Wageningen University - Department of Social Sciences

Chair Group: Marketing and Consumer Behaviour

The Effects of Trust and Distrust on Privacy Risk Perception

December 2014

MSc program: Management, Economics and Consumer Studies

Specialization: Consumer Studies

Written by: Michael Scheen (870822-732-130)

Supervised by: Dr. Andres Trujillo Barrera

Thesis code: MCB-80433

General Data

Student	Michael Scheen
Student registration number	870822-732-130
Email addresses	michael.scheen@wur.nl kl_Scheen@hotmail.com
Study program	MSc: Management, Economics and Consumer Studies (MME)
Specialisation	Consumer Studies
Course	MCB-80433 – MSc Thesis Marketing and Consumer Behaviour
Main supervisor	Dr. Andres Trujillo Barrera
Second Supervisor	Dr. Arnout Fischer
Date	December 19, 2014
Location	Wageningen, The Netherlands

Acknowledgements

Foremost, I would like to thank my thesis advisor Andres Trujillo Barrera, for his patience, motivation and reassuring words. Besides my advisor, I would like to thank the rest of my thesis committee: Arnout Fischer, Ynte van Dam and Prof. Hans van Trijp. My sincere thanks also go to Dr. Holger Steinmetz from Paderborn University, who freely shared his R-code with me and took time to engage in a discussion. I thank my family for empathy and support throughout my studies. Last but not least, I would like to express my sincere gratitude to my beloved girlfriend Lina for her sympathy, encouragement and well-meant distraction.

Abstract

The lack of trust in information privacy practices has been identified as a central problem hindering the adoption of e-commerce. Although distrust has been introduced as a distinct entity from trust a while ago, few privacy scholars have incorporated distrust in their research. Drawing on the conceptual work of Sitkin and Roth (1993), the current study proposes a mechanism by which trust and distrust influence consumers' privacy concerns and manifest their privacy risk perception. The proposed relationships are tested in the context of e-banking, using structural equation modelling. In line with previous findings, evidence was found that privacy concerns increase privacy risk perception. The proposed concern distinction according to responsiveness to task-reliability and value-orientation was not supported by the data. Interestingly, results illustrate that trust's and distrust's impact on privacy concern dimensions differs greatly in impact and valence. They also indicate that trust and distrust affect mostly those concern dimensions that are associated with exogenous uncertainty. Implications of these findings are discussed in the paper.

Keywords: Distrust, Trust, Privacy, Privacy Concerns, Risk Perception, e-Banking, e-Commerce Adoption

Contents

List of Figures

List of Tables

List of Abbreviations

AVE	Average variance extracted
CFA	Confirmatory factor analysis
CFI	Comparative fit index
CFP	Concerns for privacy
CR	Composite reliability
ML	Maximum likelihood estimator
MLM	Maximum likelihood estimator with robust standard errors and a Satorra-Bentler scaled test statistic
PCA	Principal component analysis
RMSEA	Root mean square error of approximation
SEM	Structural equation modelling
SRMR	Standardized root mean square residual
TLI	Tucker lewis index
WUR	Wageningen University

1. Introduction

1.1. Background of the Present Study

With the start of the commercial internet in the early 90's, most industries reached out to consumers worldwide, using the internet to offer rapid and flexible data exchange and business processes. This application of the internet technology has soon become to be known as e-commerce. (Omariba et al., 2012) Recognising the value of the data that accompanied these processes, organizations established the first online databases (Hiranandani, 2011). Today, with the ever-growing flood of information and the advances in the computation of large data-sets, organisations aim to base all decisions on the analysis of real data (Jagadish et al., 2011).

This alluring objective, however, comes along with concerns for privacy. Some concerns are associated with the security of the internet-system in which the information exchange takes place. With its strong reliance on technology, e-commerce introduced countless ways to unlawfully intrude transferred or stored information for opportunistic purposes (Dinev et al., 2008; Mendez, 2005). Other concerns relate to aspects more inherent in the exchange of data, namely the amount of collected data and the subsequent use of it. The more numerous and extensive the data sources become, the more difficult it is to ensure anonymity and accuracy of the data (Zimmer, 2008; Jagadish et al., 2011). Moreover, whilst most consumers are unaware of the numerous applications of personal data, they do certainly not intent to give an unlimited permission to use it (Boyd & Crawford, 2012). Even if they agree to certain terms, they might find themselves unable to verify the compliance with their agreements, as they lose almost all control over the disclosed content once it has left their own computers (Liao, 2011). No matter where privacy intrusions have their seeds, they can entail various kinds of losses for the sender, including losses of money, time, self-esteem or social-reputation (Lim, 2003). Sensing these threats, consumers might perceive e-commerce as risky and refrain from its adoption.

Attempting to encourage e-commerce adoption, various scholars have focussed on trust (Grabner-Kräuter & Kaluscha, 2003). Trust is important when it is difficult to fully regulate business agreements and where it is consequently necessary to rely on the other party not to take unfair advantage of this situation (Deutsch, 1960). From the consumers' point of view, e-commerce is such a situation. Its use is characterized by an obligation to disclose personal information and a concurrent absence of the ability to fully control or predict the outcomes of

the disclosure. Instead, it is mainly the accuracy, the competence and the sincerity of the receiver that determines the secrecy of consumers' personal information. As there is little guarantee that the receiver will refrain from undesirable or opportunistic behaviour, consumers' trust is a central element in e-commerce. (Omariba et al., 2012)

Most scholars, who attest the importance of trust in this context, implicitly assume that distrust is simply an expression of low trust and vice versa (Lewicki et al., 1998). However, some researchers challenge this assumption (e.g. Lewicki et al., 1998; McKnight & Chervany, 2001; Sitkin & Roth, 1993). Instead, they point out that distrust may be a distinct, but functional equivalent construct of trust. This implies that both constructs have independent determinants and effects. If trust and distrust are indeed separate, efforts to build trust do not necessarily diminish distrust. Moreover, outcomes hindered by high distrust might not be supported by enhancing trust and vice versa (Lewicki et al., 1998). Yet the conceptual distinction of both constructs and their impact are not sufficiently explored in the e-commerce literature.

This study advances the understanding in this regard. It ties in with Sitkin and Roth's (1993) suggestion that trust relates to assumed task reliability, while distrust is based on perceived value-incongruence. It aims to find an answer to the question "How do trust and distrust influence consumers' privacy risk perception?" The study may have important managerial implications, because today, companies make mainly trust-building efforts. In order to accurately manage consumers' privacy risk perception in e-commerce situations, they may need to reconsider their strategy and tackle distrust issues separately. (Cho, 2006) By exploring the nature and the effects of trust and distrust, this study contributes to a profound understanding, which is necessary for the development of such strategies.

The phenomenon is investigated in the context of banking. In process of their services, banks acquire exclusive information about their clients' lending and transfer history. Tapping directly into financial matters and alluding to someone's wants, habits and preferences in a long period of time, the revelation of this sensitive information is likely to be associated with risk feelings. (Omariba et al., 2012) Some characteristics of electronic banking, such as the extensive use of technology, the impersonal nature of the online environment and the uncertainty entailed in using an open technological infrastructure, make it arguably riskier than face to face interactions. (Omariba et al., 2012) Also, due to the lack of direct insight on banks' mostly intangible services and practices, consumers are likely to consult trust and distrust when forming their risk perception (Bravo et al., 2012; Adams et al., 2010).

1.2. Structure of the Present Study

The organisation of this paper is as follows. Firstly, Chapter 2 introduces the reader to the concepts of risk (perception), privacy, privacy concerns, trust and distrust. The discussion of these definitional issues serves as foundation to move into the construction of a research model. Here, the different concepts are interlinked and a number of hypotheses are derived that concern these linkages. Chapter 3 then clarifies how the former considerations are tested empirically. The research context, the measurements as well as the process of data collection and analysis are described in detail. Chapter 4 discusses the results of the empirical investigation. Finally, Chapter 5 addresses research limitations and suggests research topics for the future.

2. Theoretical Foundation

2.1. Privacy Risk Perception in Online Environments

2.1.1. The Concept of Risk and Risk Perception in Online Environments

Likewise applied by researchers, professionals and lay people, risk is a concept, which holds many meanings. According to Möller et al. (2006), risk can be defined as:

- an *unwanted event* which may or may not occur,
- the *cause* of an unwanted event which may or may not occur,
- or the *probability* of an unwanted event which may or may not occur.

The inclusion of both, probability and unwanted event is helpful to envision the richness of the risk concept. First, it helps us to understand that risk consists of a cognitive and an affective aspect. The cognitive aspect relates to the probability estimation about the occurrence of an event. The affective aspect relates to the emotional evaluation of this occurrence (Nickel & Vaesen, 2012). Second, risk is construed (Sjöberg, 2000) and comprises a timely dimension, because it relates to possible outcomes in the future. Third, probability points towards uncertainty. One perceives risk, because she/he faces uncertainty about potentially undesirable outcomes triggered by decisions (Lim, 2003).

