Managing Trust – A Design Theory and Design Principles

Completed Research Paper

Fahame Emamjome
Queensland University of Technology
Brisbane, Australia
f.emamjome@qut.edu.au

Michael Rosemann
Queensland University of Technology
Brisbane, Australia
m.rosemann@qut.edu.au

Abstract

Technological developments along with socio-economical changes (e.g., COVID-19) have increased the trust intensity of social and business interactions and have created new trust concerns. On the other hand, the affordances of new technologies facilitate new trust opportunities. Trust is one of the well-cited and popular research areas in Information Systems research. However, despite the depth and breadth of knowledge on trust and related concepts, it remains an elusive concept in practice. We know more about what trust is than how to deal with it. Accordingly, in the absence of a prescriptive trust theory, drawing on existing trust literature and the expertise of senior stakeholders from different companies, we develop a design theory for trust, proposing complementary design principles to build trust into the processes of customers' interaction with a company, considering contemporary trust concerns and leveraging the opportunities provided by new technologies.

Keywords: Design theory, Design principles, trust, technology, trust opportunities, trust concerns

Introduction

Trust is the basis of relationships in all aspects of our life. The current socio-technical ecosystem is amplifying the role of trust and has led to a duality in the trust debate. Technological developments such as the loss of human control in autonomous vehicles, the lack of tangibility in online shopping, the limited transparency once private data is handed over or the technology dominance in environments such as the Amazon Go store, have increased the trust intensity of social and business interactions dramatically and have created new trust concerns. On the other hand, the affordances of technologies such as blockchain (Ostern et al. 2020) or social media (Botsman 2017) facilitate entirely new trust opportunities.

Trust is a widely recognized concept across a variety of disciplines. In Information Systems (IS) trust research has started to grow since 1990. With the increasing ubiquity and advancement of technology, trust remained an increasing concern and as a result, the related literature has grown substantially as one of the well-cited areas of research in IS (Söllner et al. 2016). In IS, trust has been studied in four main categories of interactions (Söllner et al. 2016): interpersonal trust between people, trust between people and organizations, trust between people and technology, and trust between organizations. However, there has been less focus on understanding trust along with the customer's end-to-end interaction with an organization (Rosemann 2019). And while research on the identification of trust concerns within a business process has matured, the body of knowledge on *how* to address and overcome such concerns is still very limited.

IS research on trust is mostly descriptive, defines trust, antecedents of trust and trust measures and explains the relationship between trust and other constructs, e.g., trust and purchase behavior (Pavlou and Fygenson

2006) or system usage (Gefen et al. 2003). Existing trust theories in IS consist of theories for analyzing (e.g., McKnight et al. 2002), for explaining (e.g., Kumar et al. 1998), and for predicting and explaining (e.g., Gefen et al. 2003). There are, however, limited examples of prescriptive trust theories (or theories type 5 in Gregor (2006)). As a result, trust being a well-developed concept in academia remains an elusive concept in practice (Shockley et al. 2016). We know more about what trust is than how to deal with it.

In light of the significance of current trust concerns and opportunities, and the absence of prescriptive trust-related theories, we chose to develop a new design theory and complementary design principles. "A design theory is a prescriptive theory based on theoretical underpinning which says how a design process could be carried out which is effective and feasible" (Walls et al. 1992, p.37). Hence, in this paper, we investigate the following research question: *"How can an organization build trust into processes of interactions with its customers considering contemporary trust concerns and leveraging technologies?"* To answer this question, we studied and consolidated related literature to derive the initial constructs of the design theory. Next, we used explorative interviews with senior stakeholders from retail companies to develop operational design principles. The proposed design theory is developed based on (Gregor and Jones 2007) guidelines and we followed (Gregor et al. 2020) in the development of our in total ten design principles.

This paper is structured as follows. In the next section, we further motivate the development of a trust design theory. Then, we explain the research methodology, followed by theoretical underpinning and the introduction to the proposed design theory and its ten design principles. Finally, we discuss the results before elaborating on limitations and future research opportunities.

Related Literature

The long tradition and variety of disciplines and research approaches depicts that trust is a complex and dynamic phenomenon across cognitive, affective and social levels (Castaldo et al. 2010). Definitions of trust have evolved, and many scholars believe that there is no general and accepted definition of trust (Castaldo et al. 2010; McAllister 1995). The current trust definitions and ontologies are "really a recognized mess", with many domain-specific definitions, models and claims which contradict each other (Castelfranchi and Falcone 2009, p.2). Castaldo et al. (2010) conducted a thematic analysis of trust definitions and identified that most of these definitions include a set of common building blocks (conceptual nature, subject, object, consequences, and characteristics of the context). The heterogeneity in trust definitions is seen as the result of choosing different specifications and combinations of these blocks.

Despite the importance of the "specific action and outcomes" as one of the building blocks of trust definitions (Castaldo et al. 2010), this aspect is usually overlooked in current trust research in IS. Trust as a primary artefact has not made it into the design of the process of customers' interactions with a company (Rosemann 2019). As a result, the trust a customer has with an organization emerges organically and implicitly as opposed to being the outcome of a dedicated trust-building intervention.

The digital economy and new technologies have empowered customers and have created new forms of trust-building mechanisms (Botsman and Capelin 2016). In response to these changes in the trust ecosystem, IS researchers have investigated trust in relation to technology (Söllner et al. 2016). Two main trust-related roles can be identified for technology in these studies: 1) technology as a trust mediator between people and 2) technology as the trustee (Hoffmann et al. 2012).

Research that focuses on designing trustworthy IT systems usually belongs to the latter category. Related studies suggest that trust is the key factor of technology adoption and use (Gefen et al. 2003; Lee and See 2004). Based on the insights from behavioral studies and human-computer interactions, these studies provide prescriptive approaches in designing trustworthy IT systems. For example, Gregor and Benbasat (1999) proposed design principles for knowledge-based systems. Komiak and Benbasat (2006) investigated the impact of personalization on trust in the context of e-commerce websites. (Söllner 2014) proposed a guideline to enable developers to systematically identify trust-supporting design elements. All these studies focus on specific features that constitute the trustworthiness of a certain type of technology (e.g., chatbots (Zierau et al. 2020)) as the trustee). One of the premises of this stream of trust research is that trust can be engineered into the design of technology (Leimeister et al. 2005).

On the other hand, IS research investigating the role of technology as a trust mediator, mostly draws on well-established models of human behavior to develop explanatory and predictive theories for the

relationship between technology features as antecedents of trust (in a vendor) (e.g., Komiak and Benbasat 2006; Punyatoya 2019). These studies, in most cases, investigate e-commerce websites (Söllner et al. 2016) and how different features in the design of e-commerce websites could influence the customer's trust in a vendor (Xiao and Benbasat 2011).

