

IDENTIFY THE ANTECEDENTS OF DISTRUST IN A WEBSITE

Jinbi Yang, School of Business, Jiangnan University, China, yjinbi2-c@my.cityu.edu.hk

Choon Ling Sia, Department of Information Systems, College of Business, City University of Hong Kong, Hong Kong, iscl@cityu.edu.hk

Carol Xiaojuan Ou, Department of Information Management, Tilburg University, Netherlands, carol.ou@uvt.nl

Abstract

It has been widely accepted that distrust is qualitatively different from trust. Yet scholarly knowledge about the antecedents of distrust is scarce, while the antecedents of trust have received extensive attention. Furthermore, little empirical research has explored how website factors impact on the formation of distrust in a user. Drawing upon the review of distrust literature and competence-motive perception, we propose a new theoretical framework to explain how website factors impact on perceptions of the attributes of a given website, which in turn form user distrust. In this research, distrust is triggered by website evaluations in two areas, namely malevolence and incompetence. These two attributes are determined by three website factors: lack of structural assurance, interface design, and lack of third-party recognition. The proposed research model of distrust formation in the online context is verified by an online survey with 283 valid responses. We offer theoretical and practical implications for our findings.

Keywords: Distrust, Competence and motive perception, Malevolence, Incompetence, Website factors.

1 INTRODUCTION

More and more new Internet companies are joining the fight for the profits offered by the Internet. In this competitive environment, trust is the key to maintaining site viability and increasing page hits. Trust leads to continued success, while distrust means failure. As social trust is becoming a serious issue, distrust is also particularly important in online context. For example, the Chinese Academy of Social Sciences announced that the degree of social trust had dropped to an unacceptable level in 2013, which also implies that the Chinese are more likely to distrust online stores. Thus, a large portion of investment of e-commerce is used to alleviate “distrust”. Avoiding distrust should be the primary concern of websites, and therefore research into distrust is very important. Moreover, the unique characteristics of e-commerce could easily cause financial damage, psychological damage to users, loss of time, and loss of private information (Xiao and Benbasat 2011). These dangers are all potential sources of distrust. For online sellers, distrust could either increase their costs and reduce their profits, or even result in e-commerce failure (Hsiao 2003). Sellers need to spend considerable sums to compensate for distrust to ensure a successful transaction. Moreover, owing to distrust, online businesses could suffer from losses in sales and reputation. Therefore, it is meaningful and urgent to understand clearly how distrust is engendered, by exploring the antecedents of distrust in a website and how they impact on the formation of distrust.

Distrust is defined as “A user’s negative expectations regarding a website’s conduct” [(Ou and Sia 2010), p. 915]. Distrust is induced by some strong evidence, and protects oneself from the harmful conduct of the other party. While trust has received extensive attention, fewer investigations into distrust have been conducted. This may be due to the habitual assumption that distrust and trust are bipolar constructs. However, these assumptions have been challenged. Lewicki (1998) argued that high trust is not the same as low or no distrust. Some scholars have asserted that the same factors could contribute to asymmetries in judgments regarding trust and distrust (Cho 2006; Kramer 1999; Lewicki and Tomlinson 2003). More specifically, Dimoka (2010) explained distrust and trust as distinct constructs associated with different neurological processes, further clarifying the difference in the function and effects of distrust and trust. All of the prior research cited above has claimed that distrust and trust are different and separate constructs, with different antecedents and consequences. Moreover, Cho (2007) proved that distrust exerted even greater effects on online behaviour than trust did. While lots of mature studies reach consensus on the antecedents of trust - integrity, benevolence and ability (Jarvenpaa et al. 1998; Lee and Turban 2001; Mayer et al. 1995; McKnight et al. 2003), there is no consistent opinion on the antecedents of distrust. Therefore, our research question is what the antecedents of distrust are in the online context.

Exploring the antecedents of distrust is meaningful. For website owners and designers, distrust could either increase their costs and reduce their profits, or even result in e-commerce failure (Hsiao 2003). They can eliminate user distrust and increase user trust by improving or controlling those website factors which give rise to distrust. For online users, understanding the formation of distrust helps them to recognize risky shopping environments, and to make rational decisions. Theoretically, this research enriches the existing literature on distrust by exploring the process of distrust formation in the online context, rather than just adopting antecedents of trust directly as the antecedents of distrust in most prior research.

2 LITERATURE REVIEW

2.1 Distrust Conception

Since Lewicki (1998) discussed the relationship between trust and distrust systematically, stating that trust and distrust were separate dimensions having different antecedents and outcomes, an increasing number of scholars have begun to pay attention to the relationship between trust and distrust. Distrust is not merely the mirror image of trust, but operates quite differently. It has been verified that trust and distrust activate different brain areas and have different effects (Dimoka 2010). Trust is believed to be emotionally associated with hope, positive rewards and cooperative intentions, while distrust is

associated with the fear of loss and intense negative emotions of worry and fear. Therefore, distrust is not merely the opposite of trust – “not trust” (Kramer and Cook 2004; Lewicki et al. 1998). “Not trust”, which is not a sufficient condition for distrust, refers only to an ambiguous psychological status (Ullmann-Margalit 2004). One instance of “not trust” is “I do not trust that this website is honest”. While “not trust” does not form any certain views - neither trust nor distrust, distrust aims to reach a certain status. In the same example, distrust should be expressed as “I trust that this website is not honest”. The two statements allow us to grasp intuitively the difference between “not trust” and distrust. The modern use of the term “distrust” is quite different from the former conception of distrust, which we now describe as “not trust”. Distrust and trust are equivalent social alternatives (Baba 1999). One can choose to trust, to distrust or both to trust and distrust.

The most widely-recognised and comprehensive definition of distrust is that of Lewicki (1998) - the trustor’s confident negative expectations regarding the trustee’s conduct, signaling “a fear of, a propensity to attribute sinister intentions to, and a desire to buffer oneself from the effects of another’s conduct” (Tomlinson & Lewicki 2006; Komiak et al. 2008; Benamati et al. 2007). This definition covers much information, including emotion, attribution and consequence. We believe it is too general and ambiguous for our study. Given the research topic and context, we instead adopt Ou’s (2010) definition of distrust - A user’s negative expectations regarding a website’s conduct. Distrust is characterized by fear, worry, or cynicism, and is induced by some strong evidence (Barnett 2008). It evokes fear and prompts action to protect oneself from the harmful conduct of the other party. A state of distrust is the mental system’s signal that an environment is not normal, following the intense negative emotions of wariness, caution, defensiveness, vigilance, anger, hate and betrayal (Dimoka 2010). Under such circumstances, individuals sense they should be on guard, and are likely to avoid routine strategies (Schul et al. 2008).