Risks differ from hazards in the sense that the undesirable outcome has not yet manifests itself in reality. While hazards demand for a reaction on the inevitable, risks still incorporate choice and the chance of avoidance. As human beings naturally strive to avoid negative outcomes (Frewer, 1999), researchers and policy makers came to realize that an understanding of risk is crucial to guide and understand human behaviour.

However, experts quickly recognized that behaviour in risky situations is not just based on technical risk estimates, but also on the subjective perception of risk. (Sjöberg, 2000; Frewer, 1999) Technological innovations, such as the internet, are no exceptions. Although every new technology comes with its proper benefits, the public often remains sceptical, suspecting unknown, potentially undesirable consequences (Sjöberg & Fromm, 2001). Advocates of today's information technologies present them as useful tools to enhance social connection and security, while their opponents perceive them as restricting invasive and dangerous (Hiranandani, 2011). To account for these subjective differences, risk debate partly shifted its

focus from risk estimates towards risk perception. Risk perception can be defined as someone's mental representation of risk (Nickel & Vaesen, 2012).

2.1.2. Privacy Intrusion as (Perceived) Risk in Online Environments

The Oxford dictionary defines privacy as a "state in which one is not observed or disturbed by other people" (Oxforddictionaries.com, 22.04.2014). The definition as a state has been part of a dichotomous conceptualization of information privacy, where anonymity and intimacy lay at the ends of a continuum and people strive to reach and maintain anonymity (Smith et al., 2011). Others include a notion of action to the concept, defining it as a protection of a personal realm from unreasonable intrusion (Patton, 2000). This proactive characteristic relates to central aspect of privacy, namely self-determination and control (Keith et al., 2013). Most scholars perceive the *right* for privacy as a mean, which provides individuals with the ability or the right to control information related to their personal life (Hiranandani, 2011). Of course, this control is not unlimited. Words such as "unauthorised" or "unreasonable" emphasise that privacy comprises a normative aspect. The control one is meant to exert is bound to a judgement about right and wrong. It is the result of societal negotiation that defines an intangible space in which control about personal information can be rightfully claimed. This space defines one's informational belongings, contrasts them with the outside world and links them to the expectation that they are left alone by the outside.

Compliance with this expectation, however, cannot be taken for granted. There is always a risk that third parties engage in undesired, even malicious behaviour that intrudes privacy (Hiranandani, 2011). Technological advances in surveillance, data gathering and information storage techniques have manifold privacy threats and increased the concerns about privacy violations (Junglas, 2008). Given that a whole branch of industry now collects and sells information for commercial purposes (Hiranandani, 2011), it is important to note that privacy invasion does not just refer to an act, where information is unwillingly taken away from individuals. It also applies to acts, where personal information is misused after it has been legitimately obtained in course of legal exchange. This detail might remain unnoticed in many definitions, describing privacy as, for instance, a freedom from unauthorized intrusion (Stone et al., 1983). I therefore adopt the more sophisticated definition from Xu and Teo (2004) that gives sufficient consideration to the new possibilities emerging from technological progress. They see privacy as a right or as an ability to control how information is collected, retained and/or maintained, used and communicated, disclosed or shared (Xu & Teo, 2004).

Even though several marketing, policy and computer-science studies focus on the relation between privacy and risk perception, the studies where privacy risk was examined in detail are rather limited. Instead, most studies measure risk perception in a general fashion. The few studies, which distinguish privacy risk perception from general risk perception, mention it briefly, but do not conceptualize the construct precisely. Those, who do, differ greatly, depending on their area of application. (Featherman et al., 2010)

For example, Lim (2003) defines perceived privacy risk as "the possibility that online businesses collect data about individuals and use them inappropriately" (p. 219). Even though she acknowledges that privacy can be threatened by the internet vendors and by hackers, her definition specifies online businesses as the only actors involved in privacy risks. This paper adopts the perspective of Malhotra et al. (2004), where perceived privacy risk is defined as "the expectation that a high potential for loss is associated with the release of personal information to the firm" (p. 341).

2.1.3. Privacy-related Sources of Uncertainty and Reasons to Worry

Actual risk incorporates uncertainty about the occurrence of unwanted future outcomes (Nickel & Vaesen, 2012). The exchange of information via open technological infrastructures is accompanied with a diminishment of control over the disclosed content and is therefore associated with high levels of uncertainty (Liao, 2011). This uncertainty can result from the following two sources:

- *Endogenous uncertainty* refers to outcomes, which result from decisions made by actors involved in the exchange process. They are caused by asymmetric distribution of information or opposing goals between these actors.
- *Exogenous uncertainty* refers to outcomes, which result from the complexity of environmental factors that cannot be avoided by agreements with the actors. In e-commerce, exogenous uncertainty primarily relates to technological sources of error and security gaps. (Grabner-Kräuter & Kaluscha, 2003)

However, the assessment of consumers' subjective privacy perception requires a more fine-grained differentiation of the potential sources for privacy intrusion. In 1996, Smith et al. published a scale that aimed at measuring consumers' privacy concerns. They identified the following four dimensions that cause concerns about organizational information privacy practices:

- *Collection:* Individuals feel that their privacy is threatened, if great quantities of data concerning their personality, personal background or activities are collected and stored without a proper reason or purpose. This concerns category also comprises concerns about 'mosaic effects' (i.e. the retrieval of enriched insights through the combination of multiple data sources).
- *Unauthorized secondary use:* Sometimes information is collected for one purpose, but used for another, without authorisation from its owner. This unauthorized usage can relate to the gathering organization or to third, external parties after the information has been shared or exchanged.
- *Improper access:* This dimension comprises concerns about personal data becoming accessible to individuals, who do not have a real need to know or may even have malicious motives. This unapproved access can be the results of the defiance of technological access constraints (e.g. for identity theft, financial fraud...) or inappropriate organizational policies.
- *Errors:* Many individuals are concerned that accidental errors in personal data could lead to privacy issues. This dimension relates to concerns about the procedures for minimizing such errors, the responsibility in spotting errors (i.e. by software or individuals) or the reluctance to delete obsolete data.

Smith et al. (1996) did not define the term "concern", but - adopting the definition of the Oxfords dictionaries - concerns can be seen as "a cause of anxiety or worry" (Oxforddictionaries.com, 05.05.2014). The four dimensions should therefore not be confused with unwanted outcomes. The scale does not measure privacy risk perception, but assesses respondents' agreement about what potentially causes worries about organizational information privacy practices.

Moreover, it is important to notice that the uncertainty reflected through these four dimensions is partly endogenous and partly exogenous. That is, whether there is reason to be worried depends partly on the agreements with and the actions of the exchange partner. The remaining part depends on environmental factors and actors not directly involved in the exchange.

Just as Smith and colleagues had intended, their effort to develop a validated concern for privacy (CFP) measurement instrument evoked a research stream in which the application of their measurement eased the creation of comparable and accumulative findings. (Smith et al., 1996) Researchers from various scientific areas have devoted her attention to the exploration of privacy concerns in recent years (Li, 2012). Some studies examined the antecedents of CFP,

including perceived vulnerability, perceived ability to control, (Dinev & Hart, 2004) internet literacy, social awareness, (Liao, 2011) personality traits (Junglas, 2008) and gender differences (Fogel & Nehmad, 2009). Other studies focussed on the effects of CFP on the adoption of new technologies, such e-commerce (Udo, 2001), location-based services (Xu & Gupta, 2009; Zhou, 2010) or radio frequency identification (Lee et al., 2007). Empirical evidence has also shown that CFP have a significant positive influence on peoples' privacy risk perception (e.g. Malhotra et al., 2004; Van Slyke et al., 2006; Keith et al., 2013).

2.2. The Role of Trust and Distrust in Privacy Risk Perception

A great deal of literature shows that trust is believed to be one of the most relevant factors in explaining privacy risk perception (Malhotra et al., 2004). Trust has often been framed according to the three-place predicate, consisting of two actors (A and B) and a valued object (C). It works as follows:

1. Actor A judges actor B trustworthy.
2. Therefore, actor A trusts actor B with a valued thing C.
3. By doing so, A becomes vulnerable for B's powers over the entrusted thing C (Wang & Emurian, 2005; originally from Baier p. 99, 1994).

In the consumer-based e-commerce context, consumers can be seen as trustors (A). They disclose sensitive information, such as e-mail addresses, credit card numbers and personal preferences, while lacking the ability to control or monitor the further usage. The online firm, on the other hand, functions as the trustee (B), as it receives the private information and determines the consumer's fortune through its subsequent behaviour. Hence, information disclosure imposes vulnerability on the consumers and gives power to the online firm. Accordingly, trust – addressing the endogenous uncertainty involved – is wildly believed to be the key driver for successful e-commerce (Bhattacherjee, 2002). However, as versatile the inclusion of trust in privacy research is, as inconsistent is its conceptualization. The following section is dedicated to these definitional issues. Afterwards, distrust and its relationship to trust are discussed.