In this paper, we draw on both of these streams of research to provide prescriptive guidelines to design trust in customers' interactions with a company. We argue that to trust a company, trusting one system is not sufficient (for example trusting the online payment system). A customer interacts with a variety of systems, resources and processes through one single interaction. A variety of mechanisms (IT-enabled and others) needs to be applied to ensure the whole interaction is perceived as trustworthy and is trusted by customers. Accordingly, both roles, technology as a trustee and technology as trust mediator, are relevant when proposing technology-enabled mechanisms to build trust. To develop a prescriptive theory to build trust into the process of customers' interaction with a company, we focus on leveraging technologies in building trust. We present a design theory that guides researchers to specify the trust requirements and trust design principles to address and operationalize the design theory in practice.

A design theory is a prescriptive theory, that links the explanatory and predictive theories to actions and agents. In IS, design theories put theories from behavioral and social science into design and action (Aier and Fischer 2011). Building on the rich source of theories on trust from different disciplines, we develop a design theory that focuses on building trust systematically through customers' interactions with an organization.

Methodology

To develop a design theory, consistent with (Markus and Rowe 2018), we adapted the framework suggested by (Lee et al. 2011). A key underlying assumption of this framework is that theorizing for design happens in two distinctive domains: an abstract and an instance domain. In the abstract domain, an abstract solution is identified for an abstract problem. An abstract problem is referred to as "a class of problems" rather than specifics. In the instance domain, an instance solution is applied to solve a particular problem. An instant solution might not be novel and as interesting as the abstract one. This duality is also reflected in the elements of a design theory proposed by (Gregor and Jones 2007)

According to (Lee et al. 2011) there are four activities involved in developing a design theory: abstraction, solution search, de-abstraction, and registration. We conducted these activities in four different stages: 1) identifying the abstract problem based on the existing studies and 2) identifying an abstract solution in an iterative process. This process started with identifying the main components of trust as trustworthiness and confidence through conceptualization, then identifying the general requirements-in relation to these two components. This search (from problems space to solution space) was done iteratively through conceptualizing and theorizing and was revised based on the finding of a series of interviews with senior executives. 3) In this stage the requirements were translated to design principles and sets of mechanisms. This stage is again informed by the interview results and revised based on existing studies. Each design principle in this stage followed (Gregor et al. 2020). All design principles were focused on IT solutions (IT-enabled mechanisms) to address the requirements identified in the previous stage. 4) In this paper, the artificial evaluation of the proposed design theory has been conducted through real-world examples of the proposed mechanisms within each design principle. These examples were either derived from interviews or secondary data. The registration process is part of theory building and the mechanisms proposed in the design principles are revised based on the examples as well. Further registration of the theory can be conducted through future interviews and industry focus groups involving stakeholders beyond the ones that have been selected as part of this study (e.g., end customers) (Hevner and Chatterjee 2010).

Data Collection and Analysis

To better understand the instance domain, we conducted 10 interviews with senior executives of eight large companies in the retail or an affiliated sector. In these interviews, we focused on exploring the role of IT as the enabler of trust in business interactions. The explorative interviews were conducted with retail executives across Australia and the United States. We decided to focus on retail companies as they are in a direct relationship with customers and trust plays an important and increasing role in the relationship between customers and retailers (e.g., a COVID-19 induced trend towards online shopping, comes with new

trust requirements). To get rich data and to understand the full context and role of technology in shaping trust, we decided to contact the senior executives (details below) of significant retail companies to participate in the interviews. Top managers represent the key informants and players on organizations insights and changes (Isabella 1990). We chose a purposive sampling approach to identify the companies and the CEOs to contact (Marshall 1996). Table 1 shows the details of the ten individuals and the firms who took part in our interviews.

Company	*Country*	*Role*	*#Staff*	*#Stores*
Supermarket	Australia	CIO	112000	800
Supermarket	Australia	Media Manager	112000	800
Convenience Store	Australia	CEO	8800	700
Convenience Store	Australia	Head of Marketing	8800	700
Postal Service	Australia	State Manager	80000	4400
Retailer	Australia	GM marketing and Ecommerce	12000	670
Multinational retailer	USA	Director, product manager	2.3 m	10500
Airport	Australia	CEO	260	1
Fast Food Corporation	USA	CEO (now retired)	7000	7000
Travel Agency	Australia	HR director	6000	550

Table 1. Interviewees details

A semi-structured interview approach was chosen to allow for probative follow-up questions and to explore the areas of interest not anticipated by the researchers and to further develop our understanding of actions and context. The interview protocol was informed by design theory constructs and requirements derived within our literature review, but it was also open for participants to add further insights. In our interviews, we first asked the participants to define trust and to explain their trust-related strategies. Second, we asked about how the organization is using technology in building trust. Third, we explored how each organization dealt with the two conceptually identified elements of trust, i.e. trustworthiness and confidence. We did not mention any design principles, but these emerged from coding the interviews in combination with existing studies. The interviews were recorded, transcribed, and then coded by two researchers independently.

Since the purpose of our analysis is to discover operational mechanisms ("acts, activities, form/shape/ architecture") as part of design principles (Gregor et al. 2020, p.1633), the coding and analysis followed an abductive approach (Timmermans and Tavory 2012). We began by following the guidelines by (Glaser and Strauss 2017) and identified the initial concepts inductively (open coding), then we grouped the initial codes into categories (axial coding). At the third stage, we reflected on the constructs and requirements of our design theory and how they are related to categories that emerged from axial coding stage. This helped to identify new requirements which were not initially derived from our literature review. In the next stage, we investigated, if the findings from the interviews were supported by existing theories and literature. If required, mechanisms then were re-worded or combined into higher level of abstraction. These steps of analysis were not linear but followed a recursive approach (Corley and Gioia 2004).

A Design Theory for Building Trust

The design theory we propose in this paper consists of six core components and two additional components as specified by Gregor and Jones (2007). A brief description of each component is presented below. We introduce the main constructs in our design theory (trustworthiness and confidence) and we conclude with the propositions that inform the proposed design principles. Then we introduce the general requirements

for the constructs of trustworthiness and confidence, we explain the design principles, the related mechanisms, provide justifications for each principle and finally provide examples as the instantiation of the proposed mechanisms. Since this paper focuses on customers' trust in their interaction with a business, the trustors are current and potential customers, and the trustee is a company providing products or services. Below, the component of the trust design theory are introduced:

(1) Purpose and scope: Building trust systematically into the process of customer interaction with a company. (**2) Constructs**: Confidence, trustworthiness, and general requirements. **(3) Principles of forms and function**: Ten design principles categorized in two groups. **(4) Artifact mutability**: The design principles suggested in this paper need to be adapted to different organizational contexts. Each design principle specifies a context and sets of mechanisms. For implementation purposes, each context needs to be more specified, and the mechanisms should be selected appropriately. **(5) Testable propositions**: (1) Improving trustworthiness (of a trustee) in relation to existing/relevant risks and uncertainties positively impacts trust decisions by the trustor. (2) Providing a relevant source of confidence for a trustor positively impacts their decision to trust a trustee. **(6) Justificatory knowledge**: This two-stage approach is built based on existing studies on trust. Each design principle is justified separately using existing studies. The mechanisms are derived from existing literature and the interviews with executives in the retail sector. **(7) Principles of implementation:** Not all mechanisms are necessary in every context. The choice of mechanisms is dependent on the existing technologies and the product and service portfolio of the company. **(8) Expository instantiation**: For each design principle, retail-related examples are given that depict how the proposed mechanisms are used to build trust.

