Perspectives on Information Technology Artefacts in Trust-Related Interactions

Holger Koelmann(✉)

Department of Information Systems, University of Muenster,
48149 Muenster, Germany
holger.koelmann@ercis.uni-muenster.de

Abstract. Current research often tries to measure trust in technology or argues about the possibility or plausibility of trust in technology, while neglecting other influences Information Technology artefacts (IT) might have on situations involving trust. To broaden the outlook on this area, this article focuses on perspectives that can be taken in terms of the roles IT might play in interactions that involve trust. The results of this theoretical approach provide a role framework for IT in trust-related interactions distinguishing the role of IT between a) a simple interaction enabler between two other entities, b) a mechanism for mitigating risk in an interaction between two other entities, c) a tool used in an interaction, and d) a trustee in an interaction. In addition, assumptions on the differences these roles might have on the perception of the users, i.e. reliability, control, and trust, are given for each role. Giving future research and practitioners the possibility to use the roles of the framework as lenses for further work in the area.

Keywords: Trust · Human Computer Interaction · Information Technology Artefacts · Theory · Framework

1 The Trust and IT Controversy

A recent article about seven *Grand Challenges* in Human Computer Interaction (HCI)[25], identifies trust issues as an important factor in three of the uncovered challenges, i.e. *"human-technology symbiosis"*, *"ethics, privacy, and security"*, as well as *"well-being, health, and eudaimonia"*. A deeper look into the interplay of trust and technology seems therefore necessary to further develop the field of HCI.

The role of Information Technology artefacts (IT) in trust-related interactions between entities is a disputed topic in academia, where most literature focuses on examining IT as the trustee, the object or party into which is trusted [11], of an interaction. These studies have tried to measure trust in technology with specifically developed measures in recent years [13,26]. Besides this application of measures, a long ongoing debate exists, if it is reasonable or even possible to consider the perception of trust in human-made, non-living objects, such as IT. On the one hand, Friedman et al. have once stated *"people trust people, not*

A. Moallem (Ed.): HCII 2020, LNCS 12210, pp. 445–457, 2020.
https://doi.org/10.1007/978-3-030-50309-3_29

technology" [6], which is backed by Solomon and Flores [24], thereby arguing that what we perceive when interacting with IT is only technical reliability and not trust. On the other hand though, Computers are Social Actors (CASA) [15] and Social Response Theory (SRT) [14] show people applying social norms to technology in experiments. The interplay between IT and trust thus remains disputed, which often resulted in an undifferentiated view as rather a question of faith to the general possibility of trusting IT, fading out other potential influences IT might have on trust-related interactions, and raising the question, if IT's only purpose in these interactions is the role of a potential trustee.

This article therefore aims to discuss the different roles that IT can take in interactions involving trust in a more differentiated way. Instead of a general understanding about trusting IT as either always possible or not, a set of different roles these artefacts can take in interactions with humans, depending on the specific context of the situation, is proposed. This includes additional relations between IT and trust, besides specifying IT as the object of trust. It should also provide scholars and practitioners with a better understanding on how trust and IT can be linked and influence each other. Consequently, the research questions of this work are:

RQ1: *What are the roles that IT artefacts can take in trust-related interactions?*

RQ2: *What might be the effects of these roles on the perception of the user?*

Due to the abstract nature of the above stated research questions, a theoretical *approach* is used in this article to propose a novel framework, which analyzes and describes, according to the classification of theory in the information systems discipline by Gergor [8], the roles of IT in trust-related interactions and their effects on the user's perception. In this case, relying on social sciences and psychology for an understanding of trust, which is then applied to a generalized interaction model involving IT, providing a more comprehensive perspective on the problem at hand.

Resulting from this approach, the rest of the article is *structured* as follows. In Sect. 2, the relevant fundamentals of trust are discussed. Then, a general interaction model for interactions that are related to trust and IT is deduced in Sect. 3. Based upon this, a framework showing perspectives, roles, and resulting effects on user's perception for IT in trust-related interactions is presented in Sect. 4, followed by a discussion of the work's limitations and implications for research and practice in Sect. 5. In the end, a conclusion of this work is provided in Sect. 6.