2.2.1. Conceptualizations of Trust

The inconsistencies in conceptualizing trust emerge due to several reasons. First, trust is a complex construct, which is frequently used interchangeably with other related but distinctive dimensions, such as faith, fairness, credibility or confidence. (Wang and Emurian, 2005)

Second, the understanding of trust depends on the examined trust object and the level of the relationship under examination. That is, trust is a central component of many relationships and can refer to a variety of objects, including persons, institutions, systems, physical things, deities, information and more (Wang & Emurian, 2005; originally from Nissenbaum, 2001, p. 104). Individual level trust (e.g. personal relationship) is distinct from that at group level (e.g. interdepartmental) or societal level (e.g. trust in political systems) (Bhattacherjee, 2002).

Third, trust can be seen as a personality trait or as a psychological state. Personality traits are the results of developmental and societal factors and are relatively stable regardless of any specific context. An often cited example is dispositional trust, which refers to one's consistent tendency to be willing to rely on others across a broad spectrum of situations and persons (McKnight & Chervany, 2001). In contrast, psychological states are relatively short cognitive and affective episodes, which are impacted by situational factors. (Bhattacherjee, 2002)

Fourth, trust incorporates cognitive, emotional and behavioural aspects. Consequently, trust has been construed as intention, behaviour, attitude, expectancy and beliefs. (McKnight & Chervany, 2001)

2.2.1.1. Trust as Behaviour or Behavioural Intention

As behavioural intentions are a reliable predictors for future behaviour (Fishbein & Ajzen, 1975), several researchers have conceptualized trust as an intention. Trust, in this respect, refers to the willingness to depend on another party, in spite of a lack of control over that party, and despite of possible negative consequences. (McKnight & Chervany, 2001)

Another perspective has defined trust in terms of individual's choice behaviour. As mentioned before, trusting incorporates vulnerability. Without a potential threat and the trustor's awareness about the risky situation, development of trust is not possible. If cooperation occurs, it inevitably comprises an action of deliberate risk-taking, manifesting the trustor's vulnerability through reliance on the trustee. In this account the decision to take the risk is seen as the essence of trust. (Nickel & Vaesen, 2012) Individuals are presumed to make relatively rational choices. That is, the trustors are believed to assess the likelihood that the trustee performs as expected, and the accompanying gains and losses of performance and non-performance, respectively. Behaviour is guided by the trial to maximize utility by balancing expected gains against expected losses. Applied in information privacy research, this utility function is generally called privacy calculus. (Li, 2012) The privacy calculus suggests that an individual's level of privacy concern will influence consumers' perceived risk of information disclosure. Perceived privacy risks are then weighted against perceived benefits of disclosure.

The individual's intention to share information is based upon the outcomes of this function. (Keith et al., 2013) Hence, in privacy calculus, trust is not a part of the trade-off function. Instead, it is conceptualized (often implicitly) as the very act of risk taking, namely the act of disclosing information (e.g. Awad & Krishnan, 2006; Dinev and Hart, 2006).

Several researchers emphasized the usefulness of this conceptualization due to its direct observability. However, the approaches have been criticized for their limited ability to adequately describe the way people make the trusting decision. Conceptualizing trust in terms of trust-related behaviour leads also to an overestimation of people's cognitive abilities and their engagement in conscious utility calculations for trust formation. Moreover, the presumptions regarding the rationality of choice exclude for the most part the role of emotional and social influences. (Kramer, 1999)

2.2.1.2. Trust as Attitude

In another stream of research trust is construed as a general attitude. In this account, it is believed that trust depends on a normative evaluation about appropriateness of behaviour and what should be expected from others and the system in which they live. According to the people's fundamental understanding of moral and social orders, they form judgements about how the future *should* go and built trust accordingly. (Nickel & Vaesen, 2012) Since attitudes reflect human affect for the better part, this view allows for greater emphasises on the affective aspects of trust than the behavioural conception (Bhattacherjee, 2002). However, its focus on socially learned and socially confirmed expectations is still too rough to account for subtle contextual and relational details.

2.2.1.3. Trust as Aggregation of Beliefs

Trust was also conceptualized as an aggregation of beliefs that concern the characteristics of the trustee and the relationship to the trustor. Trust beliefs refer to the trustor's perceptions of the trustee's attributes and their influence on the trustee's behaviour. These perceptions can be of cognitive or affective nature. (Bhattacherjee, 2002) Hence, rather than focussing on the trustor's interests and his/her calculative orientation toward risk (like in the calculative approach), this perspective puts more weight on the relational underpinnings of trust formation. (Nickel & Vaesen, 2012)

2.2.2. Conceptualizations of Distrust

Early psychological research has treated trust as vital part of personality development and necessary ingredient for collaboration and social order (Lewicki et al., 1998; Wang & Emurian, 2005). Distrust, on the other hand, has been regarded as psychological disorder that requires treatment. Founding on this tradition, researchers from many disciplines suggested trust to have positive effects on various outcomes. For instance, political scientists saw trust in government and institutions as substantial to guide the public risk acceptance (Poortinga & Pidgeon 2005). Likewise, management researchers examined how trust enhances satisfaction in organizational decision making and business performance (Wang & Emurian, 2005) and marketers studied trust with regard to successful relationship marketing (Luo, 2002) or suspected it to play a central role in the adoption of e-commerce (Grabner-Kräuter & Kaluscha, 2003; Luo, 2002). By treating trust as condition for collaboration and distrust as reason for non-collaboration, scholars ascribe a normative character to both constructs. This view, in turn, often entertains the assumption that trust and distrust are opposite ends of a single continuum. That is, the meaning of low trust levels is equivalent to high distrust levels and vice versa. (Marsh & Dibben, 2005)

However, this view has been questioned in the past. Lewicki et al. (1998) argued that the normative view led to an unbalanced research focus, where distrust is discounted as source for social dysfunction. Instead, they promote a perspective where trust and distrust is regarded as equally functional in relationships. They base this idea on Luhmann (1989), who argued that both, trust and distrust, serve as a mean to deal with complexity and uncertainty. Trust fosters decision making by allowing undesirable conduct of the trustee to be removed from consideration, while it allows desirable conduct to be seen as certain. Similarly, distrust simplifies the decision tree by allowing undesirable conduct to be seen as likely or even certain. Subsequently, both constructs enable an individual to take action or to refrain from doing so, respectively. Hence, distrust is seen as functional equivalent for trust and one chooses between the two. (Marsh & Dibben, 2005).

Moreover, Lewicki et al. (1998) dissociated from the bipolar view, where distrust lays one the opposite end of a single continuum. Although distrust is seen as a construct, which is linked and opposite to trust, it is viewed as an independent constructs. Accordingly, trust and distrust are no longer mutually exclusive conditions. Instead, Lewicki et al. (1998) propose that people in course of getting to know each other, can experience four relationship conditions , where trust and distrust co-exist, each of them having either high or low levels (i.e. low trust/ low distrust, low trust/ high distrust, high trust/ low distrust and high trust/ high distrust).

Even though a sizable literature agrees today that trust and distrust are distinct constructs (McKnight & Chervany, 2001), opinions deviate where exactly this distinction is situated. Sitkin and Roth (1993) suggested that trust relates to task reliability, while distrust is mainly based on estimates of value-congruence. According to their conceptualization, trust is disrupted, when an individual or a group performs unreliable on competence-related tasks or is expected to so in the future. Distrust occurs, when an individual or a group is perceived as not sharing key values. If someone is believed to operate under completely different values, his or her world view appears so alien that it is seems reasonable to suspect this individual of violating generally accepted norms in the future.

A similar argument comes from Adams and colleagues (2010), who assess distrust in large corporations and describe distrust as the extent to which an individual expects organizations' goals, intentions and outcomes to be inconsistent with social norms (Adams and colleagues, 2010). Many other trust researchers chose a similar differentiation that opposes performance to motivational qualities (although not all of them distinguished between trust and distrust). Kee and Knox (1970) distinguish trust in terms of 'motives' and 'competence'. Barber differentiates two types of trust that reflect expectations about either competent performance or moral responsibility (Sitkin & Roth, 1993, originally from Barber, 1983). Marsh and Dibben (2005) accentuate that it is the intentional component that separates distrust from trust. Gabarro (1978) as well as Whipple and Frankel (2000) differentiate between 'competence' and 'character'. And Lui and Ngo (2004) discuss 'competence-based' and 'goodwill-based' trust.

2.2.3. Conceptualization of Trust and Distrust in the Present Study

The incorporation of distrust as separate construct may have substantial implication for privacy research. Formerly, it was assumed that trust increase comes along with distrust reduction. Likewise, the outcomes of high trust were believed to be identical to those of low distrust. Lewicki et al.'s (1998) view, however, challenges these assumptions.