Theorizing: Abstract Problem to Abstract Solution

The purpose of this section is to break down the elements of the abstract problem and link them to the requirements of an abstract solution through an intuitive process of conceptualization (Lee et al. 2011). To identify what constitutes building trust, we reviewed existing definitions of trust, intending to isolate the elements that could be controlled and managed by a trustee. Then, we identified the requirements for achieving those elements through an iterative abductive process, using the findings of the interviews and reflection on existing theories.

Trust definitions in literature are usually built around a set of common building blocks; (1) the conceptual nature of trust as a belief, expectation, willingness or attitude. (2) The subjects (trustors and trustee) (3) The attributes of the subjects (trustworthiness of the trustee, propensity of the trustor) (4) The object of trust (trustors objectives in the trusting relationship) (5) Context: uncertainty, risk and vulnerability (Castaldo et al. 2010). Accordingly, we built our definition of trust based on these building blocks as "Trust is a trustor's *confidence* in a trustee's *trustworthiness* to perform specific actions and achieve certain outcomes (through customer's interaction with the company) under the situation of *uncertainty and risk*" (Castelfranchi and Falcone 2009; Giddens 2013; Rosemann 2019).

According to this definition*, risk and uncertainty* are the fundamental analytic presupposition of a trust relationship between a trustor and trustee. Without risk and uncertainty there is no need for trust (McKnight et al. 2002). Risk is a situation with well-specified probabilities. Uncertainty involves ambiguity in the probability of distribution over outcomes (Johnson and Busemeyer 2010). When a trustor decides to trust a trustee, he makes himself vulnerable to the perceived risks (and uncertainties) he believes can be caused by the reliance on the trustee. Even though, it is impossible (and possibly not favorable) to eliminate all the risks and uncertainties, a trustor can positively impact the trustee's evaluation of the situation by reducing the level of (some) risks and showing control over uncertainties. A trustor's control over risks and uncertainties is reflected in their capability or in their level of trustworthiness. *Trustworthiness* is the property of the trustee (Mayer et al. 1995; McKnight et al. 1998). A trustor only trusts a trustee and makes himself vulnerable to risks associated with the trustee's actions, when he believes that the trustee has the attributes (trustworthiness) to limit the possibility and impact of those risks. In this paper, we define trustworthiness as *the attributes of a trustee which makes them capable to deal with and minimize the risks of interactions for the trustor* (customer). Accordingly, building trustworthiness is here seen as the first component for building trust.

The second component, in our definition above, is confidence. According to Mayer (1996) and Luhmann (2000), confidence does not recognize the risk factor in a trusted relationship, rather it is an attitude of assurance (De Filippi et al. 2020). Confidence, thus, does not include personal vulnerability or calculation

of the level of risk or uncertainty. As opposed to trust, confidence does not include individual judgment, but rather a state of mind. A person does not decide to be confident but is confident in their predictions. Consistent with Luhmann (2000) we consider trust and confidence as different concepts, only the former involves an evaluation of risk and trustworthiness. Gidden (2013) explains that we base our daily activities on the confidence that we have in a variety of expert systems (legal systems, professional guides, the scientific community, etc.). These expert systems provide the guarantee in situations in which individuals could not verify themselves (Giddens 2013). Essentially, confidence operates as the platform for trust: confidence in one agent makes it easier to trust the other (related) agent (De Filippi et al. 2020). Accordingly, companies can build trust by leveraging the customers' confidence in other agents and third parties.

Based on this definition of trust we develop the following two propositions as the basis for our design theory: (1) Improving trustworthiness (of a trustee) in relation to existing/relevant risks and uncertainties can positively impact trust decisions by the trustor. (2) Providing a relevant source of confidence for a trustor can positively impact their decision to trust a trustee.

Trustworthiness Requirements

The first five design principles focus on improving trustworthiness, an attribute of the trustee. Based on the definition of trustworthiness in the previous section, trustworthiness attributes (requirements) vary and should be specified based on the existing risks (for the trustor) in the context of the interaction with the trustee. According to (Castelfranchi and Falcone 2009) when engaging in a trust-related interaction, a trustor takes three types of risks: a) risk of failure or missed gains for trustor b) risk of wasting time and investments (losses), c) risk of harm to the trustor's values and interests. Since we are focusing on the end-to-end interaction of a customer, we assume that in each stage of the interaction, a trustor is potentially exposed to all these three types of risks. Accordingly, in this paper, trustworthiness requirements are specified based on these three types of risks and revised based on the interview results.

The first type of risk refers to the trustee's capabilities to fulfil the trustor's main objectives through the whole interaction. For example, in an online shopping experience, a customer has specific objectives in terms of product quality and delivery time. The first type of risk refers to any violation of a customer's objectives (e.g., the risk of a delayed delivery). Since these types of risks could be addressed through systematic management approaches, we refer to the attributes of a trustee in relation to the first type of risk as *systemic risk management*.

Independent of the trustee's effort in reducing the first types of risk, there is always the probability of failure. The second type of risk refers therefore to the situation that despite all risk mitigations, there remains a potential loss for the trustor due to the interaction with the trustee (e.g., a product ordered online arrives damaged). The second type of trustworthiness attributes refers to a trustee's capabilities to compensate for a trustor's loss. We refer to these trustworthiness attributes as *vulnerability management*.

The third type of risk refers to the potential harm to the trustor's interests or values (rather than the main objective) through engagement with the trustee. When a trustor engages in a trusted relationship, she makes herself vulnerable in a variety of other ways. For example, a customer expects to be respected throughout all their interactions with the staff, they expect that the privacy of their personal data is protected, or they may care about a company's values in relation to sustainability and the environment. We define two design principles to build the trustworthiness attributes in relation to this type of risk; one in relation to customer interactions with the staff[1], which we refer to as *behavioral management* and the second one as *customer's values management* to refer to other types of values and interest that the trustor may have in the context of the interaction with the company.

Finally, independent of the actual risks and the requirements, a trustee needs to address customers' perceived risks and uncertainties. This category of requirements was identified through our interviews. Thus, we define the fifth design principle to build trustworthiness which addresses the information asymmetries between trustor and trustee in relation to any of the above categories of risks. We refer to this design principle as *customer's uncertainty management*.

[1] We differentiate between these two categories of requirements based on the interview results.