2 Trust

Trust has been researched for many decades with different definitions and conceptualizations for its application fields, such as psychology, sociology, economics, and computer science [1]. In this section, a definition and conceptualization of interpersonal trust is given in 2.1, with risk, as an important contextual factor, discussed in 2.2, and trust in technology, as a specific form of trust involving IT, introduced in 2.3.

2.1 Trust as an Interpersonal Concept

For the purpose of this article, trust is defined according to Mayer, Davis, and Schoorman as

> *"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"* [11].

Important elements from this definition are the willingness to make oneself vulnerable, the expected action of another party, the importance of that action to the first party, and the incapability to monitor or control the situation [11]. This definition is widely used and integrates elements of many other often used definitions, such as the one from Rousseau, Sitkin, Burt, and Camerer, who set out to create an interdisciplinary definition, which states that *"[t]rust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another"* [18]. One benefit of using the interpersonal trust definition by Mayer et al. is that they also conceptualized a model for measuring and further breaking down trust and its surrounding factors (see Fig. 1)[11].

The model describes the relationships between the relevant constructs for trust, which are [11]:

- an entity who is trusting, the trustor, with its general propensity to trust others,
- an entity in whom is trusted, the trustee, with its trustworthiness, based upon different antecedents,
- perceived risk in a situational context, and
- a resulting behaviour leading to an outcome, which then effects the trustworthiness of the trustee.

It should be noted, that there is no clear finite set of properties that influence a trustee's perceived trustworthiness. Mayer et al. have identified ability, benevolence, and integrity to be crucial antecedents for interpersonal trust [11]. Other studies though have identified additional potentially important antecedents, influencing the perceived trustworthiness, often depending on the properties of the selected trustee [10].

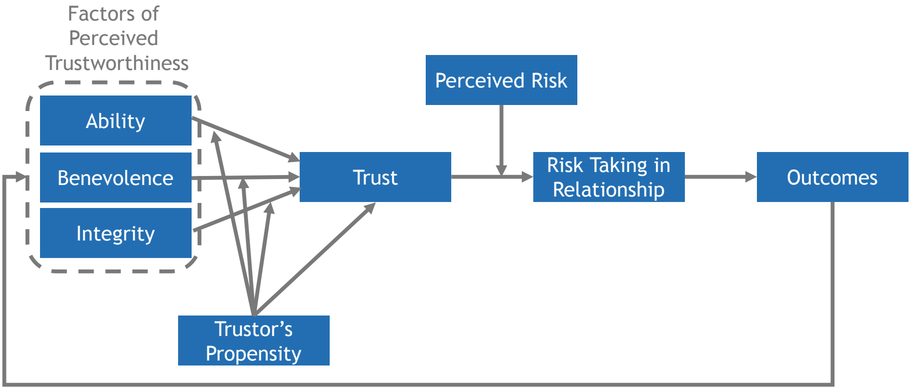

Fig. 1. Interpersonal trust model according to Mayer, Davis, and Schoorman [11]

2.2 Risk as a Contextual Factor

Besides the properties of trustor and trustee, the situational context is also highly relevant for trust to result in behaviour, a so-called trusting action [4,11]. One key contextual factor of trust is perceived risk, which is directly linked to vulnerability. Mayer et al. describe this relation as:

> *"Making oneself vulnerable is taking risk. Trust is not taking risk per se, but rather it is a willingness to take risk."* [11].

Trust is therefore important to overcome risk in a situation, because an action under risk involves willingly making oneself vulnerable, which is a key component of the definition of trust.

2.3 Trust in Technology

Under the assumption that IT can be trusted, a few changes to the interpersonal trust model above become necessary. With the conceptualization of IT as a trustee, the properties of the trustee that work as antecedents of trustworthiness, had to be changed away from properties of people to properties of technology. One commonly used translation of these properties was done by McKnight et al. [13]. In order for this to work, they remapped the trustworthiness factors identified by Mayer et al. [11] in the following way [13]:

- instead of ability, the degree of supporting the required *functionality* of an IT artefact is used,
- instead of benevolence, the degree of *helpfulness* through helper functions of IT is used, and
- instead of integrity, the *reliability* of IT is used.

