administration. Each of these relationships is characterized by the fact that the website or the social media profile often becomes the sole source of information about the transaction or communication partner (Wakefield et al. 2004; Wang and Emurian 2005). Commonly, researchers in the IS discipline describe communication or interactions through websites or, more generally, communication based on IT as asymmetric (Wang and Benbasat 2007); that is, the user cannot, to a certain degree, predict or control the actions and outcomes of the service provider's behavior (i.e., seller, communication partner, administration, etc.) (Glover and Benbasat 2011). While in interpersonal relationships the communication partner's character traits and trustworthiness as well as potential risks of an interaction can be assessed directly, in a technology-based communication, this comes about only indirectly (Verhagen et al. 2006). As a consequence, since the user has to rely on the veracity of the information given on the website, interactions through websites always include risks for the user, not only in matters of technical security (e.g., risk of privacy breaches), but also referring to the providers' trustworthiness (e.g., Pavlou 2003). When, for example, shopping for a new camera, the customer in a shop can estimate the weight, design, or functionality of the camera directly. He can also ask a vendor for more technical details and advice on alternatives. When shopping for a camera online, the customer cannot try the different functionalities or get advice from the vendor, but has to rely on photographs and written descriptions. He also has to disclose private data to perform the transactions (e.g., bank data, address) and often has to pay in advance. Therefore,

the user has to rely on information given on the website to estimate the provider's trustworthiness. Hence, trust is understood as a necessity to bridge the perceived uncertainties (Verhagen et al. 2006).

The IS discipline adopted this view from business science where trust is mainly understood as one's (the trustor's) ". . .willingness . . . to be vulnerable to the actions of another party [trustee] 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" (Mayer et al. 1995, p. 712). In this view, the trustworthiness of the trustee consists of his or her *ability* (skills, expertise, capability, etc.), *benevolence* (willingness to perform an action on behalf of the trustor without any profit motives), and *integrity* (a common or at least similar set of beliefs and principles) to perform a certain action. These so-called factors of perceived trustworthiness are not bipolar, but rather understood as a continuum with situation-specific degrees of each belief (Mayer et al. 1995). For example, one might think the plumber apprentice is willing to repair a broken water pipe and wants to do his job the best possible way. The client believes him to be benevolent and to have the needed integrity to fulfill the task. Even though the client might also think the apprentice has the needed abilities, he might, in comparison to the apprentice's foreman, believe the latter to be *more* able to fix the water pipe. Accordingly, although both of them might be perceived as being benevolent and having integrity, the client would perhaps put more trust towards the foreman due to his long lasting experience and resulting expertise. Still, the same client would not trust either of them to take care of his or her child, since the client does not know what experiences both have in child care or whether or not they are willing to do the best for the wellbeing of the child.

Trust research in the IS discipline mainly focused on e-commerce for a long time. Since the digitalization of the world proceeds quite fast, more and more parts of daily life are digitized and a lot of services are carried out online (van Eimeren and Frees 2014). Today, the World Wide Web enables more than online shopping: organizations, for example, carry out their business online and collaborate with other organizations in the form of virtual teams or use new technologies like cloud computing, and bank customers can transfer their money via online banking services from home. SNS, like Facebook or Twitter, facilitate interpersonal communication across long distances. In contrast, they not only but mainly relate to the personal sphere. Since SNS also facilitate the self-presentation of organizations and communication between businesses and their potential customers, some features of SM also relate to the business sector. More recently, governments and administrations started to enlarge their online services and some countries, such as Estonia, have, for example, initiated pilot schemes of online voting (e.g., Estonia 2015). In order to structure the different fields of online interactions, we adapt the distinction between personal sphere as well as the public and business sector as known from social and political sciences. Here, the public sphere is understood as an arena where a speaker and an audience come together to communicate (Neidhardt 1994). This public sphere is commonly defined as open and accessible to everyone and forms a contrast to the private sphere (Marschall 1998). Since businesses do not

negotiate public or political issues and are, in contrast to the public sphere, not open to everyone, they are viewed as a separate construct in this paper. The personal sphere, which only comprises private communication and interactions, is also viewed as a separate construct.

Although the described services relate to different spheres, they all have one thing in common: the user of these services has to share private and sensitive information. Aside from security or technology related concerns, foremost the user has to trust the provider, that he or she will not take advantage of this data and will take suitable measures to ensure data security and the protection of privacy. This also entails trust in the assurance of the service's frictionless operation (e.g., Corritore et al. 2003). At the same time, the users' willingness to adopt an online service is highly influenced by the perceived trustworthiness of the communication or transaction partner, meaning that the more trustworthy one is perceived, the more probable an interaction will occur (e.g., Becker et al. 2014). All online service providers therefore need to build trust through their websites (e.g., Karimov et al. 2011); trust towards an IT artifact as a mediator is therefore not only important in the business sector, but also applies to the personal sphere and the public sector. The following section presents examples of each field, business and public sectors and the personal sphere, as well as insights into some studies and research results.