Confidence requirements

There are many situations in our daily life that we do not have enough knowledge to make a trusted decision, instead in these situations we rely on the confidence we have in regulatory and educational systems and authorities. (Giddens 2013). Relying on a source of confidence simplifies and accelerates the decision to trust a trustee for the trustor. De Filippi et al. (2020) argue that confidence in a particular system (agent) can also result in trust in another system (agent). For example, confidence in legal systems, scientific and education systems can result in a trusted relationship with a trustee who is related to those higher-level systems. Drawing on this argument, we identified five types of requirements, recognizing five sources of confidence: confidence in majority's opinion (Castelfranchi and Falcone 2009), confidence in the existing network, confidence in people with a similar situation, confidence in experts (Giddens 2013), confidence in regulatory and education systems (Giddens 2013) and confidence in technology (Antonopoulos 2014). A trustee can influence a trustor's decision by utilizing and embedding these sources of confidence in their interaction with a trustor. Depending on the characteristics of the trust relationship and the context, different mechanisms could be activated in different forms and within different design principles to leverage confidence to build trust.

De-abstraction: from abstract solution to instance solution

After specifying the requirements for a general solution to build trust, in the next stage we de-abstract the requirements to more specific solutions that can be implemented using IT systems. Based on the interviews results, we propose ten design principles leveraging existing IT systems capabilities to address the above requirements. The design principles proposed in this section follow the template proposed by Gregor et al (2020). We categorized the design principles in the two categories of trustworthiness and confidence (first five focus on trustworthiness and the second five on confidence). Each design principle includes aim, context (based on the interviews), mechanisms (based on the interviews), and reasoning (based on existing literature). If relevant, the actors[2] also have been specified. For all these design principles the implementor is the organization or the company as the trustee and the user is the customer as the potential trustor. The design principles and the related mechanisms are defined on an abstract level (Gregor and Hevner 2013). For them to be applied they need to be implemented considering the context and the technology available.

DP1. Systemic risk management

The first design principle (Table 2) focuses on managing trust through improving trustworthiness in the areas related to the customers' main objectives in an interaction, such as the quality of delivered products and services, the value compared to price (Schrage et al. 2020), timely delivery, etc. Usually, these risks could be managed through management approaches such as TQM, Six Sigma, process management and improvement, quality controls etc. Different technologies are also used to manage these types of risks. For example, monitoring queue length based on Bluetooth signals and crowd counting algorithms using CCTV for queue estimates. There are different types of systematic risks depending on the nature of the business and the trust relationship. In this paper, through interviews, we identified three types of mechanisms to decrease the probability of systemic risks for customers (Table 2).

Aim	Reducing the probability of systemic risks for customers.
Context	There are existing inefficiencies and quality problems in customers' interaction processes, which increase the risk of an unsuccessful outcome for customers.
Mechanisms	Mechanism 1 (guaranteed value): IT systems allow customers (as enactors) to choose a certain product with a certain price ahead of making the purchase decision to reduce the risks related to change in the market prices or qualities. Mechanism 2 (reliable processes): IT systems allow reliable performance of the processes (reducing waiting time, delays, errors) through automation.

[2] Actors include implementor (instantiate abstract definition in concrete design context), users (those whose aims is achieved), enactors (perform actions as part of the mechanisms that used to accomplish the aim)(Gregor et al. 2020, p.1633)

	Mechanism 3 (digital trust infrastructure): IT systems allow the effective safeguarding of data, network and infrastructure through improving security and implementing data verification mechanisms in various data entry points.
Reasoning	By using IT systems to increase the capabilities and the control over the processes, data and products for company, the level of systemic risks for customers is reduced and thus the higher is the chance for customers to trust (Mayer et al. 1995; Schrage et al. 2020).
Example 1: buying fuel through My 7Eleven app	Aim: Build trust by reducing the risk of changing fuel prices for customers. Context: Fuel price is usually fluctuating and creates an increased perception of risk and anxiety for customers. Mechanism 1: The My 7Eleven app allows customers to lock in the best local fuel price for their next purchase. The Fuel Price Lock freezes the best local fuel price to ensure customers are getting the best deal. More so, if the current price of petrol is lower than their locked-in price, they can embrace the lower price.

Table 2. Design principle for systemic risk management

Dp2. Vulnerability management

In a trust relationship, the trustor needs to make themselves vulnerable to the outcomes of the interaction. The second design principle focuses on managing trust by reducing the cost of reliance (risk impact) for the customer. In other words, it is about reducing the customer's vulnerability if a failure occurs. Reducing customer's vulnerability positively influences the possibility of their involvement in a trust-intensive interaction (Schoorman et al. 2007). Based on the interviews, one of the most common forms of vulnerability management is the return-and-refund policy. If customers receive products or services which are not fulfilling their requirements, an accessible return-and-refund process is a way to manage the trustor's vulnerability. Table 3 shows the components for this design principle.

Aim	Reducing the vulnerability (impact of risk) of customers in a situation that their interaction with the business does not match with their expectations.
Context	A customer may have an unsatisfactory interaction with the organization.
Mechanisms	Mechanism 1: IT system allows customer or staff on behalf of a customer (enactors) to withdraw, refund or return within minimum time and without any cost.
Reasoning	By reducing the cost of reliance or impact of the risk for customer, they are less vulnerable (Castelfranchi and Falcone 2009) (Mayer et al. 1995; Schoorman et al. 2007)
Example Amazon return process	Aim: reducing customer vulnerability if not satisfied with the product they received. Context: A customer might not be satisfied with the fit for purpose of the item received. Mechanism: Amazon is launching an automated return processing feature that will automate a "returnless"3 refund.

Table 3. Design principle for vulnerability management

Dp3. Behavioral management

The third design principle focuses on reducing the risks that could be imposed on customers through their interaction with the staff. Staff are different in terms of their qualifications, motivations, experience and skills. This makes it difficult for organizations to provide a consistent, high-quality experience for customers, even if all service staff are trained and have clear guidelines and service scripts. Through interviews, we identified four areas of behavioral risks which could be improved through using technologies: inconsistency in terms of skills (staff ability), lack of knowledge or access to information at

[3] The "returnless refunds" feature on Amazon website, enables sellers to offer a refund to customers, for certain products, without requiring a return.

the time of the interaction, access to the right staff anywhere and at any time, access to the staff in a timely and resourceful manner considering physical restrictions. To mitigate these types of risk, the following four mechanisms were identified in our interviews.

Aim	Reducing the probability of having a disappointing experience for customers in the interaction with the staff.
Context	When part or all the customer interaction with the company involves engagement with the staff who have different levels of qualifications, experiences, and motivations.
Mechanisms	Mechanism 1 (Accessibility): IT systems allow accessibility to the right staff on time overcoming the resource scarcity (staff or customers as enactors). Mechanism 2 (omnipresence): IT systems allow access to find and connect to the appropriately qualified staff independent of location (customer as enactor). Mechanism 3 (augmentation): IT systems allow access to information for frontline staff (service staff as enactors). Mechanism 4 (robotization): IT systems automate and replace the service staff (customer as enactor).
Reasoning	By providing better accessibility to the right staff for a specific task and information for frontline staff and by automating some of the interactions, there is a lower chance of having inconsistencies in customer experience., and that has impact on perceived trustworthiness of the firm (Lee and See 2004; Mayer et al. 1995).
Example: Flight Center	Aim: To provide the same level of expertise across different products. Context: The services offered vary substantially and it is impossible to ensure that every staff has the same expertise across all products. Mechanism 2: Use meta data and real-time video communication to connect a customer with the most qualified, available staff.