Suppose that trust and distrust can coexist and that their effects are really different, an outcome that is promoted by reducing distrust is not necessarily promoted by enhancing trust. Companies, today mainly making trust-building efforts, would therefore turn out to be ineffective in repairing the negative consequences of high distrust. In order improve that effectiveness, they would need to reconsider their strategy and focus on measures to tackle distrust problems separately. The development of such measures, however, requires profound knowledge about trust and distrust. Yet little is known about the influence of distrust, and how it is distinct from those of trust.

This study contributes to this knowledge. I attempt to advance Lewicki et al.'s (1998) ideas. Trust is thus defined similarly as "confident positive expectations regarding another's conduct" (Lewicki et al.', 1998, p. 439). Distrust is defined as "confident negative expectations regarding another's conduct" (Lewicki et al.', 1998, p. 439). Expectancies can be treated as beliefs, as they differ primarily in terms of future versus present focus, respectively (McKnight & Chervany, 2001). Hence, the current conceptualization can be ascribed to the category of aggregated trust-beliefs. These beliefs are regarded as person-specific, in the sense that they relate to one or more specific others, rather than to others in general. They are also seen as domain-specific. That is, in one and the same domain (e.g. product quality) it is difficult to imagine simultaneous perception of trust and distrust (Schoorman et al. 2007). However, among different domains (e.g. product quality and privacy practices), the trustee's incentives to defect might be different for each domain, and so might the trustor's trust and distrust.

To construe trust and distrust as an aggregation of beliefs has several additional advantages. First, beliefs stand at the beginning of the pattern of the theory of reasoned action (Fishbein & Ajzen, 1975). As such, it is reasonable to believe that they will have a relevant influence on trusting intentions and subsequent trust-related behaviour (McKnight & Chervany, 2001). Second, trusting beliefs permit to incorporate affective and cognitive aspects of trust and distrust (Bhattacherjee, 2002). It has been found that various trusting beliefs are partly affective in nature (McKnight & Chervany, 2001). Since it is very difficult to make a clear separation between belief and affect, beliefs offer a more promising way to consider all aspects of trust and distrust. Third, beliefs allow construing trust and distrust on an interpersonal level with profound respect to the personal and contextual characteristics. Although trust and distrust in an e-commerce context aim at companies, consumers tend to view these firms as human-like, as they are basically collections of human beings (Bhattacherjee, 2002).

Further, I take over Sitkin and Roth's (1993) proposition. That is, the confident positive expectations regarding the receivers' conduct relate to assumed task-reliability, whilst the confident positive expectations express themselves in assumed value-incongruence. Adopting this view, the study strives to examine the influence of trust and distrust on consumers' privacy concerns and privacy risk perception.

2.3. Research Model and Hypotheses

Figure 1 presents this study's research model. The formerly discussed constructs trust, distrust, privacy concerns and privacy risk perception are included. The following sections discuss the relationship between these constructs and correspondingly hypotheses are derived.

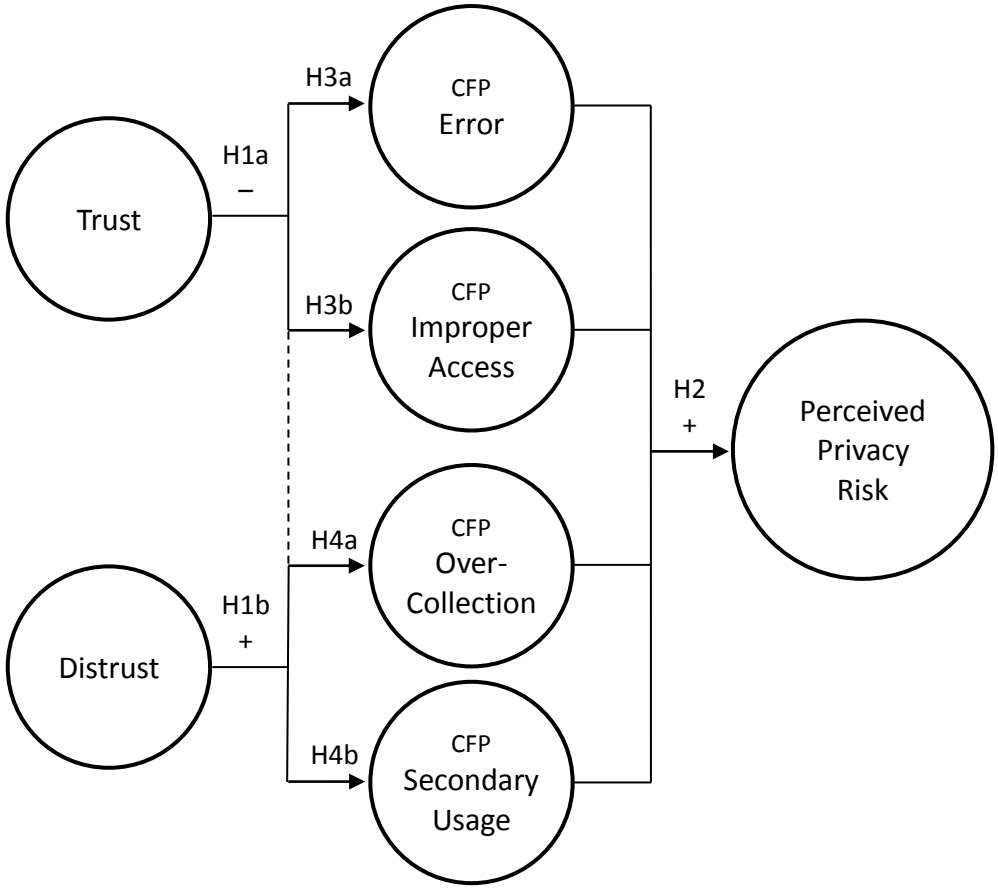

Figure 1: Proposed relationship between trust, distrust, privacy concerns & risk perception.

Trust is important when it is difficult to fully regulate business agreements and where it is consequently necessary to rely on the other party not to take unfair advantage of this situation (Deutsch, 1960). Relationships, where both parties have opposing as well as shared objectives, are likely to evoke the coexistence of high trust and high distrust levels (Lewicki et al., 1998). Considering the e-commerce situation, it becomes obvious that these circumstances are commonly prevalent in the relationship between consumers (i.e. information sender) and the

online firm[1] (i.e. Information receiver). On one hand, the information receiver and the consumer have an interest in making a fair deal that safeguards the interests of both parties (e.g. assuring consumer's need satisfaction, preserving the receiver's reputation, enabling repeated sales in the future…). On the other hand, however, there is room for opportunistic behaviour that exploits the interdependence and redounds to the advantage of one party (Wang and Emurian, 2005; Grabner-Kräuter & Kaluscha, 2003). Specifically for the disclosure of private information, the receiver is in a favourable position for opportunism. The consumer is obligated to provide personal information to the online firm without having the means to control or monitor the information practices. (Liao, 2011)

2.3.1. The General Effects of Trust & Distrust on Privacy Concerns & Risk Perception

In this study, I argued that trust and distrust impact privacy risk perception via specific concerns for privacy. As explained earlier, privacy concerns comprise several dimensions (i.e. error, improper access, over-collection and secondary usage). Their relevance depends on the uncertainty that consumers associated with the e-commerce situation. This uncertainty is partly endogenous (i.e. it depends partly on the receiver's conduct). If the receiver acts in favour of the sender, the actual amount of endogenous uncertainty decreases.

Trusting consumers are more likely to expect this favourable conduct. It is believed that by doing so, they exclude the endogenous fraction of uncertainty from consideration and ascribe lesser relevance to certain privacy concerns. Contrary, distrust reflects negative expectations regarding the receiver's conduct and it is thus likely to increase the salience of certain privacy concerns. The resulting levels of privacy concerns will alter their context-specific risk perception (Keith et al., 2013). Support for this mechanism comes from the social contract theory. Some scholars have argued that the information disclosure in e-commerce implies a social contract between sender and receiver. That is, a set of mutually understood obligations is expected to govern the behaviour of those involved (Li, 2011). Some of these obligations concern the appropriate handling of personal information to prevent privacy intrusion. Individuals' trust raises expectations of actions that promote the contract fulfilment. Distrust increases expectations of actions that are insufficient or even contra-productive to satisfy the contract. (Culnan & Armstrong, 1999) In turn certain outcomes may appear more likely (or

[1] This study discusses the business-to-consumer e-commerce. To ease the readability and to generalize over all possible B2C online transaction contexts, the term "information receiver" or "receiver" will replace alternative terminology (such as seller, web retailer, e-vendor, exchange partner…) in the following sections.