2.2 A Critical Review of Distrust Studies

In order to gain comprehensive and systematic understanding of prior IS research into distrust, particularly the determinants of distrust, we surveyed all articles on topics relevant to distrust in five reputable IS journals from 1990 to 2015 – MIS Quarterly, Information Systems Research, Journal of Management Information Systems, International Journal of Electronic Commerce, and Information & Management. Most of these studies were based on trust-related research, rendering it difficult to see distrust as distinct from trust. For this reason, we extended the scope of our review to articles whose titles related to distrust in four psychological and four management journals from 1990 to 2015, specifically the Annual Review of Psychology, Journal of Personality and Social Psychology, Psychological Bulletin, Motivation and Emotion, Academy of Management Review, Organization Science, Academy of Management Journal, and Administrative Science Quarterly. A total of 30 articles were identified, as shown in Table 1.

From the articles listed below, it would appear that the determinants of distrust have not been fully investigated. Scholars have multiple perspectives on the factors triggering distrust. In summary, distrust may be determined by four kinds of factor: (1) attributes of object, such as malevolence, discredibility, violation of trustworthiness, incompetence or deceptiveness (e.g. Dimoka 2010; Gillespie and Dietz 2009; Benamati et al. 2010; Baba 1999; Darke and Ritchie 2007); (2) personal characteristics, such as a predisposition to distrust, negative stereotyping, self-consciousness, suspicion of humanity, or past negative behaviors (e.g. Bigley and Pearce 1998; Kramer 1994 and 1999; McKnight and Chervany 2001a); (3) psychological state or emotions, such as negative affectivity, suspicion or doubt (e.g. Lewicki et al. 1998; Lewicki and Tomlinson 2003; Fein and Hilton 1994; Kramer 1999 and 2001); (4) perceptions of specific features, such as technical functionality, situational normality, information quality, ease of use, perceived usefulness or lack of structural assurance (e.g. Ou and Sia 2010; McKnight and Chervany 2001a).

Distrust can be irrational or rational (Kramer 1994). Irrational distrust occurs mainly due to an extreme form of propensity to distrust, even in the absence of evidence or specific experiences indicating untrustworthiness. Rational distrust on the other hand, arises from cognitive assessment based on a specific interaction history. Given the strong link between disposition to distrust (a personal characteristic of the trustor) and irrational distrust (Bigley and Pearce 1998), this study will focus mainly

on rational distrust, whereas irrational distrust will be controlled for. Consequently, the first type of factors will be controlled for in this study. Accordingly, the other three types of factors could induce the rational distrust. Rational distrust develops from the interaction experiences (Kramer 1994), and is triggered when the trustor encounters some strong evidence inducing negative evaluation. Moreover, the third type of determinants of distrust, i.e. “psychological state or emotion”, is not considered in our research. Since the psychological state and emotion are more individual level more than website level. Our research focuses on website characteristics.

Author	Theory/Context/ Methodology	Factors
Dimoka (2010)	<ul style="list-style-type: none"> • Functional neuroimaging (fMRI) tools; • eBay’s auction marketplace, Mp3 player; • Lab experiment, four profiles were created by manipulating each seller’s feedback text comments. 	Discredibility ; Malevolence.
Ou and Sia (2010)	<ul style="list-style-type: none"> • Two-factor theory in the workplace (Herzberg et al. 1967); Three-factor product evaluation framework (Oliver 1997); • Website design and online shopping ; • Survey. 	Functional perception: - <i>Technical functionality</i> ; - <i>Situational normality</i> ; - <i>Information quality</i> ; Bivalent factors: - <i>Structural assurance</i> ;- <i>Ease of use</i> ; - <i>Perceived usefulness</i> .
Gillespie and Dietz (2009)	<ul style="list-style-type: none"> • Systems theory, distrust regulation; • Organization. 	Trust violation; Failure.
Hsiao (2003)	<ul style="list-style-type: none"> • E-marketplace adoption; • Interpretative method 	Value-oriented distrust
Bigley and Pearce (1998)	<ul style="list-style-type: none"> • Organization and allied sciences; Problem-centered approach. 	Predisposition to distrust; Immediate situational factors; Institutional frameworks.
Sitkin (1993)	<ul style="list-style-type: none"> • Organizations with employees with HIV/AIDS; 	Reliability-oriented distrust; Value-oriented distrust;
Lewicki, and McAllister (1998)	<ul style="list-style-type: none"> • Organizations. 	Negative affectivity - <i>low: calm, relaxed, at rest</i> ; - <i>high: distressed, fearful, hostile</i>
Lewicki and Tomlinson (2003)	<ul style="list-style-type: none"> • Development of transactional relationships. 	Differences in groups: - <i>negative stereotypes</i> - <i>prior reputation</i> - <i>experience</i> - <i>trust violation</i>
Fein and Hilton (1994)	<ul style="list-style-type: none"> • A review paper, containing three studies examining costs of suspicion. 	Suspicious (contextual information-ulterior motives)- seeing actors in a more negative light; Involvement, recent experiences (moderate effects).
Kramer (1994)	<ul style="list-style-type: none"> • Groups or organizations: how tenure influences individuals; • Experiment. 	Self-consciousness; Evaluative scrutiny; Rumination on negative experiences; Location in a social system;
Kramer (1999)	<ul style="list-style-type: none"> • Review of trust; • Organizations, 	Suspicion; Self-consciousness, scrutiny; Social categorization.
Kramer (2001)	<ul style="list-style-type: none"> • Social Auditor model; • Computer Simulation. 	Uncertainty; Doubt.