Table 4. Design principle for behavioral management

Dp4. Customer's value management

To build a trusted relationship with stakeholders, companies need to consider customers' expectations in relation to ecological and social sustainability (Chen et al. 2008). Design principle four focuses on ecological and social sustainability values. We refer to them as customer's value management.

Depending on the nature and the context of the interaction between a company and its customers, these values and expectations vary. Social and ecological sustainability values are usually informed by the nature of the product or service and the social/political/economical context of the interaction. Growing public awareness about ecological sustainability, diversity, and equity, around the world, especially in developed countries, have created new trustworthiness concerns for many groups of consumers. Many companies have responded to these concerns through creating sustainability plans, equity plans, carbon footprints, etc. These values could (in some contexts) override systemic trustworthiness attributes. The negligence of these values could even result in extreme distrust.

IS researchers have already coined the term green IS as a means towards addressing these sets of values (Chen et al. 2008; Dedrick 2010). There are existing design principles and theories on the topic of IS for sustainability and green IS (Hilpert et al. 2014). Accordingly, we propose ecological sustainability by design as the mechanisms which encompass detailed design principles in relation to ecological sustainability.

Even though IS has the capacity to promote social concerns such as democracy, healthcare, equity and diversity, IS researchers tend to focus more on ecological sustainability and the aspects of social sustainability are usually ignored in the design of IS (Schoormann and Kutzner 2020). New technologies such as artificial intelligence and robotics, e.g., social equity in AI (Mouzannar et al. 2019) and machine learning fairness (Hutchinson and Mitchell 2019), provide new opportunities to develop IS design theories to improve social sustainability (Schoormann and Kutzner 2020). In this paper, we consider customers as the receivers of social sustainability initiatives. According to (Schoormann and Kutzner 2020) the role of IS

in relation to social sustainability consists of IS as an access enabler, IS as a sharer of information, IS as a connector, IS as a safeguard (privacy and safety) and IS as an includer. Based on the interview results, we propose three mechanisms that leverage IS design to protect customers' values in relation to social sustainability.

Aim	Addressing trustors' values and interest beyond their main objectives in a trust-intensive interaction.
Context	Customers may have values and interests which are not necessarily and directly linked to the quality and value of the product or services delivered. These values are usually formed based on the social, political and cultural context.
Mechanisms	Mechanism 1 (ecological sustainability by design): IT systems facilitate reducing GHG emission, reducing transportation costs, reducing travel, improving decision making by tracking and reporting factors in relation to ecological sustainability. Mechanism 2 (privacy by design): IT systems allow customers to choose the level of data sharing and control which they are comfortable with, IT systems should comply with the existing privacy regulations (in data collection, data storage, data sharing and data analysis). Mechanism 3 (safety by design): IT systems facilitate public safety. Mechanism 4 (inclusion by design): IT systems facilitate social inclusion regardless of factors such as disability, gender, culture, and income.
Reasoning	Satisfying the requirements of social and ecological sustainability are the pillars for organizational long-term success (Dyllick and Hockerts 2002). Working towards social sustainability is about eliminating factors which degrade social trust (Missimer et al. 2017).
Example 1: Woolworth	Aim: environmental sustainability Context: The increasing customers' concerns regarding sustainable practices. Mechanism 1: All of the 900 Australian Woolworths and Dan Murphy stores are connected to an energy management system which identifies opportunities to reduce energy consumption across the network.
Example 2: Australia post	Aim: Improving service accessibility around the country specifically through digital platforms Context: Australia post mobile app helps users to manage their deliveries and track their parcels. Mechanism 4: Mobile app is enhanced with features which improve accessibility for all users (with focus with people with disabilities). These features include 'voice over' on iPhone, 'talkback' in Android, 'dynamic type' and 'larger font size' and 'dark mode' to improve accessibility.

Table 5. Design principle for customers' value management

DP5. Perceived risk management

One of the bases of trust is informing the trustor about the trustee's ability and intention to achieve the trustors' goal (Lee and See 2004). Thus, the fifth design principle focuses on reducing the perceived risks and uncertainties for the trustor. According to (Pavlou et al. 2007) spatial and temporal separation between the buyer and seller could create an information asymmetry between the buyer and the seller. Information asymmetry between customers and the company can result in a higher level of perceived risk (Pavlou et al. 2007) and a higher level of perceived risk is a barrier for customers to engage in a trust-intensive interaction (Castelfranchi and Falcone 2009).

Companies can address this problem by providing more transparency for customers. Increasing transparency is one of the important factors in building trust and trust behavior (Leimeister et al. 2005). We identified (through interviews) four areas of perceived risks that can be addressed through decreasing information asymmetry and increasing transparency: performance, supply chain, product fit and delivery

process. Information asymmetry about performance or the quality of products or services is a roadblock for customers engagement. Information asymmetry about the supply chain can reduce the level of customers' trust by ensuring customers about products' journey. For example, Walmart is using blockchain technology to increase transparency and traceability in their processes.

In a buyer and seller relationship, the temporal separation between payment and delivery and incongruence of goals can create concerns around product fit, or seller opportunism, thus raising the level of perceived risk for customers (Pavlou et al. 2007). Accordingly, another area of information asymmetry is about product fit and "product diagnostic" (Pavlou et al. 2007, p.107). This is more of a concern in online shopping or where customers cannot examine the product fit themselves.

Perceived risk of seller opportunism can also be related to the delivery process (Pavlou et al. 2007). For example, if a seller collects the payment and does not deliver the product or prolong product delivery. Domino is a good example that shows how companies identify and address this area of perceived risk. An AI-controlled camera observes the process of making the pizza and identifies differences to the underlying order based on video analytics, a process that can be followed by the customer. We identified four mechanisms to address the perceived risks by increasing transparency.

Aim	Reducing information asymmetry between customers and the company.
Context	Customers may perceive the risk of an interaction higher than the actual level of risk.
Mechanisms	Mechanism 1 (performance transparency): IT systems make the information about the performance or quality of the products (or determinants of the quality) available to the customers (customer as enactor) Mechanism 2 (supply chain transparency): IT systems make the information about the product's supply chain accessible to customers (customer as enactor) Mechanism 3 (product fit transparency): IT systems allow customers to engage with products virtually through augmented reality (customers as enactors) Mechanism 4 (delivery transparency): IT systems make the information about the delivery process accessible to the customers (customer as enactor)
Reasoning	The higher the perceived uncertainty the higher the perceived risk for customers (Dowling and Staelin 1994) and thus customers are less likely to engage in a trust-intensive interaction (Castelfranchi and Falcone 2009). Reducing information asymmetry reduces adverse consequences of perceived uncertainty (Pavlou et al. 2007).
Example Alibaba	Aim: reducing uncertainty about the product's history and supply chain Context: Customers are concerned about the authenticity of the product's origin Mechanism 2: Alibaba's Hema app lets customers scan a product barcode and see product information such as how fresh it is, nutritional data and product origin.
Example Dior	Aim: helping customers in the selection process of their products when they are shopping online. Context: Online shopping has increased in significance due to COVID and its improved convenience. However, the lack of tangibility increases perceived risks. Mechanism 3: Dior's augmented reality app allows customers to experience the look of products such as sunglasses on their smart phones.