2.1 Business Sector

One of the earliest and well researched services in the IS discipline is e-commerce (e.g., Li et al. 2008; Wang and Benbasat 2008; Wang and Emurian 2005). E-commerce is not an object of scientific interest only because it is widespread, but also because it creates a typical situation of trusting behavior on the internet (e.g., Hoffman et al. 1999). The offered products cannot be assessed physically concerning quality or the price-performance ratio, and (potential) buyers have to rely on the information provided on the online merchants' websites (Verhagen et al. 2006). This entails certain risks since consumers often have to pay in advance, not knowing whether or not the product will be delivered as expected or will be delivered at all (Kim et al. 2008). Despite transaction related concerns, a lot of potential users are concerned with identity theft or abuse of private data (McKnight et al. 2002b). Thus, trust is a core constituent of successful e-commerce (e.g., Wang and Benbasat 2008; Wang and Emurian 2005). Researchers and practitioners are interested in explaining the role of trust in interactions on the internet (e.g., Lowry et al. 2008; Pavlou and Fygenson 2006; Colquitt et al. 2007; Bundesministerium des Inneren 2015).

Mayer et al. (1995) state that, besides perceptions of the trustee's ability, benevolence, and integrity, a trustor's general disposition to trust influences his or her perceptions regarding the trustee's trustworthiness. Additionally, McKnight et al. (2002b) propose the concept of *institution-based trust* what one could call security in terms of technical safety: Users are convinced that "structures like

guarantees, regulations, promises, legal recourse, or other procedures are in place to promote success [. . .and] that the environment [the Internet] is in proper order and success is likely because the situation is normal or favorable" (McKnight et al. 2002b, p. 339). Institution based trust is not necessarily vendor specific. In contrast, the factors of perceived trustworthiness describe "perceptions of specific web vendor attributes" (McKnight et al. 2002b, p. 337), which are communicated through the vendor's website. Based on the Theory of Reasoned Action (TRA), a frequently cited framework for technology adoption, the authors argue that factors of perceived trustworthiness form trusting intentions, meaning the personal intention to interact with the web-vendor (McKnight et al. 2002b). Trust in an online shop will likely lead to the intention to buy from the shop, which in turn will likely lead to an actual purchase.

Although the work of McKnight et al. (2002b) is a good framework to explain how internet-users adopt e-commerce services, the model does not explain what specific elements of a website constitute the factors of perceived trustworthiness. Karimov et al. (2011) developed a classification of trust-inducing elements a website can or should include in order to appear trustworthy. As the website functions as mediator between two unknown parties, it should be designed in a way that creates trust in the supplier, respectively trustworthiness of the supplier (Söllner et al. 2012). Following Karimov et al. (2011), this includes not only design or layout, but also content and information, technical aspects, and usability. Based on the cue-signaling theory the authors develop a classification with three categories relating to each form of trust. The authors conduct a literature analysis to classify antecedents of trust and distinguish three categories of trust-inducing website elements: the *visual design*, including all graphical and structural elements; the *social cue design*, including the availability of social media, human-like features, and assistive interfaces; and the *content design,* which comprises the informativeness of the website, brand alliances, and e-assurances (Karimov et al. 2011). In summary, the willingness of a user to depend on an online-provider and the offered online-service highly relies on the provider's website and its capability to create trust.

In addition to Karmiov et al.'s (2011) model, there are conceptualizations that also take, besides design dimensions, cultural conditions into account (Cyr 2013). In this context, Cyr (2013) shows with a cross-national study of "user perceptions of B2C Web pages" (Cyr 2013, p. 377) that perceptions of the website design are influenced by "overall cultural values" (Cyr 2013, p. 381) and that these design perceptions do influence users' trust. This shows that the development of a trust-inducing website design also depends on the context of the business as well as on cultural conditions. Although the classification of Karimov et al. (2011) is not applied by Cyr (2013), the study of Cyr includes similar perceptions of visual and content design and leads to the assumption that a careful website design can create trust. Cyr (2013) states that, especially in countries with lower uncertainty avoidance, the presentation, accuracy, and accessibility of information, as well as an appealing visual design and high usability, can create higher levels of trust in an

e-vendor (Cyr 2013). Hence, a well-designed trust-inducing website is a core factor to successful e-commerce.