With this remapping of antecedents of trustworthiness, it is possible to measure the trustworthiness of IT and consider it as a trustee in a trust relationship or interaction.

When evaluating IT or assessing its broader societal effects, models and theories, such as the Technology Acceptance Model (TAM)[5] and the Unified Theory of Acceptance and Use of Technology (UTAUT)[27] can be used to measure the acceptance, intention to use, and adoption of IT. The question of users trusting technology can be important in this context, with multiple studies identifying trust in IT or its trustworthiness as an important additional factor in a user's acceptance, intention to use, or adoption of an artefact [7,13,20,23]. Besides these outcomes, Thielsch et al. have also discovered the influence of trust in information systems on well-being, performance, and stress [26], which could relate to IT itself as well.

3 Trust-Related Interactions

Resulting from the given definition and conceptualization of trust (see 2.1), an interaction between trustor and trustee can be used to abstract and analyze a situation involving trust and IT. To find additional roles IT can play in these situations, a model of trust-related interactions with their potential ways of IT involvement is derived. As a starting point, a person (or user) is defined to be the trustor in the interaction. In terms of relevant trustees, with whom a person can interact, interpersonal trust and trust in technology have already been covered in 2.1 and 2.3. They are also included in the interaction model. Besides these, various other trustees have also been researched in the literature. For the purpose of this article, it can be argued that especially trust in organizations is of additional interest, because organizations provide the user with IT and are therefore potentially perceived to be associated with it [17,21], e.g. governments [28] and companies [9]. Therefore, organizations will be considered in the abstraction of the interaction as well. The trust-related interaction itself takes place between trustor and trustee in a situational context that involves risk. The resulting interaction model is illustrated in Fig. 2.

In the model, IT is already included as a trustee. But besides being a potential direct interaction partner, IT may serve other purposes in the context of the interaction as well. Following Söllner et al. [22] in differentiating between IT as a mediator or as a trustee, the positioning of the IT artefact in the interaction is set accordingly. Hence, an IT artefact is either a mediator within an interaction between two other entities, effectively providing a form of infrastructure, or the target of an interaction. It is noteworthy to say, while one IT artefact may serve as the trustee of the interaction, another may act as a mediator at the same time.

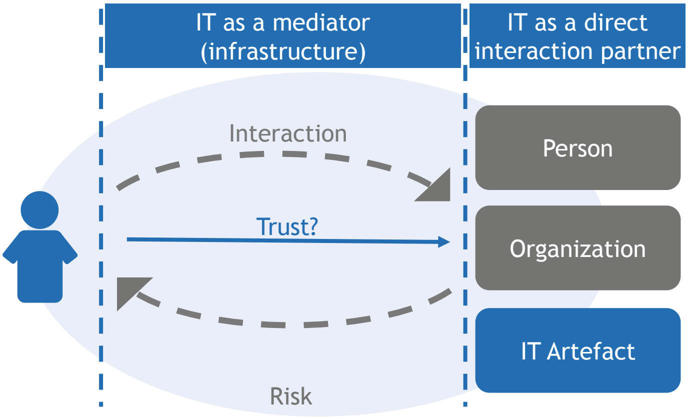
IT as a mediator (infrastructure)
IT as a direct interaction partner
Interaction
Trust?
Risk
Person
Organization
IT Artefact

Fig. 2. Trust as an interaction between different entities.

4 Perspectives on IT Artefacts in Trust-Related Interactions

This trust-related interaction model can now be analyzed to find potential roles that IT artefacts can take within the interaction. In this section, the following identified roles for IT are discussed:

1. an interaction enabler between two other entities (see 4.1),
2. a mechanism for mitigating risk in an interaction between two other entities (see 4.2),
3. a tool used in an interaction (see 4.3), and
4. a trustee in an interaction (see 4.4).

In addition, different terms for the influence on the interaction as perceived by its users are assigned to the roles and discussed further in the article. These include the perceived reliability of an artefact, the change of perceived control during the interaction, and a distinction for IT as interaction partners for which either reliability or trust is perceived. These roles and perception concepts are also visualized in Fig. 3.