unlikely) to occur, affect concerns accordingly[2] and thus, change consumers' privacy risk perception. This aligns with Pavlou et al. (2007), who found evidence that trust significantly decreases privacy concerns, which in turn reduces perceived uncertainty. Garcia-Retamero et al. (2012) also brought empirical evidence that higher perceived value similarity decreases individual's threat perception. In addition, several researchers demonstrated that privacy concerns have a significant positive influence on peoples' privacy risk perception (e.g. Malhotra et al., 2004; Van Slyke et al., 2006; Keith et al., 2013). Thus, the following hypotheses are formulated:

- *H1: Trust and distrust impact consumers' specific privacy concerns.*
  - *H1a: Trust is negatively related to specific privacy concerns.*
  - *H1b: Distrust is positively related to specific privacy concerns.*
- *H2: Consumers' specific privacy concerns are positively related to privacy risk perception.*

2.3.2. The Asymmetric Effects of Trust & Distrust on Privacy Concerns

According to Sitkin and Roth (1993), trust relates to the assumed task-reliability of the receiver and leads consumers to expect ceaseless and technical competent performance. Distrust, on the other hand, is based on assumed value-incongruence and fosters the expectation that the receiver's goals, values or motives will lead him to approach situations in an unacceptable way. (Sitkin and Roth, 1993)

I adopt Sitkin and Roth's (1993) view on trust and distrust and suggest that their impacts on certain concerns may not just be opposed, but they may also be asymmetric. That is, certain concern dimensions might be more responsive to the assumed reliability (i.e. trust) and others more to value-orientation (i.e. distrust). Support for this belief comes again from social contract theory. As Hoffman et al. (1999) point out, a web transaction involves two contracts: (1) an economic contract that governs the exchange of goods and services with all its formal, monetary and legalistic aspects and (2) a social contract characterized by implicit personal obligations and feelings of reciprocity and gratitude. They argue that consumers seek to

[2] This relationship between trust and privacy concerns has been construed reversely by Zhou (2010), with privacy concerns affecting trust. In this respect, it is important to notice that Smith et al.'s (1996) scale refers to *general* CFP, whereas the hypotheses of this study refer to *specific* CFP. Smith et al.'s (1996) scale is, loosely worded, an indicator of peoples' general privacy alertness. Zhou (2010) argues that this general alertness will make consumers more doubtful about dimensions of trustworthiness. This study, however, premises that trust and distrust are specific for each constellation of trust actors, trust object and context. It is argued that people determine trust and distrust levels for the company under examination and consult these levels in order to form their specific CFP accordingly. CFP is therefore seen as specific for the company under examination.

engage in an exchange that involves *both* types of contracts to reduce potential risks. (Hoffman et al., 1999) If trust and distrust would address both contracts differently, consumers' unique level of trust and distrust might evoke different ideas about the receiver's compliance with each contract and thus produce corresponding levels of privacy concerns.

2.3.2.1. The Effects of Trust & Distrust on 'Error' and 'Improper Access'

The fraction of endogenous uncertainty comprised in the concerns 'error' and 'improper access' are believed to be mainly reliability-related. That is, in order to avoid error or improper access, competent development and dutiful execution of standardized procedures (i.e. regular controls of data-input, cleaning of the existing data-collection, installation and maintenance of data-security systems etc.) is required. Given that, consumers' treatment will be uniformly, controlled and fair (Sitkin and Roth, 1993) and thus, privacy intrusion is less likely to occur.

Trusting people will expect the information receiver to be able and willing to execute these administrative tasks in a reliable fashion. Consequently, trust will be very effective in reassuring consumers in this respect and so they will be less concerned about the correctness and the security of the disclosed data.

The concept of distrust, however, is linked to the receiver's values and motives (Sitkin and Roth, 1993). Collecting false information or giving it away without consent and monetary compensation is not in the receiver's interest. So, even if an information receiver is believed to hold a fundamentally different set of values, it is less conclusive that he or she will jeopardize the accurateness or security of the data, as there are simply few incentives for doing so.

A theoretical rationale for this proposition is provided by the agency theory. Here, it is assumed that if the goal conflict between the principal (i.e. the consumer) and the agent (i.e. the receiver) is low, both parties share the risk of failure and thus, the agent is more likely to behave in the accordance with the principal's wishes. In this situation, behaviour-based evaluation of the agent is more efficient than outcome-based evaluation (Bergen et al., 1992). This emphasises that – in this particular situation – the central question is not whether the agent will try to achieve certain outcomes or not, because he or she is personally motivated to avoid failure anyways. Instead, the way he or she executes certain actions gains greater importance. It is therefore argued that assumed value similarity between both parties is less central than the task-reliability. The following hypotheses are formulated:

- *H3: There is an asymmetric effect of trust and distrust on the privacy concerns 'error' and 'improper access'.*

H3a: Trust has a more significant effect on lowering error-related privacy concerns than distrust does on increasing it.

H3b: Trust has a more significant effect on lowering access-related privacy concerns than distrust does on increasing it.

2.3.2.2. The Effects of Trust & Distrust on 'Over-collection' and 'Secondary usage'

Unlike error and access-related privacy threats, the analysis of personal information and online behaviour patterns can assure business advantages in a competitive business environment. Selling data to third parties can be a profitable option to the receiver as well. (Jagadish et al., 2011) The only drawback for the receiver is the consideration of consumer's privacy needs. As the goal conflict between both parties is high and the consumers have little means to prevent the receiver from defection (Pavlou et al., 2007), the endogenous uncertainty comprised in these concerns depends mostly on the receiver's value-orientation.

Given that consumers find little common ground with the receiver, they will assume value-incongruence and thus distrust the receiver. A distrusted receiver is perceived as "cultural outsider", who "does not think like us" and may therefore do the "unthinkable" (Sitkin and Roth, 1993, p. 371). Under these circumstances, violations of the social contract may seem likely and expectations might arise that this receiver will engage in opportunistic behaviour. Similarly, Hoffman et al. (1999) argue that if consumers believe that the receiver does "not share their values about information privacy in online commercial environments… [it] may likely lead to a lessened commitment to the relationship, which in turn generates higher decision-making uncertainty…" (p. 133).

The prevention of over-collection and secondary usage do not require reliable performance of the information receiver. Actually, quite the contrary is the case. Data collection and its subsequent use are the direct results of decisions and actions made by the information receiver. Hence, while inaction or incompetent performance increases the chance of error and improper access, it decreases that of secondary usage and over-collection. Simply put, the less competent the receiver appears, the less likely it seems that he will be able to gather extensive amounts of data and to use it effectively for his own profit. Trust might therefore be less effective in reducing collection-related and usage-related concerns. The following hypotheses are postulated:

- *H4: There is an asymmetric effect of trust and distrust on the privacy concerns 'over-collection' and 'secondary usage'.*

  H4a: Trust has a less significant effect on lowering collection-related privacy concerns than distrust does on increasing it.

  H4b: Trust has a less significant effect on lowering usage-related privacy concerns than distrust does on increasing it.

3. Methods

3.1. Research Context

In order to test the relationships proposed in the research model (i.e. between trust, distrust, privacy concerns and perceived privacy risk), the banking context was chosen. Banks handle great amounts of personal data. Some of the most commonly recorded information are the amount of transactions, the date, time and location of the transaction and the name of the merchant, where the transaction is taking place (Omariba et al., 2012). Tapping directly into financial matters and alluding to someone's wants, habits and preferences in a long period of time, these transaction histories provide a profound insight into consumers' private life, Inappropriate treatment of this data engenders the likelihood for several losses (i.e. loss of time, money, face) and thus can evoke risk feelings in consumers (Lim, 2003).

Although everyone knows roughly what banks are and what they do, these large corporations have highly sophisticated and complex practices, which are unfamiliar to most consumers. Due to the lack of in-depth knowledge and direct insight on mostly intangible services, respondents will be more likely to consult trust and distrust when forming their concerns and risk perception (Bravo et al., 2012; Adams et al., 2010).

Furthermore, electronic banking shows some particular characteristics, such as the extensive use of technology, the impersonal nature of the online environment and the uncertainty entailed in using an open technological infrastructure, that make it arguably riskier than face to face interactions with bank employees. (Omariba et al., 2012)

Moreover, the financial crisis in 2008 has severely damaged the reputation of the financial sector (Raithel et al., 2010) and raised questions about its responsibility. These questions concern the means of the financial sector to prevent a collapse as well as the motivations that initially caused it (Herzig & Moon, 2013). The on-going debate circles around banks' abilities and motives; both of which are central elements of this study. Under these circumstances, consumers might have formed a (probably ambivalent) stance towards these corporations (Adams et al., 2010). However, the inherent problematic does not concern banks' information practices directly and thus, the extensive media coverage is unlikely to predetermine privacy-related outcomes of this study. For these reasons, it seems very promising to explore the effects of trust and distrust in this context.