McKnight and Chervany (2001)	<ul style="list-style-type: none"> • TRA ; • Individual or between computer agents; • Not empirical. 	Suspicion of humanity; Distrust stance; No structural assurance; No situational normality; Distrusting beliefs.
McKnight and Kacmar (2004)	<ul style="list-style-type: none"> • 2*2 chart from Lewicki; • Online behavior, website quality and trust intention, LegalAdvice.com ; • Survey, questionnaire. 	Suspicion of humanity; Negative emotions.
McKnight and Chervany (2006)	<ul style="list-style-type: none"> • Internet legal advice provider, LegalAdvice.com ; • Survey, questionnaire. 	No structural assurance.
Benamati and Serva (2007)	<ul style="list-style-type: none"> • Framework of trust and distrust by Lewicki et al.1998; • No empirical. 	Suspicion.
Benamati et al. (2010)	<ul style="list-style-type: none"> • E-commerce, Online banking 	Disposition to distrust; Trustworthiness: -Ability; -Benevolence; -Integrity
Schul et al. (2008)	<ul style="list-style-type: none"> • Multiple-cue, probability-learning paradigm; • Experiments, Individual orienting tasks 	Unusual (abnormal) environments; Past negative behaviors.
Marsh and Dibben (2005)	<ul style="list-style-type: none"> • Formulae to estimate situational trust and cooperation. 	High risk situations; Limiting exposure; $T_x(y,a) < 0$ (negative intention).
Deutsch (1958)	<ul style="list-style-type: none"> • Game theory 	Suspicion; Task reliability (e.g., competence/intentional trust); Value congruence.
Komiak and Benbasat (2008)	<ul style="list-style-type: none"> • Process theory, Trust-building process, Process & outcome trust model Johns (1996). 	Awareness of unknown; Expectation evaluation; Competence attribution.
Keyton and Smith (2003)	<ul style="list-style-type: none"> • Content analysis, Bulter & Cantrell's trust dimensions 	
Cho (2006)	<ul style="list-style-type: none"> • Trust theory and Lewicki et al's trust/distrust conceptualizations; • B2C e-commerce; • Survey. 	Dimensions of trustworthiness: -Competence; -Benevolence. Performance Evaluations: Core Business operations; Relationship Investments.
Cho (2007)	<ul style="list-style-type: none"> • E-commerce; • Survey 	Violation of dimensions of trustworthiness: -Competence; -Benevolence; -Integrity.
Yin et al. (2008)	<ul style="list-style-type: none"> • Cognition/Affect Perspective; • Online bookstore; • Experiment. 	Dishonesty; Self-interest; Privacy assurance.
Baba (1999)	<ul style="list-style-type: none"> • Automotive and aerospace industries; • Case study. 	Quality/competence; Fiduciary responsibility/security.
Adams et al. (2010)	<ul style="list-style-type: none"> • Organization; • Survey. 	Corporate distrust: -Interpersonal trust -Cynicism -Human nature -Negative affect
Darke and Ritchie (2007)	<ul style="list-style-type: none"> • Experiment 	General distrust: Deceptive advertisements.

Abbasi et al. (2010)	<ul style="list-style-type: none"> • Statistical learning theory; • Experiment (evaluation); AZProtect 	Fake websites: <i>-Information</i> <i>-Navigation</i> <i>-Visual design</i>
----------------------	--	--

Table 1. Summary of Distrust Studies

2.3 Website Attributes

As stated above, the first type of factors, i.e., attributes/characteristics of object (trustee), could lead to distrust. The violation of trustworthiness, comprising competence, benevolence and integrity, has been extensively adopted as the antecedent of distrust (Benamati et al. 2010; Cho 2006; Cho 2007; Lewicki and Tomlinson 2003; McKnight and Chervany 2001). More specifically, Cho (2006) empirically demonstrated that only incompetence gives rise to significant distrust in e-commerce. Following the prior work cited above, Dimoka (2010) used discredibility and malevolence as the two indicators of distrust, integrating incompetence and dishonesty under the umbrella of discredibility. Sitkin (1993) and Hsiao (2003) argued that both value incongruities and technical incompetence could engender distrust, based on Deutsch's (1958) research. In parallel, perceptions of incompetence and lack of fiduciary responsibility both appear to be factors stimulating distrust of information technologies (Baba 1999). In summary, prior literature has identified several attributes that could give rise to rational distrust, namely violation of trustworthiness (benevolence, integrity and ability), malevolence, dishonesty, incompetence, and discredibility.

Among them, violation of trustworthiness has not been clearly defined in prior research, but directly adopts the antecedents of trust, and confusing them with malevolence, dishonesty and incompetence. This study considers these concepts differently. We take violation of benevolence to mean the absence of benevolence or self-interest, which is different from malevolence. Similarly, violation of honesty refers to "not honesty", which means withholding something intentionally, and is also distinct from dishonesty or deceit. Violation of ability and incompetence describe the same construct, because ability does not possess a distinct negative counterpart and can only be high or low. We therefore consider violation of trustworthiness as an antecedent of "not trust", as described above. Therefore, violation of trustworthiness will not be considered in this study. Given the ambiguity of malevolence and dishonesty (Baba 1999; Barnett 2008; Chopra and Wallace 2003; Deutsch 1960; Komiak and Benbasat 2008) and the overlap among incompetence, dishonesty and discredibility (Dimoka 2010), we argue that malevolence and incompetence are two main attributes of a website which may lead to distrust, among the left attributes of distrust, namely malevolence, dishonesty, incompetence and discredibility, drawing upon the cognitive-affective perspective and motive-competence perception (Barnett 2008; Kee and Knox 1970; McAllister 1995; Ridings et al. 2002). Using these two attributes not only ensures clear comprehension of the dimensions, but also covers all the attributes discussed above, without overlaps.

According to attribution theory, attribution refers to the perception or inference of cause, which is originated from the analysis of the gathered cues or information (Kelly et al. 1980). The attribution process may be automatic, where an individual has little awareness of the causal attribution, or intentional, where the causal attribution becomes more self-conscious. Apparently, the website features act as the perceived cues of information leading to the causal attribution of website in this research context, which is the fourth type of reviewed factors influencing the distrust formation.

2.4 Website Features and Distrust

The rest type of distrust factors, namely "perception of specific features", acts as an indirect determinant. Little research has empirically referred to the design issues formulating distrust. In the context of website design, some design factors are reported to result in trust or distrust. Website design is the first and major channel through which users form beliefs concerning the website. Much research has been conducted to explore the website features forming trust in the context of website trust-building (Gefen et al. 2003; Lim et al. 2006; McKnight et al. 2002). Specifically, McKnight et al. (2002) identified three main website factors – perceived vendor reputation, perceived site quality and structural assurance of the web. In the reputation category, third-party recognition may affect trust of a website (Lim et al.

2006). Following the categorization of McKnight et al. (2002), we identify three website factors leading to distrust in a website, namely lack of structural assurance, interface design and lack of third-party recognition.

Lack of structural assurance and lack of third-party recognition are negative counterparts of trust-related features, except for interface design. It is worthy of note that some distrust-related website features are not merely lower levels of trust-related features, but their negatives. We posit that low levels of trust-related features are not sufficient to engender distrust, but only low trust or “no trust”, which is different from distrust. For distrust to arise, negative perceptions are required. However, interface design is fully adopted, because “no/lack of interface design” is meaningless, and poor design is merely a low level of interface design. We therefore argue that a low level of website design is sufficient to induce distrust. In this research, website factors will be ascribed to the attributes of the website, and in turn influence distrust.