Table 6. Design principle for perceived risk management

Dp6. Customer review management

The sixth design principle focuses on building trust through leveraging the confidence in public opinion and the trust in existing customers. With pervasive access to online communication and the popularity of third-party review platforms, online reviews play an important role in building confidence between organizations and their customers (Benlian et al. 2012; Reimer and Benkenstein 2016). This is mainly incorporated through ranking systems provided by either independent platforms or the retailer and could take the form of quantified customer feedback (popularity as expressed by 'likes' or 1-5 ranking) or sales information (most sold, lowest return rate). However, the exact way that review systems are implemented,

varies depending on the context and the products. Businesses leverage these reviews in a way that they are accessible, positive and credible to the new customers (Reimer and Benkenstein 2016).

Aim	Building trust through leveraging the confidence people have in the opinion of the majority.
Context	There is the possibility or a platform where customers can share their experiences or rank the products or services.
Mechanisms	Mechanism 1 (review collection): IT systems allow customers (enactors) to share their experience and rank the products. Mechanism 2 (review presentation): IT systems present the reviews to the customers (existing and potential customers) in a meaningful and accessible way.
Reasoning	Online word-of-mouth effect on shopping behavior through reducing uncertainty (Reimer and Benkenstein 2016) and increasing customers' confidence (Castelfranchi and Falcone 2009).
Example Airbnb	Aim: Building trust through leveraging the confidence according to public opinion. Context: Staying with a stranger in a trust-intensive engagement that can be moderated by having access to the views of previous guests. Mechanism 1: Guests can leave a quantitative ranking based on a 1-5 Likert scale and add qualitative comments. Mechanism 2: Reviews are verified and publicly available on both host's and guest's profiles.

Table 7. Design principle for customer review management

Dp7. Customer network management

The seventh design principle focuses on building trust through leveraging the confidence that people have in the people in their immediate social network. When the assessment of product-fit requires information about the attitude and behavior of the potential customer, access to public mass reviews is insufficient. Trust networks allow users to gain feedback from sources (e.g., friends, colleagues) that they personally trust (Victor et al. 2011). Social network platforms such as LinkedIn and Facebook can be utilized through API management mechanisms to access product-related information from trusted contacts. This could be historical (e.g., friends who have purchased an item in the past) or in real-time (e.g., contacts who assess a product fit via digital channels in the moment of desired purchase).

Aim	Build trust through leveraging existing confidence in a trusted network.
Context	In a trust-intensive interaction, public opinion is not enough as a source of confidence.
Mechanisms	Mechanism: A trust network allows maintaining a circle of trusted contacts who can be accessed in moments that require confidence building for their immediate input or to provide referral trust.
Reasoning	Trust is a transitive concept. People trust the positive comments of people whom they know more than public opinion (Jøsang et al. 2006; Victor et al. 2011)
Example: Facebook API	Aim: Using private social networks to build trust with what would otherwise be unknown providers Mechanism: Airbnb uses the Facebook API to allow possible guests to see which of their Facebook friends have stayed with the host they consider, and then see their friends' reviews, if available, which they may regard as more trusted than the public reviews of the host.

Table 8. Design principle for customer network management

DP8. Expert opinion management

To trust a product of higher complexity, potential customers are often beyond their competence to even assess the credibility of the product of interest (Castelfranchi and Falcone 2009). Due to this complex evaluation, product-specific knowledge is required as a source of building confidence. Thus, a trustor may seek trust through their confidence in recognized experts since there is a lack of viable alternatives ways to gain insights (Layder 1997). Expert recommendation systems embedded in online platforms (such as Amazon, LinkedIn) are examples of using this design principle to build trust. When higher levels of expertise are needed to evaluate the trustee's trustworthiness, providing and displaying certifications or digital badges (confidence in education and legal systems), could also be considered as a mechanism within the 8th design principle.

Aim	Build trust through leveraging the confidence in experts.
Context	In the case of high value and complex products and services, a customer with the intention to purchase might seek the view of an expert who can comment on the capability and credibility of the offer.
Mechanisms	Mechanism 1 (expert recommendation management): Incorporating experts' reviews or endorsements in the e-commerce platform (experts and customers as enactors) Mechanism 2 (certificate management): Providing third-party certifications testifying the capabilities of the offer according to external standards.
Reasoning	People rely on expertise of informed people when assessing complex products or services (Giddens 2013).
Example: Amazon	Aim: Amazon needs to build confidence in customers when they assess the quality of a complex and often expensive product (e.g., noise cancelling headset). Context: The product has an embedded complexity and as a result customers lack the literacy to make an informed decision. However, they are willing to invest time to gain insights into the view of related experts. Mechanism 1: Amazon global experts provide their reviews of products offered on the Amazon Marketplace, so customers can gain additional, credible insights about the products of interest.

Table 9. Design principle for experts' opinion management

DP9. Community management

One of the mechanisms for building trust is through leveraging the confidence someone has in the opinion of other people who have similar needs and characteristics (Castelfranchi and Falcone 2009). A trustor may believe that they have specific requirements and expectations from a trusted relationship with the trustee. In this situation, the customer would only draw on the opinions and behavior of people with similar characteristics, to decide whether to get involved in a trusted interaction with a trustee. (Tuckett and Nikolic 2017).

Aim	Build trust through leveraging the positive experience of similar customers.
Context	In unique situations, customers have special needs and characteristics. In these cases, they value the opinions of people who share the same circumstances with them.
Mechanisms	Mechanism: Communication platform incorporates features such as peer-to-peer communication to facilitate the conversation between people in the same community.
Reasoning	People tend to conform and imitate people similar to themselves (Castelfranchi and Falcone 2009).
Example: Patientslikeme platform	Aim: Increasing patients' confidence by providing them with access to others with similar demographics and symptoms and by learning about their successful treatments. Context: As community-based data platform for medical information and advice, Patientslikeme facilitates learning from the treatments of comparable patients (e.g., all Diabetes type 2 patients).

	Mechanism: Implementing social network technologies to create a community of patients with similar demographics, symptoms and experiences with and an interest in related therapies.