3.2. Measurements

The items employed to measure specific concerns for privacy and perceived privacy risk were based on previous literature. Only slight modifications were made to adapt them to the current research context. Since scholars have not yet reached a consensus on the conceptual difference between trust and distrust, instruments that fall completely in line with the current conceptualization are hard to find. Still, recent distrust literature and the extensive work on online-trust provided a good starting point to develop tailored measurement items for both constructs. The measures used in this study are presented in Table 1.

Trust Items

Trust refers to beliefs regarding an individual or a group to perform reliable on competence-related tasks or to do so in the future. Measurement items for trust were developed based on conceptual work of Bhattacherjee (2002) and McKnight & Chervany (2001), focussing particularly on the items related to competence and task reliability.

Distrust Items

It is suggested that distrust emerges, if value-incongruence is assumed and violations of social norms are expected (Sitkin & Roth, 1993). A scale to measure value-similarity was adopted from Siegrist et al. (2000). It is anticipated that respondents estimate value-congruence to the receiver by comparing values to a typical person working at the company being judged. Eight items are judged ranging from -3 to 3. The resulting estimates are aggregated to a perception of value similarity across these values. (Garcia-Retamero et al. 2012).

Specific Concerns for Privacy Items

The privacy concern measures came from Smith et al. (1996). They were adapted to target a specific referent (i.e. the bank).

Perceived Privacy Risk Items

Perceived privacy risk items were adapted from Malhotra et al. (2004). This scale was adapted to target a specific referent, too.

Table 1: Construct and control measurements.

	Below, you can see some statements that reflect beliefs that someone might or might not have of his/her bank. From your point of view, please choose the answer that best describes your present agreement or disagreement with each statement by indicating the appropriate number between 1 and 7. (7-point Likert scale)
Trust (in dependence on Bhattacherjee, 2002 and McKnight & Chervany, 2001)	T1. My bank operates its business in a highly dependable manner. T2. My bank is reliable in conducting its business with customers. T3. My bank has access to information needed to handle its business appropriately. T4. My bank is responsible in conducting its business with customers. T5. My bank has the skills and expertise to perform in an expected manner. T6. My bank is able to deliver services with consistent quality.
Specific Concerns for Privacy (in dependence on Smith et al., 1996)	***Error*** E1. All the personal information in computer databases should be double-checked for accuracy - no matter how much this costs. E2. My bank should take more steps to make sure that the personal information in their files is accurate. E3. My bank should have better procedures to correct errors in personal information. E4. My bank should devote more time and effort to verifying the accuracy of the personal information in their databases. ***Improper Access*** A1. My bank should devote more time and effort to preventing unauthorized access to personal information. A2. My bank's databases that contain personal information should be protected from unauthorized access-no matter how much it costs. A3. My bank should take more steps to make sure that unauthorized people cannot access personal information in their computers. ***Secondary Usage*** U1. My bank should not use personal information for any purpose unless it has been authorized by the individuals who provided the information. U2. When people give personal information to their bank for some reason, the bank should never use the information for any other reason. U3. My bank should never sell the personal information in their computer databases to other companies. U4. My bank should never share personal information with other companies unless it has been authorized by the individuals who provided the information. ***Over-Collection*** C1. It usually bothers me if my bank asks me for personal information. C2. When my bank asks me for personal information, I sometimes think twice before providing it. C3. It bothers me to give personal information to so many companies. C4. I'm concerned that my bank is collecting too much personal information about me.
Perceived Privacy Risk (in dependence on Malhotra et al., 2004)	R1. There is much uncertainty associated with giving my personal information to my bank. R2. Providing my bank with my personal information could involve many unexpected problems. R3. It is risky to disclose my personal information to my bank. R4. There is high potential for loss associated with disclosing my personal information to my bank. R5. I feel safe disclosing my personal information to my bank. (reversed)
Distrust (in dependence on Siegrist et al., 2000)	**Compare yourself to the people working at your bank and indicate in the following statements how similar or dissimilar you are compared to bankers.** (7 response categories from -3 to 3) DS1. The bankers' values are... DS2. The bankers' goals are... DS3. The bankers' opinions are... DS4. The bankers' reasoning is... DS5. The bankers' motivations to act are DS6. The bankers' way to think is... DS7. The bankers' world view is... DS8. The way bankers make decisions is...
Control Variables	– Primary bank: What is the bank where you conduct the majority of your bank activities in the Netherlands? – Experience of information misuse in the past: To your knowledge, has your personal information ever been misused as the result of disclosing it to your bank? – Socio-demographics: What is your… gender/ age?

Control Variables

It has been proven that demographic variables, such as gender and age differences, affect privacy concerns (Fogel & Nehmad, 2009; Junglas, 2008) and thus, these two were measured for control. Some banks have suffered great reputational damage in the course of the financial crisis, while others were able to protect or even improve their reputation (Raithel et al., 2010). The bank's history and current reputation might account for some of the concerns. The primary bank to which a respondent is referring was therefore assessed as well. Finally, as individuals' prior experiences with banks' handling of personal information could influence respondents' concerns as well (Adams et al., 2010), respondents were asked how many times they experienced misuse of their personal information as result of sharing it with their bank.

3.3. Participants

Students from Wageningen University (WUR) were invited to participate in an online survey[3]. Within the European Union young individuals (at the age of 16 to 24) and highly educated individuals use the internet most often. The Netherlands are among the Top 3 countries with the highest internet penetration. (epp.eurostat.ec.europa.eu, 17.09.2014) As such, students living in the Netherlands represent an internet literate population, which is important for the e-commerce and has a high potential for online banking now and in the future. Moreover, it can be expected that with the beginning of their studies most students conduct the better part their banking affairs independently. Due to their young age, however, they do not patronize a bank for numerous years. As individual experiences with banks could influence someone's privacy concern levels, this relative short history as a bank client decreases the chance that these respondents primarily rely on first-hand experience and memory, rather than consulting trust and distrust to form their concern levels (Adams et al., 2010). For these reasons, students from a Dutch university are seen as suitable and highly relevant participants, who can deliver interesting results with direct implications for the e-commerce development in the future.

3.4. Data Collection

Firstly, five WUR students pre-tested the survey and several minor changes were made. Afterwards, a total of approximately 900 WUR students from different chair groups – all of them voluntary members of a mailing list for such surveys – were invited by e-mail for participation. Another invitation was placed on a social-media page, where WUR-students can

[3] The survey questions can be found under:
https://wur.az1.qualtrics.com/SE/?SID=SV_72NWhr3dUFSMIm1&Preview=Survey&BrandID=qtrial2014

offer their study books for sale. The invitation contained a hyperlink to access the questionnaire. By participation, respondents were offered a chance to win a 20€ gift card for study material. The time spent to take the survey had a median of 8 minutes. Approximately one week after sending the invitation, 197 students completed survey, 190 of whom (49.5% MSc, 43.2% BSc) remained in the sample after data screening. There were 41 males (21.6%) and 149 females (78.4%) in the sample, most of whom came from the Netherlands (71.8%). ING (36.3%), Rabobank (25.8%) and ABN Amro (25.3%) accounted for the majority of primary banks in the sample. Figure 2 illustrates the sampling composition.