3 RESEARCH MODEL AND HYPOTHESES

Based on the review and deliberation of determinants of distrust, we propose that website attributes, termed as malevolence and incompetence, directly induce distrust, while website factors affect distrust indirectly. The research model is shown in Figure 1.

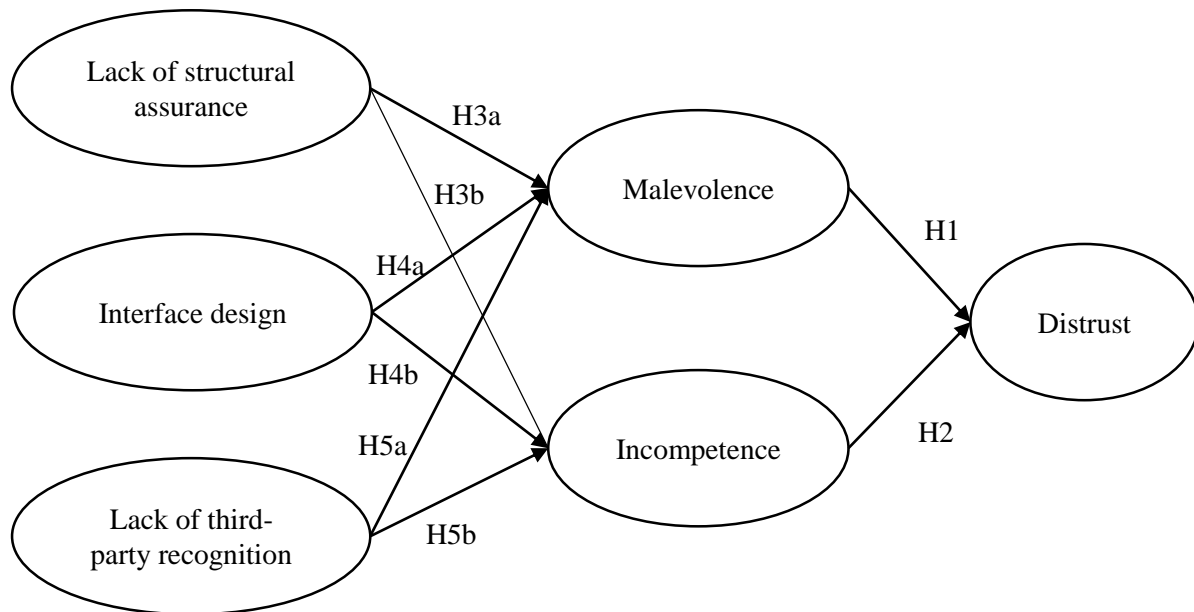


Figure 1. Research Model

3.1 Website Attributes and Distrust

3.1.1 Malevolence

Apart from incompetence, the attribution of a website’s harmful intention is the other primary antecedent of distrust. As we discussed in previous paragraphs, malevolence reflects a harmful intention that would induce distrust. Malevolence means harmful, and negative motives or sinister intentions, which denotes a broad set of malicious practices (Grazioli and Jarvenpaa 2003). Malicious websites intentionally foster an incorrect cognitive representation to instigate a desired action. Such ill-directed action may result in huge losses to the user (Grazioli and Jarvenpaa 2003). Thus, when individuals perceive malevolence in a website, they form negative expectations and cease to be vulnerable to the website to prevent negative outcomes. Therefore, we hypothesize:

H1: Perceived malevolence is positively associated with distrust in a website.

3.1.2 *Incompetence*

Distrust refers to the user's negative expectations regarding a website's conduct (Ou and Sia 2010). Competence comprises a website's knowledge, information, products, reputation, size, etc. A distrustful user tends to fear that a website does not have the ability or competence to provide the good service or product expected. If a website is perceived as incapable, it is anticipated that it will fail to perform tasks as the user expects and the website is obliged to do. In this case, distrust will form to protect the user from potential negative consequences. Thus, the violation of task competence can engender distrust. Therefore, we hypothesize:

H2: Perceived incompetence is positively associated with distrust in a website.

3.2 **Website factors and Website Attributes**

An individual evaluates possible causes when negative outcomes occur based on attribution theory. Accordingly, when a user encounters negative experiences while browsing a website, for example a link is broken, or there is a negative review or inaccurate information, some causes will be inferred from the negative cues. Therefore, we propose negative website features could evoke users' negative evaluation of website attributes, like malevolence or incompetence.

3.2.1 *Lack of Structural Assurance*

Structural assurance indicates the web environment. Rotter's (1982) social learning theory holds that behavior predictions are a result of interaction between the environment and internal factors. Thus, environment is very important for predictions concerning a website. Structural assurance reduces internet risk by employing some security technologies (Grazioli 2004). Accordingly, lack of structural assurance suggests the environment is relatively risky or dangerous. The lack of security technologies would cause users to question the motive or ability of a website. Two possible reasons are inferred, either because of the website's incapability to evolve the technology, or because of the website intentionally failing to follow privacy and security policies. Therefore, we hypothesize:

H3a: Perception of lack of structural assurance is positively associated with perceived malevolence of a website.

H3a: Perception of lack of structural assurance is positively associated with perceived incompetence of a website.

3.2.2 *Interface Design*

As fraud and deception online have become increasingly pervasive, impacting on hundreds of thousands of internet users and even generating billions of dollars of loss (Abbasi et al. 2010), internet users have become more sensitive to poor quality websites. Interface design is regarded as one important factor indicating website quality (Huizingh 2000; Ranganathan and Ganapathy 2002; Aladwani and Palvia 2002). Mavlanova (2010) noted that imperfections in website quality could provide strong cues about malicious intention to the website user. Moreover, interface design can lead to positive perceptions of quality, whether in terms of information, system or service (Cenfetelli 2004). In other words, interface design are necessary conditions to ensure a website's competence. Incompetence will be assumed if these necessary conditions are removed. In summary, poor interface design will provoke user's perception of malevolence and incompetence of website. Therefore, we hypothesize:

H4a: Interface design is positively associated with perceived malevolence of a website.

H4b: Interface design is positively associated with perceived incompetence of a website.

3.2.3 *Lack of Third-party Recognition*

Reputation represents the judgment of from others. Third-party recognition represents a website's reputation, including endorsement, reward and credentials or other certificates (Lee and Turban 2001), while lack of third-party recognition implies a lack of such features. As the internet becomes more

mature, most approved websites are recognized by reputable third-parties, so that reputable third-party recognition has become a criterion to judge of a website. When a user encounters a website without any such recognition, specific causes will be attributed to this lack, such as the possibility that the website is intentionally questioned by reputable parties, or the website is not sufficiently capable to attract support from reputable parties. Therefore, we hypothesize:

H5a: Perception of lack of third-party recognition is positively associated with perceived malevolence of a website.