It is important to note that IT can potentially fulfill each of these roles depending on the interaction or the scientific perspective taken on the interaction. To further clarify the roles and their interplay, an encrypted messaging service is used as a running example throughout this section.

4.1 IT as an Interaction Enabler

The first identified role is IT as an interaction enabler. It can clearly be identified when seeing IT as a mediator or infrastructure between a trustor and a trustee. IT can be used as a platform or channel for trustee and trustor to act, enabling

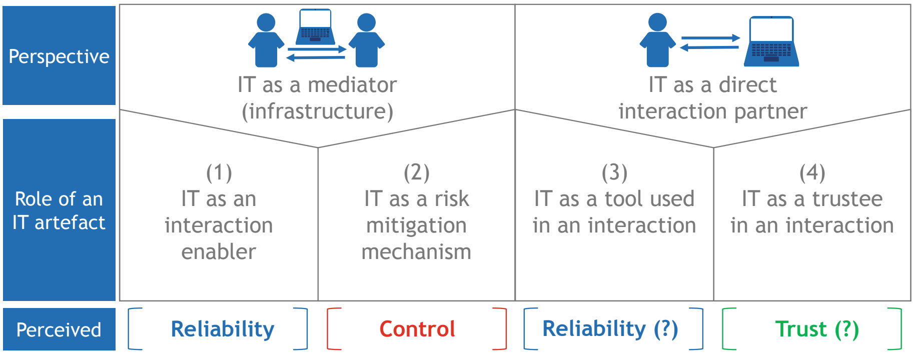
Perspective
IT as a mediator (infrastructure)
IT as a direct interaction partner
Role of an IT artefact
(1) IT as an interaction enabler
(2) IT as a risk mitigation mechanism
(3) IT as a tool used in an interaction
(4) IT as a trustee in an interaction
Perceived
Reliability
Control
Reliability (?)
Trust (?)

Fig. 3. Roles of IT in trust-related interactions.

the interaction. The parties represent themselves digitally or use digital channels within their trusting relationship. In this case, the interaction is based upon the use of technology to facilitate the interaction in any form possible. The interaction involving that role is visualized in Fig. 4.

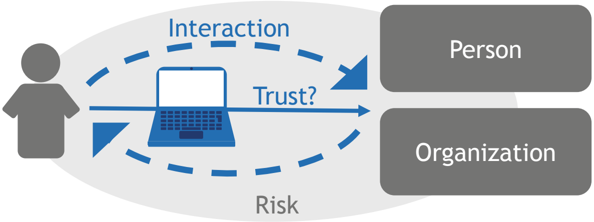

Fig. 4. IT as an interaction enabler

By using IT as an enabler for the interaction, IT can introduce new risk, such as potential system failures, affecting the interaction [6] and possibly alter or distort the perceived trust between parties involved, due to differences in media compared to non-digital alternatives [3]. In terms of the trusting relationship, the involved parties rely on it to work, to be able to interact with one another. Therefore, IT needs to be reliable in this trust interaction. The important factor for the user's perception is therefore *reliability*.

Every IT artefact that is capable of providing the basis of an interaction can potentially take this role. In the example of an encrypted messaging service, the service provides the means to interact digitally on which users rely upon to work as a basis for their interaction.

4.2 IT as a Risk Mitigation Mechanism

The second identified role is IT as a risk mitigation mechanism. From the perspective of IT as an infrastructure, IT can be used to mitigate the involved perceived risk in the context of an interaction. Hereby not affecting trust between the two parties per se, but rather the outcome of a trust evaluation against the perceived risks involved, resulting in a potentially different trust-based action [4]. This role is depicted in Fig. 5.