2.2 *Personal Sphere*

In the past few years another web-based technology has attracted much attention: SNS and SM like Facebook or Twitter. Since the usage of these services has rapidly increased over the past few years and still grows, scholars have started to investigate why users trust services like Facebook, and not only transmit but also disclose private data (e.g., Bryce and Fraser 2014; Taddei and Contena 2013). The use of SNS or SM forms a situation to users that is similar to e-commerce, although the risks involved are different. When using a social network website, users disclose very personal information not only through their own profiles but also through interpersonal communication with other users (Canfora and Visaggio 2012). In contrast to e-commerce, users do not necessarily risk a material loss, like paying for a product, which is not delivered. SM users rather risk the theft or abuse of their private data (Sherchan et al. 2013). In contrast to the e-commerce context, trust in the provider, its website, and the underlying technology, as well as trust in other users might be relevant (Lankton and McKnight 2011). Lankton and McKnight (2011) differentiate between interpersonal trust and technological trust (trust in the IT-artifact itself). Although this distinction can be made and the two types exist, the authors state that SNS "represent a technology in which the distinction between human and technology characteristics is less clear" (Lankton and McKnight 2011, p. 34). Their survey consequently shows "that [Facebook] users blend human demonstrations of trust with technology demonstrations of trust. This could be because users think of the Facebook website both as a technology and a quasi-person, even though it is a technical artifact" (Lankton and McKnight 2011, p. 47).

Besides the fact that users of SNS view these services as technology as well as an organization led by humans, other difficulties arise in studies of trust in social networks. While the usage of guarantees or (official) seals (e.g., http://www.trustedshops.de/) is steadily disseminating in the field of e-commerce or e-businesses in particular, most SNS cannot control the actions of their users. A user may trust Facebook to not abuse personal or private data because Facebook, as a company, has general terms and conditions to which it is legally bound. But users should not necessarily trust (unknown) other users to be benevolent or have integrity since other companies or users can create fake profiles to contact other users to come into possession of personal data (Canfora and Visaggio 2012). Therefore, a user may trust the website (the technology as well as the provider), but at the same time distrust other users. Currently, in addition to questions of interpersonal vs. technological trust (e.g., Lankton and McKnight 2011), mechanisms to manage *trust in other users* in the context of SM are under research (e.g., Canfora and Visaggio 2012).

The steady dissemination of SM also leads to a growing embedding of SM applications into other websites. Karimov et al. (2011) states that customer reviews belong to the group of social media that can enhance the feeling of humaneness on a website and thus influence users' trust. For instance, a study conducted by Kumar and Benbasat (2006) shows that recommendations and consumer reviews embedded in online shops can influence perceptions of human warmth, which in turn can be seen as a strong predictor of trust (Walter et al. 2013). SM (components) like consumer reviews and user-to-user support platforms are considered to lead to more trust, since they are seen to raise feelings of human contact and sociability and consequently partly compensate for the lack of closeness as known from face-to-face interactions (Kumar and Benbasat 2006; Ortbach et al. 2014).

2.3 Public Sector

The public sector (administrations and governments) has also made use of IT-artifacts, mainly websites, to deliver services to citizens. In the beginning, authorities mainly used the internet as a mere digital brochure to inform about opening hours or contact persons. Today, most administrations sophisticatedly use web services and offer numerous services online (e.g., Horst et al. 2007; Hofmann et al. 2012). Besides a lacking supply of online-services in some countries or districts, currently, the adoption behavior of citizens is occupying the scientific interest of researchers around the globe (e.g., Bélanger and Carter 2008; Akkaya et al. 2011; Belanche et al. 2012; Hofmann et al. 2012; Hofmann and Heierhoff 2012). There is broad agreement that, similar to e-commerce adoption, trust and risk perceptions are of great importance to the success or failure of e-government services (Akkaya et al. 2011). Therefore, theoretical frameworks popular in the IS discipline, like the Technology Acceptance Model (TAM) (e.g., Belanche et al. 2012) or the TRA (e.g., Bélanger and Carter 2008), are also used in the research of e-government service adoption (e.g., Hofmann et al. 2012).

The usage of e-government services comprises similar risks to those in e-commerce services: citizens face security breaches and the potential abuse of private and personal data as users do not have control over how public administrations use transmitted data (Akkaya et al. 2011). Furthermore, as with any other service, administrations are not immune to data theft by hackers. Here, again, users' trust can either relate to the technology as the trustee or the mediator of trust. In the latter case, the trustees are service providing administrations. Bélanger and Carter (2008) distinguish these forms of trust into *trust of the internet* (IT) and *trust of the government* (organization). Besides concerns about the handling of private data (which relates to trust of the government), Akkaya et al. (2011) show that trust in respective public authorities is a key differentiator in the acceptance and adoption of e-government services. This emphasizes the need of administrations to build trust through their websites. As Bélanger and Carter (2008) state, governments should "take advantage of trust-building mechanisms used by e-commerce vendors,

such as posting security and privacy seals, to encourage adoption of e-government services" (Bélanger and Carter 2008, p. 172). Studies like this show that similar mechanisms apply to e-government adoption as to e-commerce, but that there are also great differences. While e-vendors are either completely unknown or can build on an ongoing trust relationship, governments face the problem that they are already known to the potential users and only offer a new form of their services. They have to deal with their already existing reputation and perceptions among the population. Hence, Horsburgh et al. (2011) state that "it is possible that those [citizens] with low trust in politicians may mistrust government information, including that provided via e-government channels." (Horsburgh et al. 2011, p. 233). As Beldad et al. (2010) further point out in their literature review, the offline presence of a provider may influence perceptions of this provider's online presence. This could be especially true for e-government services since most citizens presumably hold strong beliefs about the government, which in turn influence perceptions about its benevolence, integrity, and ability to provide helpful and secure online services.