H5b: Perception of lack of third-party recognition is positively associated with perceived incompetence of a website.

3.3 Control Variable: Irrational Distrust - Suspicion of Humanity

Suspicion of humanity is adopted as the control variable in our research model. Although it is not the focus of this research, since personal characteristics are one category of distrust determinants, the potential influence of this factor on the model is controlled, and thus included in the full model. Suspicion of humanity is one dimension of distrust propensity, and is believed to influence the formation of distrust (McKnight et al. 2004).

4 METHODOLOGY

4.1 Measurement

The instruments for most constructs were adapted from previous studies, while measure of interface design was self-developed from the summary of website design features and fake website features (Abbasi et al. 2010; Zhang and Von Dran 2000), and measures of lack of structural assurance, lack of third-party recognition, and incompetence were the negative counterparts of the measures of structural assurance, third-party recognition, and competence (McKnight and Choudhury 2006; McKnight et al. 2003; Ou and Sia 2010), with some modification according to their definitions, as shown in table 2. The validity of these self-developed and modified constructs was checked through card sorting.

Construct	Item	Measure	Source
Lack of Structural Assurance	LSA1	This website does not have enough safeguards to make me feel comfortable when I am using it.	Negative counterpart measures based on McKnight (2006)
	LSA2	I feel worried that there aren't enough legal structures to adequately protect me from problems on this site.	
	LSA3	I fear that strong enough technological protections do not exist on this website for me to feel safe.	
Interface Design	ID1	This website has poor design, containing inappropriate use of color, fonts and graphics.	New measurements based on Abbasi et al. (2010); Zhang et al. (2000)
	ID2	The website's design makes it difficult to find the desired information.	
	ID3	This website has an illogical layout.	
Lack of Third-party Recognition	LPA1	This website is not recognized by well-known, reputable third parties (e.g., portal, certificate, testimonial, etc.)	Negative counterpart measures based on Ou (2010)
	LPA2	There are no reputable third-party bodies assuring interactions with this website.	
	LPA3	Existing third-party recognition for this website is insufficient.	
Malevolence	MAL1	I believe this website is interested only in its own interests, not mine, and even bears ill will.	Adapted from Dimoka (2010)
	MAL2	I believe this website will engage in harmful behavior towards me.	
	MAL3	I believe this website will perform in a fraudulent way.	
	MAL4	I believe that the website does not have good intentions towards its customers.	

Incompetence	INA1	I think this website is incompetent in providing its service.	Negative counterpart measures based on McKnight (2003)
	INA2	I think this website does not perform its role of providing service very well.	
	INA3	I think this website is inept.	
	INA4	This website does not seem to be knowledgeable.	
	INA5	This website does not seem capable to me.	
Distrust	DIST1	I think this website seems untrustworthy.	Adapted from Ou (2010)
	DIST2	I feel nervous relying on this website.	
	DIST3	I must be very watchful and wary when dealing with this website.	
	DIST4	I am fearful of dealing with this website.	
	DIST5	I feel that I cannot depend on this website.	
Suspicion of Humanity	SH1	People are usually out for their own good.	Adapted from Mcknight et al. (2004)
	SH2	People pretend to care more about one another than they really do.	
	SH3	Most people inwardly dislike putting themselves out to help other people.	
	SH4	Most people would tell a lie if they could gain by it.	
	SH5	People don't always hold to the standard of honesty they claim.	
	SH6	Most people would cheat on their income tax if they thought they could get away with it.	

Table 2. Measurement of Constructs

4.2 Data Collection

Considering that distrust matters in a risky and uncertain environment, and a potential loss situation is more likely to trigger distrust (McKnight and Chervany 2001), an online bookstore new to users was chosen as the website for our survey. In order to improve participant involvement and ensure recognition of some negative features, some tasks were assigned to the subjects before completion of the questionnaire. These tasks are steps that online consumers usually follow when they conduct purchases.

The data were collected from an online survey related services website - SOJUMP, whose sample comes from website partners, search engine, blog/forum recruitment, members' recommendation, and persons who filled in questionnaires before covering all range of ages and working groups. The questionnaires were randomly distributed to the whole sample pool through email by SOJUMP. 15 RMB was provided for each response as an incentive, increasing motivation, and thus the credibility of the responses.

5 DATA ANALYSIS AND RESULTS

5.1 Subjects

283 responses were obtained in all. 55.5% of the participants were female and most of their ages ranged from 21 to 40. Over 98% held at least a two-year college degree. More than 90% of the participants spent more than one hour per week browsing various websites.

5.2 Measurement Model – Reliability and Validity

Partial Least Squares (PLS) was used to test the measures and hypotheses, because PLS is able to examine measurements and structural models simultaneously and work with relatively small samples (Chin et al. 2003).

Reliability and convergent validity were assessed by examining Cronbach's alpha, composite reliability (CR) and average variance extracted (AVE) (Hair et al. 1998), as shown in Table 3. The threshold values for Cronbach's alpha, CR and AVE are 0.70, 0.70 and 0.50, respectively (Chin et al. 2003). As the table illustrates, the Croncach's alpha and CR of all the constructs are above 0.80: the AVE of most

constructs is above 0.8, except for suspicion of humanity, with values of 0.512. These results confirm the good reliability of the measurement model.

Constructs	Item	Loading	AVE	Composite Reliability	Cronbachs Alpha
Distrust	DIST1	0.887	0.802	0.953	0.938
	DIST2	0.891			
	DIST3	0.871			
	DIST4	0.896			
	DIST5	0.931			
Incompetence	INA1	0.874	0.828	0.960	0.948
	INA2	0.909			
	INA3	0.926			
	INA4	0.926			
	INA5	0.912			
Lack of Structural Assurance	LSA1	0.905	0.832	0.937	0.899
	LSA2	0.931			
	LSA3	0.901			
Lack of Third-party Recognition	LPA1	0.928	0.836	0.939	0.902
	LPA2	0.930			
	LPA3	0.885			
Malevolence	MAL1	0.909	0.845	0.956	0.939
	MAL2	0.914			
	MAL3	0.920			
	MAL4	0.934			
Suspicion of Humanity	SH1	0.545	0.512	0.859	0.828
	SH2	0.869			
	SH3	0.836			
	SH4	0.794			
	SH5	0.639			
	SH6	0.533			

Table 3. Reliability and Convergent Validity.