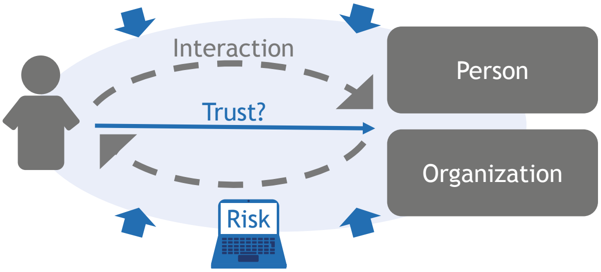

Fig. 5. IT as a risk mitigation mechanism

By actively mitigating the amount of perceived risk involved in a situation, IT acts as a control system for the context in which the interaction takes place [19]. IT taking this role is thus affecting the perceived *control* over a situation.

In the example of an encrypted messaging service, especially the encryption of the transferred massages stands out to be of importance for mitigating the risk in an interaction, e.g. involving to talk about activities that involve high amounts of risks, such as submitting information out of crisis regions [12]. Other examples of IT use mitigating risk can be found in additional forms of transparency or obfuscation technology. Recent developments in blockchain technologies are even often called trust-free technologies or ecosystems [2,16], because trust becomes irrelevant through control in their contexts.

4.3 IT as a Tool Used in an Interaction

The third identified role is IT as a tool used in an interaction. In this case, IT is viewed from the perspective of IT as the interaction partner, which is visualized in Fig. 6.

According to Solomon and Flores, trust, as *“a function of human interaction”* [24], only applies to beings with agency, responding to our actions according to their own attitudes towards the situation and their own intentions [24]. Following this logic, IT artefacts cannot be considered to be trustworthy in a reciprocal relationship on which trust usually is based [24]. Shneiderman put the perception and related behavior of a human user towards IT the following way:

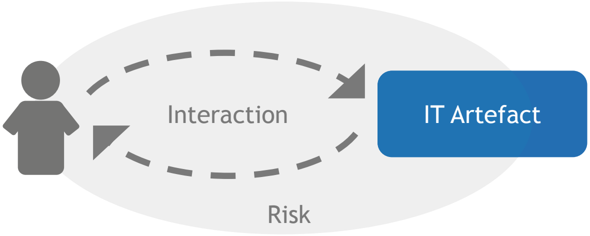

Fig. 6. IT as an interaction partner

> *"If users rely on a computer and it fails, they may get frustrated or vent their anger by smashing a keyboard, but there is no relationship of trust with a computer."* [21]

For any trust-related interaction involving IT, this would mean that we won't be able to view IT as the trustee in the interaction, but would have to refer to IT's perceived *reliability* when using the perspective of IT as the interaction partner.

When considering the example of an encrypted messaging service, this would mean, using the perspective of IT being the direct interaction partner, the importance of the perceived reliability of the service is the important perception for its user.

4.4 IT as a Trustee in an Interaction

The fourth and last identified role is IT as a trustee in an interaction. This role is depicted in Fig. 7, which strongly resembles Fig. 6, differing only in an added trust relationship. When directly interacting with IT, the IT artefact might also be seen as the trustee in a user-to-IT trust relationship.

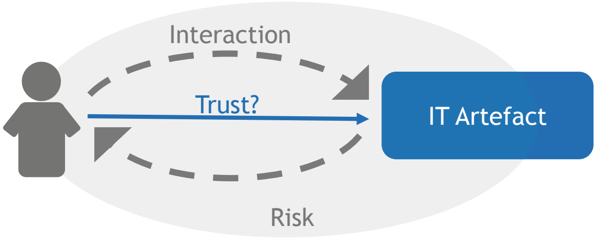

Fig. 7. IT as a trustee in an interaction

CASA [15] and SRT [14] provide insights into how people apply human behaviour, such as social norms, towards technology. It is important to note, the people in the experiments, examined to demonstrate the attribution of human traits to IT through users, were aware that their behaviour might seem unreasonable [15]. Nass et al. derived from this that human *"individuals' interactions with computers are fundamentally social"* [15]. Following this line of argument, a user's perception in an interaction with IT as the direct interaction partner may include the perception of *trust* in IT.

Looking back into the example of an encrypted messaging service, the user might perceive trust in the service and therefore be willing to use it even in situations involving a high amount of perceived risk.

5 Discussion

The proposed framework of roles that IT can take in trust-related interactions, has some limitations and implications for academics as well as practitioners.