3 Trust in Quasi-Humans

Besides visual and content cue design, social cue design is also important when designing websites to be more trustworthy (Karimov et al. 2011). This dimension is important as the digitized world is usually characterized by a high social distance between interacting parties such as buyers and sellers or consumers and online service providers (Gefen and Straub 2003; Pavlou 2003). There are a multitude of options for how social cues can be embedded into websites; for example, human images may be used (Cyr et al. 2009). However, besides non-interactive social cues, human or non-human interaction website features also exist. Regarding human features, these may, for example, be contact forms that forward website visitor messages to user support employees. More sophisticated are live-chats embedded into a website. While the common notion may be that these applications are operated by humans, in some live-chats users may actually be paired with chat-bots; i.e., software programs that are trained to adequately respond to user input. Moreover, while in some cases, at first, a chat-bot deals with user requests, this chat-bot may switch roles with a human as soon as conversations take courses that a chat-bot cannot handle. In addition to a shared service provision of humans and computers, there are also software applications that complement human support staff to an even greater extent. These so-called quasi-humans are virtual agents referred to as "animated embodiments [i.e., visual, often human-looking representations] that respond to users through verbal and nonverbal communication" (Chattaraman et al. 2012, p. 2055). Many companies make use of them on their websites. In terms of trust, a kind of virtual agent who is not only capable of holding conversations but can also give recommendations about products and services is especially relevant (Hess et al. 2009). As a consequence, these agents, so-called

social recommendation agents, are the object of many studies of trust in the field of Information Systems (Walter 2014). While they have primarily been tested in e-commerce and real estate (Qiu and Benbasat 2009; Richards and Bransky 2014), current studies also validate their influence in the context of cloud computing services (Walter et al. 2014).

Academic research in the Information Systems discipline has dealt with the question of how to make these agents more trustworthy (e.g., Hess et al. 2009; Qiu and Benbasat 2005, 2009). There are different approaches that lead to this goal. The basic notion is that the design of social recommendation agents can be influenced. The design of a social recommendation agent refers to its appearance; i.e., the type of embodiment, output signals like voice or text-to-speech, and even an agent's personality, use of gestures, and options to interact with users (Walter 2014). One study shows, for example, that an extroverted social recommendation agent that is designed with respect to more outgoing statements, a voice with faster pace and volume, and more extensive use of gestures leads to more trust than an introverted agent (Hess et al. 2009). Other studies suggest that the facial expressions of an agent are important in raising users' trust (Lisetti et al. 2013).

In the digitized world, relationships between interacting parties are not only characterized by a higher social distance than face-to-face interactions, but also by information asymmetry (e.g., Xiao and Benbasat 2007). Sellers, for example, usually know more about their delivery reliability or product quality. When it comes to social recommendation agents, the issue of information asymmetry also exists (Xiao and Benbasat 2007). Does a social recommendation agent really provide the best recommendation in the users' interest (i.e., regarding the users' (previously stated) preferences), or does the agent perhaps optimize the recommendation with respect to the online shop's profit margin? Why does a specific provider embed a social recommendation agent anyway? The main reason may be because the provider has learned this would instill more trust because there is a real interest for the users' needs, i.e., the provider really wants users to be better educated about product and service information. The human interface of virtual agents may obscure the fundament that is 'behind' those agents, namely algorithms. Thus, it does not matter whether or not there is a simple chat-bot without an embodiment or a social recommendation agent with sophisticated 3D animation. Both systems are solely based on algorithms. The additional humanness may not, from a rational and pragmatic standpoint, count as more trustworthy as it may be open to influence from providers like most other information systems. This brings us to the question of how far information systems and the underlying operations (i.e., algorithms) can be trusted at all.

4 Trust in Technology

The advent of new technologies and the rapid pace of technological change in the digital world present new challenges with regard to trust. With the increasing use of digital services and the resulting increasing amounts of data, data security and privacy become more and more important social issues. The widespread concerns about data security and privacy and the lack of trust leads to the fact that many individuals and organizations make only limited use of some of these new technologies or do not use them at all (Deutsche Telekom/T-Systems 2014). The role of trust and risk perceptions in the acceptance and adoption of technologies has been the object of scientific research in the IS discipline for quite some time. For example, recent research has shown that beyond the perceived ease of use (PEOU) and perceived usefulness (PU), the intention to use a new IT highly depends on trust (Gefen et al. 2003). The fact that trust is an important factor influencing the acceptance and usage intention of (new) technologies led to the extension of the technology acceptance model (TAM) by the factor trust (Gefen et al. 2003). Consequently, trust can be seen as a key factor influencing the acceptance and use of emerging technologies, especially whenever risk perceptions (such as concerns about data security and privacy) are in place.