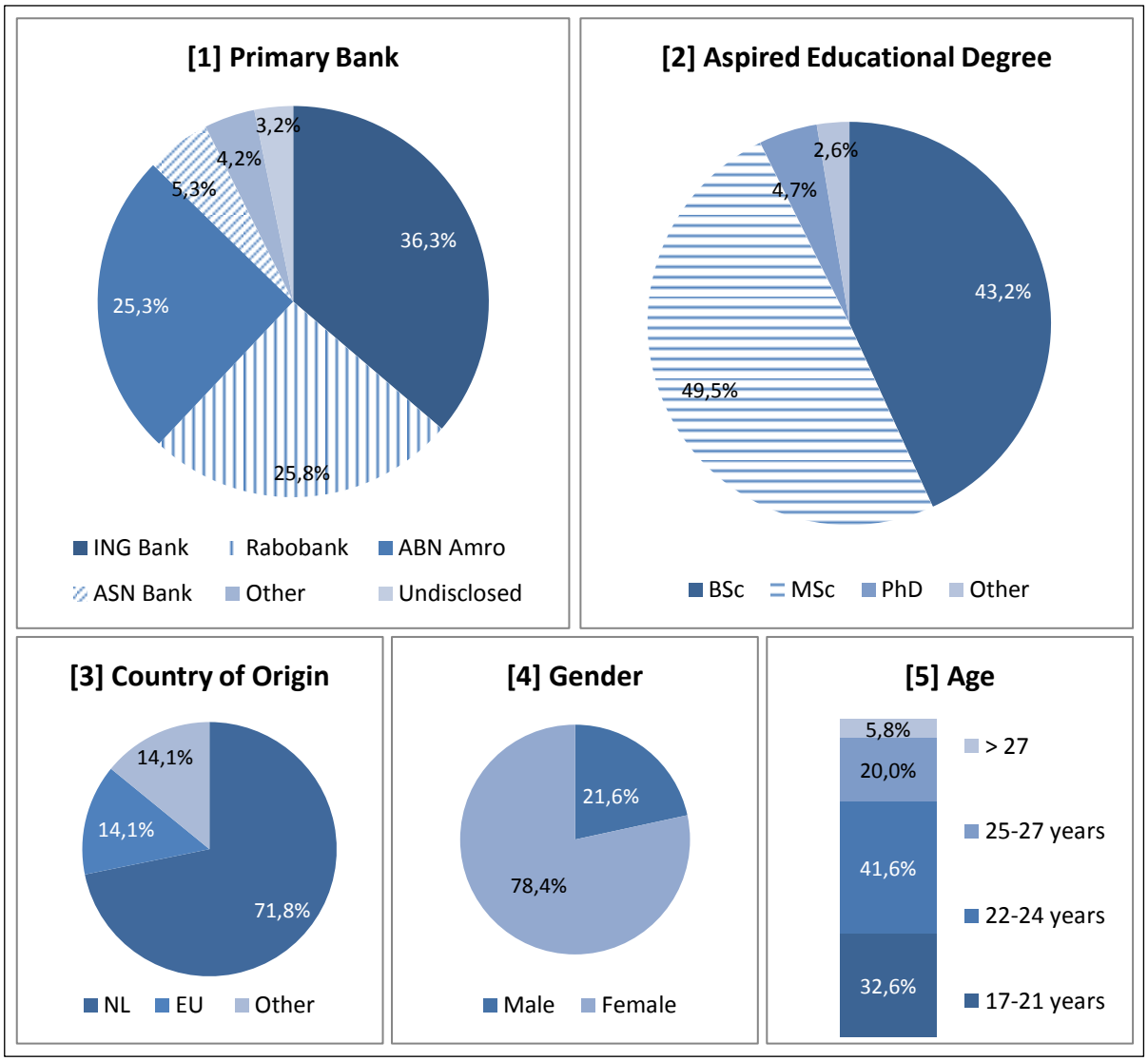

Figure 2: Descriptive statistics of the sample composition (N=190)

3.5. Data Analysis

3.5.1. Data Screening

SPSS 20 was used for the first steps of analysis. To identify unengaged or invariant responses, all cases were evaluated according to their standard deviation and the completion time. Subsequently, distributional properties were tested. Boxplots and Mahalanobis distances were calculated to identify and exclude univariate and multivariate outliers. In total, seven responses were excluded from the dataset. The Kolmogorov-Smirnov and Shapiro-Wilk test was conducted to see whether the responses were normally distributed. The significance values ($p < 0.001$) indicated that the responses deviated significantly from normal distributions. To gain further insight into this issue, the skewness and kurtosis scores of each item was transformed into z-scores, by dividing them through their respective standard errors and comparing the results to a normal distribution values (cut-off: ±2.58) (Field, 2009). Several items of 'trust', 'access' and 'secondary usage' showed negative skewness and positive kurtosis, indicating that participants scored similar and mostly high on these items. This is not surprising, as prior research has shown that consumers are distinctly dichotomized between those who are quite concerned about privacy and those who are not concerned at all (Acquisti & Grossklags, 2003). Thus, it is noted that the data set contains several significant departures from normality.

3.5.2. Construct Validation

Principal component factor analysis (PCA) was performed to see (1) whether the items of latent constructs loaded more on their own construct than on another construct, and (2) whether the average of these loadings exceeded at least 0.70 per construct. The PCA revealed cross-loadings between items of 'access' and 'error'. To solve this problem, Farrell's (2010) recommendations to deal with poor discriminant validity were followed. First, in an iterative process, offending items were removed and several promising solutions with different item combinations were derived from PCA. In the subsequent confirmatory factor analysis (CFA), however, the comparison of inter-construct correlation matrices with AVE scores indicated that the issue persisted. However, discriminant validity is an imperative requirement for path analysis, as its absence would cast doubt on all subsequent conclusions (Farrell, 2010). As it was not possible to collect additional data, the only available option was to collapse measures into one single construct, rather than conduct dimension-by-dimension analysis (Farrell, 2010).

Under these circumstances, the collapse was deemed justified and a six factor solution[4] (Table 2) was chosen for further analysis.

Table 2: Factor loadings of the six factor solution.

Item	Factors					
	1 Rel. Concern	2 Trust	3 Risk Perception	4 Distrust	5 Over-Collection	6 Sec. Usage
E2	0.898					
E4	0.898					
E3	0.852					
A3	0.738					
E1	0.734					
A1	0.680					
T2		0.876				
T6		0.803				
T5		0.799				
T3		0.702				
T4		0.682				
R2			0.852			
R3			0.825			
R4			0.787			
R1			0.767			
DS1				0.834		
DS7				0.819		
DS3				0.765		
DS6				0.684		
U4					0.822	
U1					0.777	
U3					0.776	
U2					0.664	
C1						0.853
C3						0.787
C2						0.763

Extraction method: principal component analysis. Rotation method: Promax with Kaiser Normalization.
Notes: Loadings below 0.30 were excluded.

3.5.3. Measurement Model

'Lavaan', a software package for latent variable modelling in 'R', was used to conduct the CFA. With non-normal data, the maximum likelihood test statistic (ML) tends to reject true models more frequently than the nominal (0.05) rejection rate and the underestimated standard errors can cause inflated Type I error rates when z tests are used to assess parameter significance (Tomarken & Waller, 2005). As previous tests indicated a deviation from normality, maximum likelihood estimation with robust standard errors (MLM) and a Satorra-Bentler scaled test statistic is used to estimate the model. The model fit is evaluated using Kline's (2010) recommendations regarding RMSEA, CFI, TLI and SRMR. The results suggested that the proposed factor structure has a good model fit (CFI = 0.96, TLI = 0.95, RMSEA = 0,036

[4] The resulting construct was named „reliability concern, because this study proposed that the dependence on consumers' task-reliability judgement (i.e. trust) represents a communality of both dimensions.

and SRMR = 0.061). Additionally, reliability, the convergent validity and the discriminant validity were examined. Construct scales are said to be reliable if the composite reliability (CR) > 0.70. As shown in Table 3, the CR's range from 0.79 to 0.90 and exceed the recommended cut-off value. The test of convergent validity involved two steps. First, it was confirmed that the average variance extracted (AVE) for all constructs was higher than the recommended threshold of > 0.50 (Table 3). Second, it was checked if all loadings to their corresponding constructs exceeded a minimum value of 0.60. The lowest loading was 0.65 and all loadings were significant at the $p < 0.001$ level. The evaluation of discriminant validity involved a comparison of the shared variance between each pair of constructs (i.e. the square of their correlation coefficient) to the corresponding AVE of each constructs. That is, for any construct A and B, the AVE estimate for A and the AVE estimate for B have to be greater than the shared variance estimate between A and B (Fornell & Larcker, 1981). Table 3 demonstrates that this condition is met. Overall, the evidence of good model fit, reliability, convergent validity and discriminant validity indicates that the measurement model is appropriate for testing the structural model at a subsequent stage.

Table 3: Composite reliability, estimated factor correlation matrix, AVE and shared variance from the measurement model.

			Correlation\Shared Variance Matrix					
		CR	1	2	3	4	5	6
1	Trust	0.85	**0.54**	0.07	0.00	0.19	0.00	0.03
2	Distrust	0.81	-0.26	**0.51**	0.01	0.04	0.06	0.05
3	Reliability Concerns	0.90	-0.05	0.12	**0.59**	0.15	0.16	0.19
4	Secondary Usage	0.82	0.44	0.21	0.39	**0.53**	0.18	0.02
5	Over-Collection	0.79	0.02	0.24	0.40	0.43	**0.56**	0.40
6	Risk Perception	0.85	-0.17	0.22	0.44	0.14	0.63	**0.58**

Notes: Correlations are below the diagonal, squared correlations are above the diagonal, and AVE estimates are presented on the diagonal. CR = Composite reliability.

3.5.4. Structural Model

The structural model was tested using the structural equation modelling (SEM) technique. Several studies on privacy risk perception relied on SEM (e.g. Malhotra et al., 2004; Cho, 2006; Featherman et al., 2010; Keith et al., 2010; Keith et al., 2013).

Figure 3 depicts the results of the SEM analysis. Fit indices of the proposed structural model reported a relatively poor fit with the data: (CFI = 0.91, TLI = 0.90, RMSEA = 0,048 and SRMR = 0.100). High modification indices between the different concerns indicated a relation between the concern dimensions. They are seen as distinct but related constructs and thus, it seemed

reasonable to allow them to covary. After inclusion, the model displayed an improved fit to the observed data (CFI = 0.95, TLI = 0.94, RMSEA = 0,039 and SRMR = 0.063). Furthermore, the model explained a fair amount of variance in the outcome variables. It explained 9.6% of variance in concerns for over-collection, 34.2% in secondary usage and 48.5% of privacy risk perception. Variance explained in reliability concerns was rather small with 5.1%.