Limitations of the Framework. Since this is a theoretical article, the conceptual framework still needs to be tested to fully prove its actual usefulness for academia in future research and practice. Specifically, the distinction in terms of IT as an interaction partner into reliability and trust needs to be clarified and checked for proof, if this holds true. Therefore, the question of the plausibility of trust in IT still remains open.

Implications for Research. This work shows that IT can have multiple implications on situations that involve trust, providing the possibility to use roles of the framework as scientific lenses for research to fixate a certain perspective on the analyzed artefact, while further examining it. Using these roles as lenses on IT, scientists can differentiate properly, what effects they can expect for their studies and measurements when using IT in a trust-related situation. It shows that IT can fulfill different purposes in relation to trust, providing a more differentiated look into what is actually happening.

In addition, resulting from this work, some additional open questions for future research arise:

- How does IT as a risk mitigation factor affect interpersonal or person-to-organizational interactions?
- Is trust in IT actually reasonable and under which circumstances?
- What are processes surrounding IT or attributes of IT that lead to the perception of trust in IT artefacts by its users?
- How can IT be developed and used to work best according to the role or roles it is fulfilling in relation to trust?
- What are roles in case of a more sociotechnical information systems perspective?

Research hence still needs to guide practice towards a better understanding of the social interplay their developments encounter as well as what influences their IT may have on their users.

Implications for Practice. Practitioners can use the proposed roles to think about the influence their IT artefacts may have on the trust-related interactions of their users and can evaluate as well as develop them according to the social role they fulfill. Further work from researchers and practitioners should find guidelines and best practices to better understand their influence points in designing IT according to each potential role.

6 Conclusion

This articles answered what roles IT artefacts can take in trust-related interactions and what the effects of these roles on the perception of the user might be from a theoretical perspective. The resulting framework (Fig. 3) for IT and trust shows clear roles IT can take in trust-related interactions. With the proposed distinction between these roles, research and practice can gain better insights into the effects of IT on the real social world.

Acknowledgements. This work was supported by the "*Trust and Communication in a Digitized World*" research project (promotion reference 1712/1), funded by the German Research Foundation (DFG).

References

1. Alzahrani, L., Al-Karaghouli, W., Weerakkody, V.: Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: a systematic review and a conceptual framework. Int. Bus. Rev. **26**(1), 164–175 (2017). https://doi.org/10.1016/j.ibusrev.2016.06.004
2. Beck, R., Stenum Czepluch, J., Lollike, N., Malone, S.: Blockchain-the gateway to trust-free cryptographic transactions. In: Proceedings to the European Conference on Information Systems, ECIS, Research Papers (2016). https://aisel.aisnet.org/ecis2016_rp/153
3. Daft, R.L., Lengel, R.H.: Organizational information requirements, media richness and structural design. Manage. Sci. **32**(5), 554–571 (1986). https://doi.org/10.1287/mnsc.32.5.554
4. Das, T., Teng, B.S.: The risk-based view of trust: a conceptual framework. J. Bus. Psychol. **19**(1), 85–116 (2004). https://doi.org/10.1023/B:JOBU.0000040274.23551.1b
5. Davis, F.D., Bagozzi, R.P., Warshaw, P.R.: User acceptance of computer technology: a comparison of two theoretical models. Manage. Sci. **35**(8), 982–1003 (1989). https://www.jstor.org/stable/2632151
6. Friedman, B., Khan Jr., P.H., Howe, D.C.: Trust online. Commun. ACM **43**(12), 34–40 (2000). https://doi.org/10.1145/355112.355120