Table 10. Design principle for community management

Dp10. Digital confidence management

With the emergence of technologies such as blockchain, the idea of technology as "trustless trust" and "trusting math" emerged among blockchain advocates (Antonopoulos 2014). However, in this paper, we agree with (De Filippi et al. 2020) that technology does not eliminate the need for trust but mostly increases the level of confidence. In a complex and trust-intensive transaction, mature technologies can work as a "confidence machine" and only indirectly reduce the need to trust in the whole system. Traditional examples of technology as a confidence machine are calculators in invoicing processes or navigation systems in distribution logistics systems. AI recommendation systems are another example of a confidence machine.

Aim	Building trust through leveraging the confidence in mature technologies.
Context	There are certain technologies and algorithms which overtime have created confidence in their performance. In complex and trust-intensive transactions these technologies reduce the need to build trust.
Mechanisms	Mechanism: Where possible, technologies with a level of reliable performance are integrated with existing IT systems and processes.
Reasoning	"Confidence in a particular system can also contribute to the establishment of greater and better trust relationships in another system." (De Filippi et al. 2020).
Example Walmart	Aim: Improve the trust a customer has in the supply chain of a product. Context: Discovering the source of an outbreak of a food-borne disease can take days, if not weeks. Better traceability of fresh products could help companies to act faster. Mechanism: Walmart uses an app to provide in-store information on the customer's smart phone displaying the actual, blockchain-secured (Hyperledger Fabric) supply chain of the products (food products).

Table 11. Design principle for digital confidence management

Discussion, Limitations and Conclusion

In this paper, we proposed a two-staged design theory for trust, based on the concepts of trustworthiness and confidence. Existing trust theories are either explanatory or predictive and if prescriptive, they are limited in terms of their scope. The design theory we proposed here focuses on the process of customer interaction with a company, is built based on existing trust theories and breaks down trust to manageable constructs and requirements. For each requirement, we developed one design principle which specifies how a requirement can be addressed through trust-building mechanisms. Each design principle consists of a context, mechanisms (which were derived from the interviews with executives of the retail sector across Australia) and reasoning for appropriateness of the mechanisms, derived from existing literature. Where possible, we provided further examples of these mechanisms being practised in the industry.

The research presented in this paper comes with a number of *limitations* including the limited quantity of the interview partners. Though each participating organization was substantial in size and each interview partner was very senior as per role, an increased qualitative dataset would have allowed to derive conclusions with a higher validity. Moreover, our study concentrates on one sector only, i.e., retail. However, since the constructs in our design theory (confidence, trustworthiness and the requirements related to them) are derived from existing, largely industry-agnostic theories, they are not limited to the retail sector. Applying abductive reasoning, the mechanisms within each design principle are abstract enough to be applied in similar wider contexts. Also, it is important to note that the design principles and related mechanisms are focusing on technologies and how technology design can be used to address the trust requirements. We are not focusing on other resources and how they could be used to address trust

requirements. Our paper contributes to the academic body of knowledge by providing an entirely new trust-related theory with the two core constructs trustworthiness and confidence. This is a significant addition to the dominating, but often difficult to operationalize focus of the academic debate on ability, integrity and benevolence.

To apply this design theory to build trust in practice, first, the requirements related to trustworthiness and confidence should be examined based on the level of trust intensity of an interaction with a customer. Then, the related design principles should be selected to address those requirements. The choice of mechanisms within each design principle depends on the context, technological, cultural and situational feasibilities. As (Gregor et al. 2020) point out, each mechanism could further be broken down into more detailed design principles. In future studies, we are aiming to work on trust profiling and linking the design principles to trust intensity and characteristics of the context of customer interaction.

Finally, a design theory, like any other theory, should be evaluated based on specific criteria. (Aier and Fischer 2011) developed a set of criteria for the evaluation of design theories: usefulness, internal and external validity, simplicity, and fruitfulness. In future research, we will develop approaches to test the proposed theory against these criteria.

References

Aier, S., and Fischer, C. 2011. "Criteria of Progress for Information Systems Design Theories," *Inf Syst E-Bus Mange* (9:1), pp. 133-172.

Antonopoulos, A. 2014. "Bitcoin Security Model: Trust by Computation," *Forbes. com, February* (20).

Benlian, A., Titah, R., and Hess, T. 2012. "Differential Effects of Provider Recommendations and Consumer Reviews in E-Commerce Transactions: An Experimental Study," *Journal of Management Information Systems* (29:1), pp. 237-272.

Botsman, R. 2017. *Who Can You Trust?: How Technology Brought Us Together–and Why It Could Drive Us Apart*. Penguin UK.

Botsman, R., and Capelin, L. 2016. "Airbnb: Building a Revolutionary Travel Company," *Said Business School Case, University of Oxford*).

Castaldo, S., Premazzi, K., and Zerbini, F. 2010. "The Meaning(S) of Trust. A Content Analysis on the Diverse Conceptualizations of Trust in Scholarly Research on Business Relationships," *Journal of Business Ethics* (96:4), pp. 657-668.

Castelfranchi, C., and Falcone, R. 2009. *Trust Theory : A Socio-Cognitive and Computational Model*. Hoboken, N.J: Wiley.

Chen, A. J., Boudreau, M. C., and Watson, R. T. 2008. "Information Systems and Ecological Sustainability," *Journal of Systems Information Technology* (10:3).

Corley, K. G., and Gioia, D. 2004. "Identity Ambiguity and Change in the Wake of a Corporate Spin-Off," *Administrative science quarterly* (49:2), pp. 173-208.

De Filippi, P., Mannan, M., and Reijers, W. 2020. "Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance," *Technology in Society* (62), p. 101284.

Dedrick, J. 2010. "Green Is: Concepts and Issues for Information Systems Research," *Communications of the Association for Information Systems* (27:1), p. 11.

Dowling, G. R., and Staelin, R. 1994. "A Model of Perceived Risk and Intended Risk-Handling Activity," *Journal of consumer research* (21:1), pp. 119-134.

Dyllick, T., and Hockerts, K. 2002. "Beyond the Business Case for Corporate Sustainability," *Business strategy the environment* (11:2), pp. 130-141.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and Tam in Online Shopping: An Integrated Model," *MIS quarterly* (27:1), pp. 51-90.

Giddens, A. 2013. *The Consequences of Modernity*. John Wiley & Sons.

Glaser, B. G., and Strauss, A. L. 2017. *Discovery of Grounded Theory: Strategies for Qualitative Research*. Routledge.

Gregor, S., and Benbasat, I. 1999. "Explanations from Intelligent Systems: Theoretical Foundations and Implications for Practice," *MIS quarterly* (23:4), pp. 497-530.

Gregor, S., Chandra Kruse, L., and Seidel, S. 2020. "Research Perspectives: The Anatomy of a Design Principle," *Journal of the Association for Information Systems* (21:6), p. 2.