Discriminant validity of constructs may be estimated by checking whether the square roots of the AVE are higher than the correlations involving the construct (Fornell and Larcker 1981). In this study, all the square roots of the AVEs of all the reflective constructs are higher than 0.9, as shown in Table 4. Although some of the variable intercorrelations are quite high, the items demonstrated satisfactory discriminant validity (Wixom and Todd 2005). In all cases, the square roots of the AVE for each construct are larger than the correlations of that construct with all other constructs in the research model.

Constructs	Distrust	Incompetence	Interface design	Lack of structural assurance	Lack of third-party recognition	Malevolence	Suspicion of humanity
Distrust	0.895						
Incompetence	0.721	0.910					
Interface design	0.543	0.611	NA*				
Lack of structural assurance	0.717	0.675	0.515	0.912			
Lack of third-party recognition	0.569	0.553	0.410	0.569	0.915		
Malevolence	0.765	0.628	0.509	0.595	0.430	0.919	
Suspicion of humanity	0.104	0.092	0.065	0.063	0.171	0.029	0.716

* AVE is not applicable for formative construct.

Table 4. Discriminant Validity (Diagonal elements are square roots of the average variance extracted).

5.3 Structure Model

Overall, the SmartPLS results support the theoretical model. Figure 2 shows that two website attributes, malevolence ($\beta=0.518$, $t=10.094$) and incompetence ($\beta=0.390$, $t=7.755$), were found to have significant effects on distrust. As for the website factors, most of them had a significant relationship with malevolence and incompetence. Institution-based factor, lack of structural assurance exerted significant positive effects on malevolence ($\beta=0.410$, $t=6.283$) and incompetence ($\beta=0.396$, $t=6.469$). Quality-based factor, interface design significantly affects malevolence ($\beta=0.261$, $t=4.058$) and incompetence ($\beta=0.328$, $t=5.709$). Reputation-based factor, lack of third party was proved to influence incompetence significantly ($\beta=0.193$, $t=3.404$), but not for malevolence ($\beta=0.090$, $t=1.493$). In summary, only one of the hypotheses was not supported by the data. The control variable, suspicion of humanity did not have a significant effect on distrust.

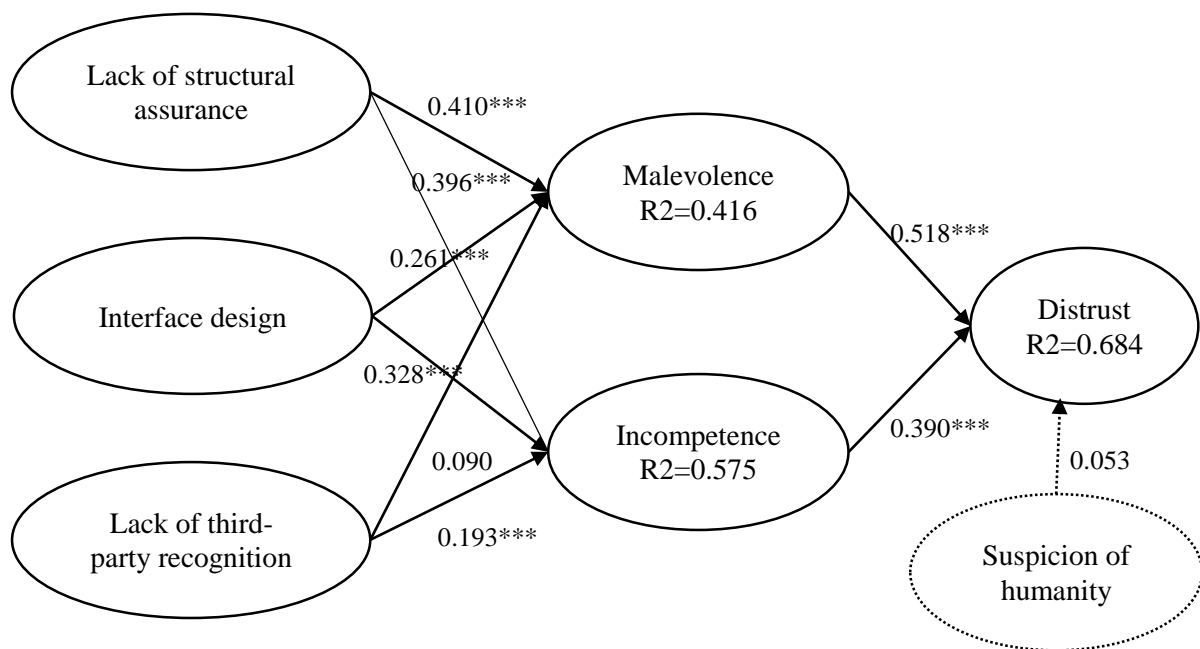


Figure 2. Results of Structural Model

6 DISCUSSION AND IMPLICATION

6.1 Discussion

H1 and H2 are significantly supported, indicating that perceptions of website malevolence and incompetence have a strong effect on a user's distrust of the website. A user has negative expectations of an incompetent website, because it does not have the ability to do for the user what s/he needs done. A website of malicious intention towards users may cause financial loss, steal private information, induce the purchase of unwanted goods, etc. Users will not allow themselves to become vulnerable to such a website to prevent negative outcomes. Therefore, as the review of distrust literature suggested, certain attributes of a website, namely malevolence and incompetence are two main antecedents of distrust in the website.

The empirical evidence also shows that the three categories of website factors strongly influence user perceptions of website attributes, although one of the hypotheses is not significantly supported (H5a). The results of H3 and H4 supported indicate that users regard the website of lack of structural assurance or poor interface design as malevolence or incompetence, which then trigger the distrust in it. The relationship between lack of third-party recognition and incompetence is also significant, while the

relationship between lack of third-party recognition and malevolence is not significant, which means that users only treat the website of lack of third-party recognition as incompetence rather than malevolence. Specifically, the website without third-party would not give rise to the attribution of ill intention. There is evidence for this argument. McKnight (2003) theorized that endorsement by a professional party would promote high competence belief.

6.2 Limitation and Future Study

There are several limitations for our research. First, this study may have limited generalizability, because of the regional data used, the website selected and/or the tasks assigned. Second, limit website factors are measured on a single website. We can include more website features in future study. Third, an online survey was used as the method to collect data. One often cited disadvantage of self-reported surveys is the threat of common method bias (Malhotra et al. 2006). In future, other methods should be employed to broaden this research.

6.3 Implications

There are some theoretical implications. First, the current research innovatively develops a distrust formation model in the online context. The research model provides clear knowledge of the way in which distrust is formed online. Second, this research advances understanding of the relationship between website features and distrust. Website factors are demonstrated to have indirect impacts on distrust in this research. They automatically evoke user evaluations of website attributes, rather than leading to distrust directly. Third, this research extends understanding of the antecedents of distrust. From the review of distrust literature, we divide distrust determinants into four categories.