7. Gefen, D., Karahanna, E., Straub, D.W.: Trust and tam in online shopping: an integrated model. MIS Q. **27**(1), 51–90 (2003). https://doi.org/10.2307/30036519
8. Gregor, S.: The nature of theory in information systems. MIS Q. **30**(3), 611–642 (2006). https://doi.org/10.2307/25148742
9. Lankton, N.K., McKnight, D.H.: What does it mean to trust facebook? Examining technology and interpersonal trust beliefs. ACM SIGMIS Database DATABASE Adv. Inf. Syst. **42**(2), 32–54 (2011). https://doi.org/10.1145/1989098.1989101
10. Lee, J.D., See, K.A.: Trust in automation: designing for appropriate reliance. Hum. Factors **46**(1), 50–80 (2004). https://doi.org/10.1518/hfes.46.1.50_30392
11. Mayer, R.C., Davis, J.H., Schoorman, D.F.: An integrative model of organizational trust. Acad. Manag. Rev. **20**(3), 709–734 (1995). https://doi.org/10.5465/AMR.1995.9508080335
12. McGregor, S.E., Charters, P., Holliday, T., Roesner, F.: Investigating the computer security practices and needs of journalists. In: 24th {USENIX} Security Symposium ({USENIX} Security 15), pp. 399–414. {USENIX} Association, Washington, D.C. (2015). https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/mcgregor
13. McKnight, D.H., Carter, M., Thatcher, J.B., Clay, P.F.: Trust in a specific technology: an investigation of its components and measures. ACM Trans. Manage. Inf. Syst. **2**(2), 1–25 (2011). https://doi.org/10.1145/1985347.1985353
14. Nass, C., Moon, Y.: Machines and mindlessness: social responses to computers. J. Soc. Issues **56**(1), 81–103 (2000). https://doi.org/10.1111/0022-4537.00153
15. Nass, C., Steuer, J., Tauber, E.R.: Computers are social actors. In: Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pp. 72–78 (1994). https://doi.org/10.1145/191666.191703
16. Notheisen, B., Cholewa, J.B., Shanmugam, A.P.: Trading real-world assets on blockchain. Bus. Inf. Syst. Eng. **59**(6), 425–440 (2017). https://doi.org/10.1007/s12599-017-0499-8
17. Rosenbloom, A.: Trusting technology: introduction. Commun. ACM **43**(12), 31–32 (2000). https://doi.org/10.1145/355112.355119
18. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: a cross-discipline view of trust. Acad. Manage. Rev. **23**(3), 393–404 (1998). https://doi.org/10.5465/amr.1998.926617
19. Schoorman, F.D., Wood, M.M., Breuer, C.: Would trust by any other name smell as sweet? reflections on the meanings and uses of trust across disciplines and context. In: Bornstein, B.H., Tomkins, A.J. (eds.) Motivating Cooperation and Compliance with Authority. NSM, vol. 62, pp. 13–35. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16151-8_2
20. Shareef, M.A., Archer, N., Dwivedi, Y.K.: An empirical investigation of electronic government service quality: from the demand-side stakeholder perspective. Total Qual. Manage. Bus. Excel. **26**(3–4), 339–354 (2015). https://doi.org/10.1080/14783363.2013.832477
21. Shneiderman, B.: Designing trust into online experiences. Commun. ACM **43**(12), 57–59 (2000). https://doi.org/10.1145/355112.355124
22. Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., Leimeister, J.M.: Understanding the formation of trust in IT artifacts. In: Proceedings of the International Conference on Information Systems, ICIS (2012)
23. Söllner, M., Hoffmann, A., Leimeister, J.M.: Why different trust relationships matter for information systems users. Eur. J. Inf. Syst. **25**(3), 274–287 (2016). https://doi.org/10.1057/ejis.2015.17

24. Solomon, R.C., Flores, F.: Building Trust: In Business, Politics, Relationships, and Life. Oxford University Press, Oxford (2003)
25. Stephanidis, C., et al.: Seven HCI grand challenges. Int. J. Hum. Comput. Inter. **35**(14), 1229–1269 (2019). https://doi.org/10.1080/10447318.2019.1619259
26. Thielsch, M.T., Meeßen, S.M., Hertel, G.: Trust and distrust in information systems at the workplace. PeerJ **6**, e5483 (2018). https://doi.org/10.7717/peerj.5483
27. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**(3), 425–478 (2003). https://doi.org/10.2307/30036540
28. Welch, E.W., Hinnant, C.C., Moon, M.J.: Linking citizen satisfaction with e-government and trust in government. J. Public Adm. Res. Theor. **15**(3), 371–391 (2005). https://doi.org/10.1093/jopart/mui021