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS quarterly* (37:2), pp. 337-355.
Gregor, S., and Jones, D. 2007. "The Anatomy of a Design Theory," *Journal of the Association for Information Systems* (8:5), pp. 312-335.
Hevner, A., and Chatterjee, S. 2010. "Design Science Research in Information Systems," in *Design Research in Information Systems*. Springer, pp. 9-22.
Hilpert, H., Kranz, J., and Schumann, M. 2014. "An Information System Design Theory for Green Information Systems for Sustainability Reporting-Integrating Theory with Evidence from Multiple Case Studies," *Proceedings of the European Conference on Information Systems (ECIS)*, Tel Aviv, Israel
Hoffmann, A., Söllner, M., Hoffmann, H., and Leimeister, J. M. 2012. "Towards Trust-Based Software Requirement Patterns," *2012 Second IEEE International Workshop on Requirements Patterns (RePa)*: IEEE, pp. 7-11.
Hutchinson, B., and Mitchell, M. 2019. "50 Years of Test (Un) Fairness: Lessons for Machine Learning," *Proceedings of the Conference on Fairness, Accountability, and Transparency*, Atlanata, GA, USA, pp. 49-58.
Isabella, L. A. 1990. "Evolving Interpretations as a Change Unfolds: How Managers Construe Key Organizational Events," *Academy of Management journal* (33:1), pp. 7-41.
Johnson, J. G., and Busemeyer, J. R. 2010. "Decision Making under Risk and Uncertainty," *Wiley Interdisciplinary Reviews: Cognitive Science* (1:5), pp. 736-749.
Jøsang, A., Gray, E., and Kinateder, M. 2006. "Simplification and Analysis of Transitive Trust Networks," *Web Intelligence Agent Systems: An International Journal* (4:2), pp. 139-161.
Komiak, S. Y., and Benbasat, I. 2006. "The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents," *MIS quarterly* (30:4), pp. 941-960.
Kumar, K., Van Dissel, H. G., and Bielli, P. 1998. "The Merchant of Prato-Revisited: Toward a Third Rationality of Information Systems," *MIS quarterly* (22:2), pp. 199-226.
Layder, D. 1997. *Modern Social Theory: Key Debates and New Directions*. Psychology Press.
Lee, J. D., and See, K. A. 2004. "Trust in Automation: Designing for Appropriate Reliance," *Human factors* (46:1), pp. 50-80.
Lee, J. S., Pries-Heje, J., and Baskerville, R. 2011. "Theorizing in Design Science Research," *Lecture Notes in Computer Science* (6629), pp. 1-16.
Leimeister, J. M., Ebner, W., and Krcmar, H. 2005. "Design, Implementation, and Evaluation of Trust-Supporting Components in Virtual Communities for Patients," *Journal of Management Information Systems* (21:4), pp. 101-131.
Luhmann, N. 2000. "Familiarity, Confidence, Trust: Problems and Alternatives," *Trust: Making breaking cooperative relations* (6:1), pp. 94-107.
Markus, M. L., and Rowe, F. 2018. "Is It Changing the World? Conceptions of Causality for Information Systems Theorizing," MIS Quarterly (42:4) , pp. 1255–1280.
Marshall, M. N. 1996. "Sampling for Qualitative Research," *Family practice* (13:6), pp. 522-526.
Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *cademy of management review* (20:3), pp. 709-734.
McAllister, D. J. 1995. "Affect-and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations," *Academy of management journal* (38:1), pp. 24-59.
McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information systems research* (13:3), pp. 334-359.
McKnight, D. H., Cummings, L. L., and Chervany, N. L. 1998. "Initial Trust Formation in New Organizational Relationships," *Academy of Management review* (23:3), pp. 473-490.
Missimer, M., Robèrt, K.-H., and Broman, G. 2017. "A Strategic Approach to Social Sustainability – Part 1: Exploring the Social System," *Journal of Cleaner Production* (140), pp. 32-41.
Mouzannar, H., Ohannessian, M. I., and Srebro, N. 2019. "From Fair Decision Making to Social Equality," *Proceedings of the Conference on Fairness, Accountability, and Transparency*, New York, pp. 359-368.
Ostern, N., Rosemann, M., and Moormann, J. 2020. "Determining the Idiosyncrasy of Blockchain: An Affordances Perspective," *Proceedings of the International Conference on Information Systems (ICIS)*, India
Pavlou, P. A., and Fygenson, M. 2006. "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), pp. 115-143.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.

Punyatoya, P. 2019. "Effects of Cognitive and Affective Trust on Online Customer Behavior," *Marketing Intelligence Planning* (37:1), pp. 80-96.

Reimer, T., and Benkenstein, M. 2016. "When Good Wom Hurts and Bad Wom Gains: The Effect of Untrustworthy Online Reviews," *Journal of Business Research* (69:12), pp. 5993-6001.

Rosemann, M. 2019. "Trust-Aware Process Design," *International Conference on Business Process Management*, Austria: Springer, pp. 305-321.

Schoorman, F. D., Mayer, R. C., and Davis, J. H. 2007. "An Integrative Model of Organizational Trust: Past, Present, and Future." Academy of Management Briarcliff Manor, NY 10510.

Schoormann, T., and Kutzner, K. 2020. "Towards Understanding Social Sustainability: An Information Systems Research-Perspective," *Proceesing of The International Conference on Information Systems(ICIS)*, India

Schrage, R., Kenning, P., Guhl, D., and Gabel, S. 2020. "Price Personalisation Technology in Retail Stores: Examining the Role of Users' Trust," *Proceedings of the Internation conference on Information Systems* India

Shockley, E., Neal, T. M., PytlikZillig, L. M., and Bornstein, B. H. 2016. *Interdisciplinary Perspectives on Trust: Towards Theoretical and Methodological Integration*. Switzerland Springer.

Söllner, M. 2014. *Deriving Trust Supporting Components for Ubiquitous Information Systems*. Kassel Kassel University Press

Söllner, M., Benbasat, I., Gefen, D., Leimeister, J. M., and Pavlou, P. A. 2016. "Trust," in MIS Quarterly Research Curations, Ashley Bush and Arun Rai, Eds.*, http://misq.org/research-curations*.

Timmermans, S., and Tavory, I. 2012. "Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis," *Sociological theory* (30:3), pp. 167-186.

Tuckett, D., and Nikolic, M. 2017. "The Role of Conviction and Narrative in Decision-Making under Radical Uncertainty," *Theory Psychology* (27:4), pp. 501-523.

Victor, P., De Cock, M., and Cornelis, C. 2011. "Trust and Recommendations," in *Recommender Systems Handbook*. Springer, pp. 645-675.

Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. 1992. "Building an Information System Design Theory for Vigilant Eis," *Information systems research* (3:1), pp. 36-59.

Xiao, B., and Benbasat, I. 2011. "Product-Related Deception in E-Commerce: A Theoretical Perspective," *MIS Quarterly* (35:1), pp. 169-195.

Zierau, N., Hausch, M., Bruhin, O., and Söllner, M. 2020. "Towards Developing Trust-Supporting Design Features for Ai-Based Chatbots in Customer Service," in: *In proceeding of the International Conference on Information Systems (ICIS)*. India