One of the most discussed technology trends in the last few years is cloud computing. The use of cloud computing promises considerable advantages, such as cost savings, but also poses several data protection risks for potential users (Armbrust et al. 2010; Kerschbaum 2011; Takabi et al. 2010; Zissis and Lekkas 2012). Third parties, for example, could gain unauthorized access to sensitive user data stored in the cloud (Kerschbaum 2011). Furthermore, users of cloud services are often not able to completely control the data handling practices of cloud computing providers (Takabi et al. 2010). They do not always know whether their data is handled in a lawful manner (Takabi et al. 2010). Since the emergence of cloud computing, issues relating to data privacy and the security of personal and sensitive data became even more the focus of public attention. Consequently, cloud computing providers face the challenge of gaining the trust of potential users with the objective to motivate them to use their services (Öksüz 2014; Walter et al. 2014). From the perspective of computer science, the trust problem can be solved by developing new security technologies and solutions (e.g., new encryption methods to prevent unauthorized access to sensitive data) in order to make the cloud safer and more secure (Kerschbaum 2011). In this sense, computer scientists understand trust as security and aim to enable cloud computing providers to protect customer data more securely. Research in this area might have significantly contributed to the fact that improvements in cloud security have been achieved over time and that data security will keep getting better (Allouche 2014). However, the mere development and implementation of new security measures is not enough to gain potential users' trust (Öksüz 2014). This is because trust is based on perceptions regarding a cloud provider's ability and willingness to protect (potential) users' data and ensure privacy (Chellappa and Pavlou 2002). This in turn depends

on (potential) users' perceived security level (Chellappa and Pavlou 2002). The perceived security level determines the subjective probability with which users believe that their data will be protected against loss, abuse, and unauthorized access or hacker attacks at any time (Chellappa and Pavlou 2002). Potential users' perceived security level might differ from the actual security offered by the cloud provider (Chellappa and Pavlou 2002). It could be, for example, that users do not perceive a high security level even though a provider is able and willing to protect users' (personal) data by using the latest security and privacy measures (Öksüz 2014). One of the reasons for this is often a lack of communication or transparency (Khan and Malluhi 2010; Öksüz 2014). Communication is a key element in the formation of perceptions (Rogers 2003). Cloud providers have to provide information on their data handling practices and their implemented security measures in order to gain users' trust (Khan and Malluhi 2010; Öksüz 2014). They have to adequately communicate which security and privacy measures they have implemented in order to protect users' data and to ensure privacy (Khan and Malluhi 2010; Öksüz 2014). Thus, for trust building it is important that cloud providers first implement appropriate security measures and take responsibility for their clients' data, and second, adequately communicate the implemented security measures and data handling practices.

Beyond that, potential users also have to trust in the mechanisms (security and privacy measures) implemented by the provider to protect user data (Zissis and Lekkas 2012). In this context, some researchers state that trust in IT or trust in the technology also plays an important role in the acceptance and adoption of new technologies (Li et al. 2008; McKnight et al. 2011). However, very few research directly deals with trust in certain technology (McKnight et al. 2011). To some extent, research on trust in social recommendation agents focuses on trust in an IT artifact (McKnight et al. 2011; Orlikowski and Iacono 2001). This is because (social) recommendation agents are automated online assistants helping users to decide among various product alternatives (Wang and Benbasat 2007). In this sense, social recommendation agents are IT artifacts (McKnight et al. 2011). However, social recommendation agents act like humans and interact with users in human-like ways (Hess et al. 2009). As a result, studies on trust in social recommendation agents have measured trust in the social recommendation agent by using trust-in-people scales (McKnight et al. 2011). Thus, trust in social recommendation agents has not actually been studied in terms of trust in IT, but rather in terms of trust in humans (McKnight et al. 2011).