This research makes a significant practical contribution. Knowing that distrust and trust have different antecedents is necessary for website designers and owners. It implies that a strategy of building trust is not sufficient, because merely enhancing the antecedents of trust will not decrease user distrust. When the importance of distrust is recognized, website designers will pay more attention to the website factors that induce user distrust. Understanding and eliminating such factors would help website designers to minimize user distrust. Moreover, the distrust generation process is unfolded in our study, by explaining how users interpret the website factors, and which perception of website attributes are evoked accordingly. Knowing how a user interprets website factors is also beneficial for website designers. For example, if a website designer or owner finds that users regard the website as incompetent because of some website factors, s/he should firstly eliminate the factors leading to incompetence. S/he could then enhance the factors that could increase user perceptions of competence, rather than other positive factors, such as those related to benevolence or integrity.

References

- Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker, J. J. F. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory. *MIS Quarterly*, 34 (3), 435-461.
- Adams, J. E., Highhouse, S., and Zickar, M. J. (2010). Understanding General Distrust of Corporations. *Corporate Reputation Review*, 13 (1), 38-51.
- Aladwani, A., and Palvia, P. (2002). Developing and Validating an Instrument for Measuring User-Perceived Web Quality. *Information & Management*, 39 (6), 467-476.
- Awad, N. F., and Ragowsky, A. (2008). Establishing Trust in Electronic Commerce through Online Word of Mouth: An Examination across Genders. *Journal of Management Information Systems*, 24 (4), 101-121.
- Baba, M. L. (1999). Dangerous Liaisons: Trust, Distrust, and Information Technology in American Work Organizations. *Human Organization*, 58 (3), 331-346.
- Barber, K. S., Fullam, K., and Kim, J. (2003). Challenges for Trust, Fraud and Deception Research in Multi-Agent Systems. *Trust, Reputation, and Security: Theories and Practice*, 8-14.
- Barnett, M. L. (2008). An Attention-Based View of Real Options Reasoning. *Academy of Management Review*, 33 (3), 606-628.
- Benamati, J. S., Serva, M. A., and Fuller, M. A. (2010). The Productive Tension of Trust and Tistrust: The Coexistence and Relative Role of Trust and Distrust in Online Banking. *Journal of Organizational Computing and Electronic Commerce*, 20 (4), 328-346.
- Bigley, G., and Pearce, J. (1998). Straining for Shared Meaning in Organization Science: Problems of Trust and Distrust. *Academy of Management Review*, 23 (3), 405-421.
- Cenfetelli, R. T. (2004). Inhibitors and Enablers as Dual Factor Concepts in Technology Usage. *Journal of the Association for Information Systems*, 5 (11/12), 472-492.
- Chin, W. W., Marcolin, B. L., and Newsted, P. R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research*, 14 (2), 189-217.
- Cho, J. (2006). The Mechanism of Trust and Distrust Formation and Their Relational Outcomes. *Journal of Retailing*, 82 (1), 25-35.
- Cho, J. E. (2007). The Effects of Trust/Distrust on Information Privacy Concerns (Ipc) and the Moderating Roles of Individual Propersities. *International Journal of Business Research*, 7 (3), 107-115.
- Chopra, K., and Wallace, W. A. (2003). Trust in Electronic Environments. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences IEEE*.
- Darke, P. R., and Ritchie, R. J. (2007). The Defensive Consumer: Advertising Deception, Defensive Processing, and Distrust. *Journal of Marketing Research*, 44 (1), 114-127.
- Deutsch, M. (1958). Trust and Suspicion. *Journal of Conflict Resolution*, 2 (4), 265-279.
- Deutsch, M. (1960). The Effect of Motivational Orientation Upon Trust and Suspicion. *Human Relations*, 13 (2), 123-139.
- Dimoka, A. (2010). What Does the Brain Tell Us About Trust and Distrust? Evidence from a Functional Neuroimagine Study. *MIS Quarterly*, 34 (2), 373-396.
- Ethier, J., Hadaya, P., Talbot, J., and Cadieux, J. (2008). Interface Design and Emotions Experienced on B2c Web Sites: Empirical Testing of a Research Model. *Computers in Human Behavior*, 24 (6), 2771-2791.
- Fein, S., and Hilton, J. (1994). Judging Others in the Shadow of Suspicion. *Motivation and Emotion*, 18 (2), 167-198.
- Fornell, C., and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18 (1), 39-50.
- Gefen, D., Benbasat, I., and Pavlou, P. A. (2008). A Research Agenda for Trust in Online Environments. *Journal of Management Information Systems*, 24 (4), 275-286.

- Gefen, D., Karahanna, E., and Straub, D. W. (2003). Trust and Tam in Online Shopping: An Integrated Model. *MIS Quarterly*, 27 (1), 51-90.
- Gillespie, N. and Dietz, G. (2009). Trust Repair after an Organization-Level Failure. *Academy of Management Review*, 34 (1), 127-145.
- Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet. *Group Decision and Negotiation*, 13 (2), 149-172.
- Grazioli, S. and Jarvenpaa, S. L. (2003). Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence. *International Journal of Electronic Commerce*, 7 (4), 93-118.
- Gruen, T., Osmonbekov, T., and Czaplewski, A. (2006). Ewom: The Impact of Customer-to-Customer Online Know-How Exchange on Customer Value and Loyalty. *Journal of Business Research*, 59 (4), 449-456.
- Hair, J. F., Anderson, R. E., Tatham, R. L., and William, C. (1998). *Multivariate Data Analysis*. Upper Saddle River, NJ, Prentice Hall.
- Hsiao, R. (2003). Technology Fears: Distrust and Cultural Persistence in Electronic Marketplace Adoption. *The Journal of Strategic Information Systems*, 12 (3), 169-199.
- Huizingh, E. K. (2000). The Content and Design of Web Sites: An Empirical Study. *Information & Management*, 37 (3), 123-134.
- Jarvenpaa, S. L., Knoll, K., and Leidner, D. E. (1998). Is Anybody out There? Antecedents of Trust in Global Virtual Teams. *Journal of Management Information Systems*, 14 (4), 29-64.
- Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication*, 5 (2).
- Kee, H. W., and Knox, R. E. (1970). Conceptual and Methodological Considerations in the Study of Trust and Suspicion. *Journal of Conflict Resolution*, 14 (3), 357-366.
- Kelley, H. H., and Michela, J. L. (1980). Attribution Theory and Research. *Annual Review of Psychology*, 31(1), 457-501.
- Keyton, J. and Smith, F. (2003). A Comparative Empirical Analysis of Theoretical Formulations of Distrust. 16th Annual IACM Conference Melbourne, Australia.
- Komiak, S. and Benbasat, I. (2008). A Two-Process View of Trust and Distrust Building in Recommendation Agents: A Process-Tracing Study. *Journal of the Association for Information Systems*, 9 (12), 727-747.
- Komiak, S. Y. X. and Benbasat, I. (2006). The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. *MIS Quarterly*, 30 (4), 941-960.
- Kramer, R. (1994). The Sinister Attribution Error: Paranoid Cognition and Collective Distrust in Organizations. *Motivation and Emotion*, 18 (2), 199-230.
- Kramer, R. (1999). Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. *Annual Review of Psychology*, 50, 569-598.
- Kramer, R. (2001). Trust Rules for Trust Dilemmas: How Decision Makers Think and Act in the Shadow of Doubt. *Trust in Cyber-Societies*, 9-26.
- Kramer, R. M. and Cook, K. S. (2004). *Trust and Distrust in Organizations: Dilemmas and Approaches*. Russell Sage Foundation Publications.
- Laczniak, R. N., DeCarlo, T. E., and Ramaswami, S. N. (2001). Consumers' Responses to Negative Word-of-Mouth Communication: An Attribution Theory Perspective. *Journal of Consumer Psychology*, 11 (1), 57-73.
- Lee, M. and Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, 6 (1), 75-91.
- Lewicki, R., McAllister, D., and Bies, R. (1998). Trust and Distrust: New Relationships and Realities. *Academy of Management Review*, 23 (3), 438-458.
- Lewicki, R. and Tomlinson, E. (2003). The Effects of Reputation and Post Violation Communication on Trust and Distrust. 16th Annual IACM Conference, p. 28, Melbourne, Australia.

- Lim, K., Sia, C., Lee, M., and Benbasat, I. (2006). Do I Trust You Online, and If So, Will I Buy? An Empirical Study of Two Trust-Building Strategies. *Journal of Management Information Systems*, 23 (2), 233-266.
- Marsh, S. and Dibben, M. (2005). Trust, Untrust, Distrust and Mistrust - an Exploration of the Dark (Er) Side. *Trust Management*, 34(77), 17-33.
- Mavlanova, T. and Benbunan-Fich, R. (2010). Counterfeit Products on the Internet: The Role of Seller-Level and Product-Level Information. *International Journal of Electronic Commerce*, 15 (2), 79-104.
- Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20 (3), 709-734.
- McAllister, D. (1995). Affect-and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *Academy of management journal*, 38 (1), 24-59.
- McKnight, D. and Chervany, N. (2001). Trust and Distrust Definitions: One Bite at a Time. *Trust in Cyber-Societies*. R. Falcone, M. Singh and Y.-H. Tan (eds.). Springer Berlin / Heidelberg, 27-54.
- McKnight, D. and Choudhury, V. (2006). Distrust and Trust in B2c E-Commerce: Do They Differ? *Proceedings of the 8th international conference on Electronic commerce: ACM*, 482-491.
- McKnight, D., Choudhury, V., and Kacmar, C. (2002). The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model. *Journal of Strategic Information Systems*, 11 (3-4), 297-323.
- McKnight, D., Choudhury, V., and Kacmar, C. (2003). Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Information Systems Research*, 13 (3), 334-359.
- McKnight, D., Kacmar, C., and Choudhury, V. (2004). Dispositional Trust and Distrust Distinctions in Predicting High-and Low-Risk Internet Expert Advice Site Perceptions. *E-Service*, 3 (2), 35-58.
- Mizerski, R. W. (1982). An Attribution Explanation of the Disproportionate Influence of Unfavorable Information. *Journal of Consumer Research*, 9 (3), 301-310.
- Ou, C. X. and Sia, C. L. (2010). Consumer Trust and Distrust: An Issue of Website Design. *International Journal of Human-Computer Studies*, 68 (12), 913-934.
- Ranganathan, C. and Ganapathy, S. (2002). Key Dimensions of Business-to-Consumer Web Sites. *Information & Management*, 39 (6), 457-465.
- Richins, M. L. (1984). Word-of-Mouth Communication as Negative Information. *Advances in consumer research*, 11 (1), 697-702.
- Ridings, C., Gefen, D., and Arinze, B. (2002). Some Antecedents and Effects of Trust in Virtual Communities. *The Journal of Strategic Information Systems*, 11 (3-4), 271-295.
- Riedl, R., Hubert, M., and Kenning, P. (2010). Are There Neural Gender Differences in Online Trust? An Fmri Study on the Perceived Trustworthiness of Ebay Offers. *MIS Quarterly*, 34 (2), 397-428.
- Rosalind H. Searle, K. S. B. (2004). The Development of Trust and Distrust in a Merger. *Journal of Managerial Psychology*, 19 (7), 708 - 721.
- Rotter, J. B. (1982). Social Learning Theory. *Expectations and Actions: Expectancy-Value Models in Psychology*, 241-260.
- Schul, Y., Mayo, R., and Burnstein, E. (2008). The Value of Distrust. *Journal of Experimental Social Psychology*, 44 (5), 1293-1302.
- Sitkin, S. and Roth, N. (1993). Explaining the Limited Effectiveness of Legalistic" Remedies" for Trust/Distrust. *Organization Science*, 4 (3), 367-392.
- Tullberg, J. (2008). Trust--the Importance of Trustfulness Versus Trustworthiness. *Journal of Socio-Economics*, 37 (5), 2059-2071.
- Ullmann-Margalit, E. (2004). *Trust, Distrust, and in Between*. New York: Russell Sage Foundation.
- Wixom, B. H. and Todd, P. A. (2005). A Theoretical Integration of User Satisfaction and Technology Acceptance. *Information Systems Research*, 16 (1), 85-102.

- Xiao, B., and Benbasat, I. (2011). Product-Related Deception in E-Commerce: A Theoretical Perspective. *MIS Quarterly*, 35 (1), 169-196.
- Xu, G., Feng, Z., Wu, H., and Zhao, D. (2007). Swift Trust in a Virtual Temporary System: A Model Based on the Dempster-Shafer Theory of Belief Functions. *International Journal of Electronic Commerce*, 12 (1), 93-126.
- Yang, Z., Cai, S., Zhou, Z., and Zhou, N. (2005). Development and Validation of an Instrument to Measure User Perceived Service Quality of Information Presenting Web Portals. *Information & Management*, 42 (4), 575-589.
- Zhang, P., and Von Dran, G. M. (2000). Satisfiers and Dissatisfiers: A Two-Factor Model for Website Design and Evaluation. *Journal of the American society for information science*, 51 (14), 1253-1268.