McKnight et al. (2011) have developed a conceptual definition and operationalization of trust in technology. In doing so, they explain how trust in technology differs from trust in people. Similar to trust in people, users' assessments of attributes reflect their beliefs about a technology's ability to deliver on the promise of its objective characteristics (McKnight et al. 2011). The researchers suggest that, with respect to the characteristics or attributes of a technology, the counterpart to competence is functionality, to benevolence is helpfulness, and to integrity is reliability (McKnight et al. 2011). *Functionality* refers to the question of whether or not the technology functions as promised by providing features that are required

to fulfill a task (McKnight 2005). *Helpfulness* represents "users' beliefs that the technology provides adequate, effective, and responsive help" (McKnight et al. 2011, p. 5). *Reliability* means that the technology or IT artifact operates continually (i.e., with little or no downtime) or responds predictably to inputs (e.g., printing on command) (McKnight et al. 2011). However, from other researchers' point of view "people trust people, not technology" (Friedman et al. 2000, p. 36). They assume that trust can only exist if the trustee has his or her own will and a freedom of choice and thus, can consciously decide between right and wrong at his or her own discretion (Friedman et al. 2000). Since technology has no moral principles, users perceive no caring emotions when interacting with technologies (McKnight et al. 2011; Friedman et al. 2000). These two contrary views show that there is no broad consensus on "trust in IT" yet. Nevertheless, for trust building in providers of IT-based services—where data security and privacy is of high importance—it is important that potential users believe in the functionality of the implemented security and privacy measures.

5 Conclusion and Outlook

Trust in information systems and IT offers two sides of a coin. Looking from a more computer science driven perspective, it is a question of security—and trust in IT. Lots of research was and still is invested in the question of how to make information systems and their underlying technology more secure in terms of privacy, data protection, and further issues. In fact, this is comparable to the rabbit and the hedgehog phenomenon. Once the 'rabbits' developed a new, secure algorithm or data protection concept, the 'hedgehogs' are already there and have found a new way to bypass the protection. In the end, there is no absolute security. Therefore, we need a second concept of trust. We have to believe in the technology and, even more, in the providers of technology, that they provide us with the best possible security; we also have to believe in their honesty about boundaries of security and what we additionally have to do or consider when using their technology. A good example of this is the new aspect of trustworthiness Google implemented in their search engine. The 'Knowledge Vault' database consists of assured facts, which are found first when using Google as a search engine. Even if other aspects (or 'wrong facts') are searched more often, if they are not accepted as 'true' they will not occur in the upper search results (cf. e.g., Hodson 2014).

We face an era of digitalization. In fact, we are transforming into a world permeated by IT and will be digitized. In this article, we argue that IT is becoming normal, not only in the business sector but also in the personal sphere. Our complete lives, in every aspect, are depending more and more on digital goods and digital support.

Our society is changing completely. Amazon, for example, is working on a new way to deliver their goods to customers, faster than before: Amazon Prime Air will be a service that delivers customer orders with drones—minutes after the receiving

the order (Amazon 2015). With this, technology is becoming more and more complex and we will more and more not understand aspects of security. Therefore, trust in IT, trust in quasi-humans, and trust in individuals, but being contacted through IT, becomes increasingly important.

For future research on trust and IT and in its facets and characteristics, this implies that the discussion of trust and trustworthiness of IT will become more and more important in the coming years. We have to trust that the information we have is correct and trustworthy without having the possibility to prove this on our own. Research in disciplines such as Psychology, Communication Science, and IS—together—have to investigate this phenomenon and the impact on our society and personal lives. Not only does trust in IT have influence on our personal decisions of usage or non-usage of IT, which is a single and, more or less, private decision (Ortbach et al. 2015), but it also has influence on our business decisions and thus on the growth of our economy. Information technology has become the undisputable engine and key success factor of our economic growth. Companies and sectors dealing with these aspects of trust will be more effective in the position to use this key factor for their success.

References

Akkaya, C., Obermeier, M., Wolf, P., & Krcmar, H. (2011). Components of trust influencing eGovernment adoption in Germany. In M. Janssen, H. J. Scholl, M. A. Wimmer, & Y.-H. Tan (Eds.), *Electronic government. 10th IFIP WG 8.5 International Conference, EGOV 2011 Delft, The Netherlands, August/September 2011. Proceedings* (pp. 88–98). Heidelberg: Springer.

Allouche, G. (2014). The future of cloud computing. *CMS Report*. http://cmsreport.com/articles/the-future-of-cloud-computing-8210. Accessed 6 April 2015.

Amazon. (2015). *Amazon Prime Air*. http://www.amazon.com/b?node=8037720011. Accessed 9 April 2015.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., et al. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243–268.

Becker, J., Heddier, M., Öksüz, A., & Knackstedt, R. (2014). The effect of providing visualizations in privacy policies on trust in data privacy and security. In *47th Hawaii International Conference on System Sciences (HICSS)* (pp. 3224–3233).

Belanche, D., Casaló, L. V., & Flavián, C. (2012). Integrating trust and personal values into the technology acceptance model: The case of e-government services adoption. *Cuadernos de Economía y Dirección de la Empresa, 15*(4), 192–204. doi:10.1016/j.cede.2012.04.004.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems, 17*, 165–176. doi:10.1016/j.jsis.2007.12.002.

Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3), 245–270.

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.

Benbasat, I. (2010). HCI research: Future challenges and directions. *AIS Transactions on Human-Computer Interaction, 2*(2), 16–21.

Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. *Computers in Human Behavior, 30*, 299–306.

Bundesministerium des Inneren. (2015). *Digital Trust is a location factor of fundamental importance*. http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2015/02/security-congress-rogall.html. Accessed 6 April 2015.

Canfora, G., & Visaggio, C. a. (2012). Managing trust in social networks. *Information Security Journal: A Global Perspective, 21*(4), 206–215. doi:10.1080/19393555.2012.660677.

Chattaraman, V., Kwon, W.-S., & Gilbert, J. E. (2012). Virtual agents in retail web sites: Benefits of simulated social interaction for older users. *Computers in Human Behavior, 28*(6), 2055–2066. doi:10.1016/j.chb.2012.06.009.

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

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *The Journal of Applied Psychology, 92*(4), 909–927.

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. (2013). Website design, trust and culture: An eight country investigation. *Electronic Commerce Research and Applications, 12*(6), 373–385.

Cyr, D., Head, M., Larios, H., & Pan, B. (2009). Exploring human images in website design: A multi-method approach. *MIS Quarterly, 33*(3), 539–566.

Deutsche Telekom/T-Systems. (2014). *Sicherheitsreport 2014: Ergebnisse einer repräsentativen Bevölkerungsumfrage*. https://www.telekom.com/static/-/244706/5/140801-sicherheitsreport2014-s. Accessed 6 April 2015.

Estonia. (2015). *i-Voting*. https://e-estonia.com/component/i-voting/. Accessed 6 April 2015.

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

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success factors for deploying cloud computing. *Communications of the ACM, 55*(9), 62–68.

Gartner. (2013). Gartner identifies the top 10 strategic technology trends for 2014. *Press release*. http://www.gartner.com/newsroom/id/2603623. Accessed 6 April 2015.

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., & Straub, D. W. (2003). Managing user trust in B2C e-services. *e-Service, 2*(2), 7–24.

Glover, S., & Benbasat, I. (2011). A comprehensive model of perceived risk of e-commerce transactions. *International Journal of Electronic Commerce, 15*(2), 47–78. doi:10.2753/JEC1086-4415150202.

Hess, T. J., Fuller, M., & Campbell, D. (2009). Designing interfaces with social presence: Using vividness and extraversion to create social recommendation agents. *Journal of the Association for Information Systems, 10*(12), 889–919.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.

Hodson, H. (2014). Google's fact-checking bots build vast knowledge bank. *NewScientist*. http://www.newscientist.com/article/mg22329832.700-googles-factchecking-bots-build-vast-knowledge-bank.html#.VSVJGuG2KHR. Accessed 9 April 2015.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80–85.

Hofmann, S., & Heierhoff, L. (2012). Adoption of municipal e-Government services – A communication problem? *18th Americas Conference on Information Systems (AMCIS 2012)* (pp. 1–10).

Hofmann, S., Räckers, M., & Becker, J. (2012). Identifying factors of e-Government acceptance - A literature review. *Thirty Third International Conference on Information Systems, Orlando* (pp. 1–19).

Horsburgh, S., Goldfinch, S., & Gauld, R. (2011). Is public trust in government associated with trust in e-Government? *Social Science Computer Review, 29*(2), 232–241. doi:10.1177/0894439310368130.

Horst, M., Kuttschreuter, M., & Gutteling, J. M. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Computers in Human Behavior, 23*, 1838–1852. doi:10.1016/j.chb.2005.11.003.

Karimov, F. P., Brengman, M., & Van Hove, L. (2011). The effect of website design dimensions on initial trust: A synthesis of the empirical literature. *Journal of Electronic Commerce Research, 12*(4), 272–301.

Kerschbaum, F. (2011). Secure and sustainable benchmarking in clouds. *Business & Information Systems Engineering, 3*(3), 135–143.

Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT Professional, 12*(5), 20–26.

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*, 544–564.

Kumar, N., & Benbasat, I. (2006). The influence of recommendations and consumer reviews on evaluations of websites. *Information Systems Research, 17*(4), 425–439. doi:10.1287/isre.1060.0107.

Lankton, N. K., & McKnight, D. H. (2011). What does it mean to trust facebook? Examining technology and interpersonal beliefs. *ACM SIGMIS Database, 42*(2), 32–54. doi:10.1145/1989098.1989101.

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. *The Journal of Strategic Information Systems, 17*(1), 39–71.

Lisetti, C., Amini, R., Yasavur, U., & Rishe, N. (2013). I can help you change! An empathic virtual agent delivers behavior change health interventions. *ACM Transactions on Management Information Systems, 4*(4), 1–28. doi:10.1145/2544103.

Lowry, P. B., Vance, A., Mood, G., Beckman, B., & Read, A. (2008). Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites. *Journal of Management Information Systems, 24*(4), 199–224.

Marschall, S. (1998). Netzöffentlichkeit - eine demokratische Alternative? In W. Gellner & F. von Korff (Eds.), *Demokratie und Internet* (pp. 43–54). Baden-Baden: Nomos Verlag.

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

McKnight, D. H. (2005). Trust in information technology. In G. Davis (Ed.), *The Blackwell encyclopedia of management* (Management Information Systems, Vol. 7, pp. 329–331). Oxford: Blackwell.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems, 2*(2), 1–15.

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

Neidhardt, F. (1994). *Öffentlichkeit, öffentliche Meinung, soziale Bewegungen. Kölner Zeitschrift für Soziologie und Sozialpsychologie*. Opladen: Westdeutscher Verlag.

Öksüz, A. (2014). Turning dark into white clouds – A framework on trust building in cloud providers via websites. In *Proceedings of the 20th Americas Conference on Information Systems (AMCIS 2014)*, Savannah, Georgia.

Orlikowski, W. J., & Iacono, C. (2001). Desperately seeking the "IT" in IT research: A call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121–134.

Ortbach, K., Gaß, O., Köffer, S., Schacht, S., Walter, N., Maedche, A., et al. (2014). Design principles for a social question and answers site: Enabling user-to-user support in organizations. In *Proceedings of the Advancing the Impact of Design Science: Moving from Theory to Practice* (Lecture Notes in Computer Science, Vol. 8463, pp. 54–68). doi:10.1007/978-3-319-06701-8_4.

Ortbach, K., Walter, N., & Öksüz, A. (2015). Are you ready to lose control? A theory on the role of trust and risk perception on bring-your-own-device policy and information system service quality. In *Proceedings of the 23rd European Conference on Information Systems (ECIS 2015)*.

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., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behaviour. *MIS Quarterly, 30*(1), 115–143.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105–136.

Qiu, L., & Benbasat, I. (2005). Online consumer trust and live help interfaces: The effects of text-to-speech voice and three-dimensional avatars. *International Journal of Human-Computer Interaction, 19*(1), 75–94.

Qiu, L., & Benbasat, I. (2009). Evaluating anthropomorphic product recommendation agents: A social relationship perspective to designing information systems. *Journal of Management Information Systems, 25*(4), 145–182.

Recker, J. (2013). *Scientific research in information systems: A beginner's guide*. Heidelberg: Springer.

Richards, D., & Bransky, K. (2014). ForgetMeNot: What and how users expect intelligent virtual agents to recall and forget personal conversational content. *International Journal of Human-Computer Studies, 72*(5), 460–476.

Rogers, E. M. (2003). *Diffusion of innovations*. New York: Free Press.

Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys, 45*(4), 1–33.

Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., & Leimeister, J.M. (2012). Understanding the formation of trust in IT artifacts. In *Thirty Third International Conference on Information Systems* (pp. 1–18), Orlando.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821–826.

Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy, 8*(6), 24–31.

van Eimeren, B., & Frees, B. (2014). Ergebnisse der ARD/ZDF-Onlinestudie 2014: 79 Prozent der Deutschen online – Zuwachs bei mobiler Internetnutzung und Bewegtbild. *Media Perspektiven, 7–8*, 378–396.

Verhagen, T., Meents, S., & Tan, Y.-H. (2006). Perceived risk and trust associated with purchasing at electronic marketplaces. *European Journal of Information Systems, 15*(6), 542–555.

Wakefield, R. L., Stocks, M. H., & Wilder, W. M. (2004). The role of web site characteristics in initial trust formation. *Journal of Computer Information Systems, 45*(1), 94–103.

Walter, N. (2014). "Do you trust me?" – A structured evaluation of trust and social recommendation agents. In *SIGHCI 2014 Proceedings*.

Walter, N., Öksüz, A., Walterbusch, M., Teuteberg, F., & Becker, J. (2014). "May I help you?" Increasing trust in cloud computing providers through social presence and the reduction of information overload. In *Proceedings of the 35th International Conference on Information Systems (ICIS 2014)*.

Walter, N., Ortbach, K., Niehaves, B., & Becker, J. (2013). Trust needs touch: understanding the building of trust through social presence. In *Proceedings of the 19th Americas Conference on Information Systems (AMCIS 2013)*. Chicago, IL.

Wang, W., & Benbasat, I. (2007). Recommendation agents for electronic commerce: Effects of explanation facilities on trusting beliefs. *Journal of Management Information Systems, 23*(4), 217–246.

Wang, W., & Benbasat, I. (2008). Attributions of trust in decision support technologies: A study of recommendation agents for e-commerce. *Journal of Management Information Systems, 24*(4), 249–273.

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

Xiao, B., & Benbasat, I. (2007). E-commerce product recommendation agents: Use, characteristics, and impact. *MIS Quarterly, 31*(1), 137–209.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592.