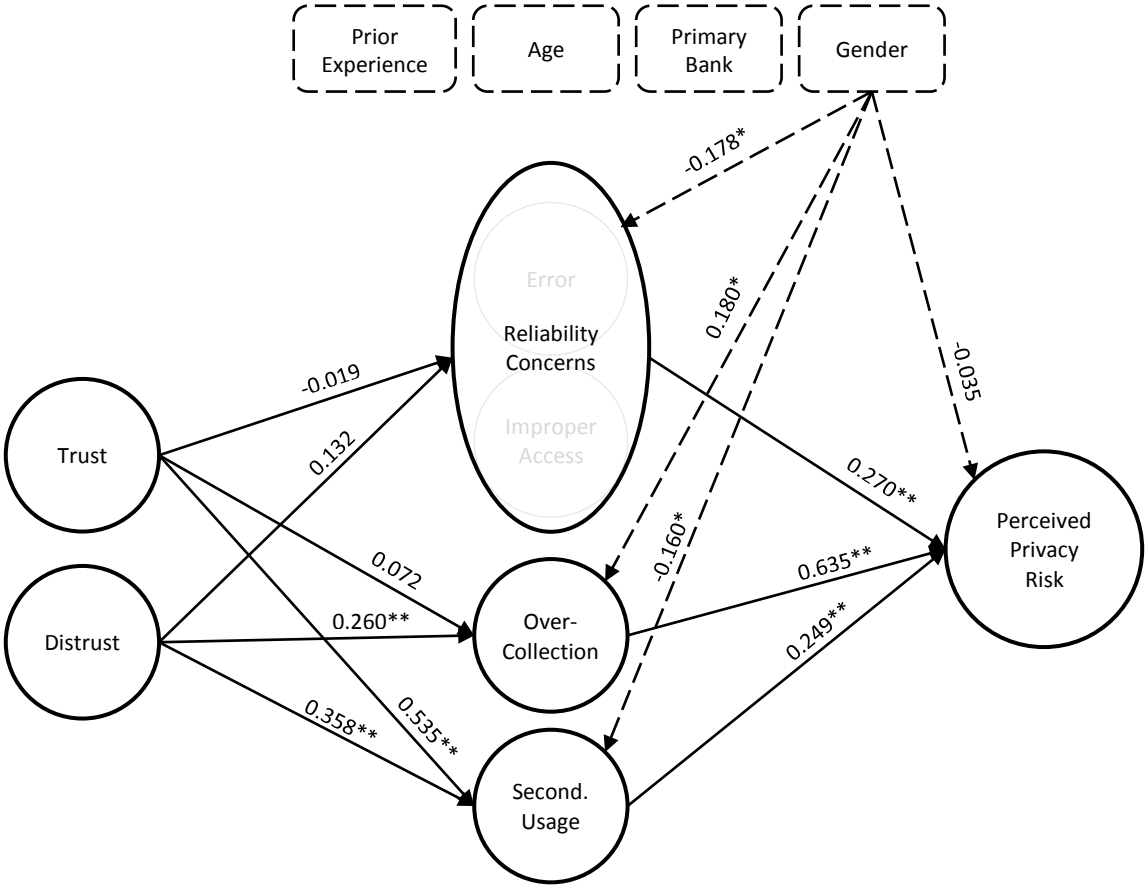

Figure 3: Path analysis.

Notes: Influences of insignificant control variables are not included. ** p < 0.01 * p < 0.05

Participants' age, primary bank, gender and their prior experience with data misuse were included into the model to account for additional effects on privacy concerns and privacy risk perception. Only three people reported prior experience with information misuse. The majority of respondents were between 18 and 24 years old. Due to the little variance, none of these variables showed a significant influence and neither did the variable 'primary bank'. Gender, however, influenced all three concern dimensions significantly. Male respondent's showed overall lesser concerns for reliability (β= -0.178 p < 0.05) and secondary usage (β= -

0.160 p < 0.05), but higher concerns for over-collection (β= 0.180 p < 0.05). Risk perception was slightly lower for male respondents, but the effect remained insignificant (β= -0.035 p > 0.05).

Hypotheses 1 and 2 are tested through consideration of the beta coefficients and their significance (p > 0.05). The negative relation between trust and CFP was not supported (H1a). Only the path towards reliability concerns was negative (β= -0.019 p > 0.05). The paths to over-collection (β= 0.072 p > 0.05) and secondary usage (β= 0.535 p < 0.01) were both positive, whilst only the latter one was found to be significant. The data supports H1b, which proposed a positive relationship between distrust and CFP. Distrust had a significant positive effect on concerns for over-collection (β= 0.260 p < 0.01) and secondary usage (β= 0.358 p < 0.01). The positive effect on reliability concerns fell just under the significance level of 0.1 (β= 0.132 p= 0.101). The positive relationship between CFP and privacy risk perception (H2) was confirmed: the paths from reliability concerns (β= 0.256 p < 0.01), over-collection (β= 0.263 p < 0.01) and secondary usage (β= 0.650 p < 0.01) were all significant.

The asymmetric effects proposed in H3 and H4 should be tested by imposing an equality constraint on the structural model, which sets a particular pair of path-coefficients equal. This approach is adopted from Cho (2006). In a repetitive process, several coefficient combinations are constrained (e.g. βTrust*Over-collection = βDistrust*Over-collection) and the model fit of each constrained model is compared to that of the unconstrained model. The difference in the Chi^2 (ΔChi^2) is used as a criterion to evaluate the hypotheses. A significant difference would be indicating that the absolute strengths of positive and negative coefficients are significantly different. (Cho, 2006) The results of this procedure are documented in Table 4.

Table 4: Model test of coefficient equality.

Effects of trust/distrust on concern dimensions	Chi^2 (308) = 396.47	
Equality Constraint	Chi^2 (309)	ΔChi^2
βTrust*Rel.Concern = βDistrust*Rel.Concern	398.40	2.00
βTrust*Over-collection = βDistrust*Over-collection	398.78	2.45
βTrust*Sec.Usage = βDistrust*Sec.Usage	399.81	2.95

Notes: Rel.Concern = Reliabilty Concerns; Sec.Usage = Concern for secondary usage; Over-collect = Concern for over-collection. ** p < 0.01 * p < 0.05.

As the concern dimensions ‘error’ and ‘access’ were merged in course of principal components analysis, the individual influences of trust and distrust on these dimensions could no longer be distinguished. Distrust is found to influence the concern dimensions ‘reliability concern’ and

'over-collection' more than trust. Trust had a greater impact on secondary usage. However, with p= 0.16 for 'reliability concerns', p= 0.12 for 'over-collection' and p= 0.86 for 'secondary usage', the Chi^2 difference test did not indicate a significant difference for any pair of coefficients. Hence, the asymmetric effects (H3 & H4) are not supported. The implications of these findings are discussed in the following section. Table 5 summarizes the study findings.

Table 5: Summary of the findings.

Hypotheses		
H1a	Trust is negatively related to specific privacy concerns.	Not supported
H1b	Distrust is positively related to specific privacy concerns.	Supported
H2	Consumers' specific privacy concerns are positively related to privacy risk perception.	Supported
H3a	Trust has a more significant effect on lowering error-related privacy concerns than distrust does on increasing it.	Not supported
H3b	Trust has a more significant effect on lowering access-related privacy concerns than distrust does on increasing it.	Not supported
H4a	Trust has a less significant effect on lowering collection-related privacy concerns than distrust does on increasing it.	Not supported
H4b	Trust has a less significant effect on lowering usage-related privacy concerns than distrust does on increasing it.	Not supported

4. Discussion

Even though many researchers acknowledge that trust and distrust are separate constructs, which are likely to have different effects on outcomes (McKnight & Chervany, 2001), I found little empirical research on privacy in e-commerce that incorporates distrust. However, trust scholars seeking to understand the governance of e-commerce acceptance might need to measure trust and distrust independently. To advance this understanding, I developed a theoretical model and that relates three major components to consumers' privacy risk perception: trust, distrust and privacy concerns. The paper provides insight into the impact of distrust, as a separate construct from trust and examines their impact on the different privacy concern dimensions. A valuable target group for e-commerce has been questioned about their perceptions and structural equation modelling technique has been applied to examine the proposed relationships.

(H1a) Trust's Impact on Privacy Concern Dimensions Differs greatly in impact and valence

The path coefficient between trust and reliability concerns is negative, but insignificant. Trust affects the concern dimensions 'secondary usage' and 'over-collection' positively, even though only the path towards 'secondary usage' is significant. At first, this seems to stand in contradiction to prior findings (e.g. Pavlou et al., 2007) and the theoretical reasoning that trust facilitates self-disclosure, since it deems the receiver competent and reliable in handling and protecting the disclosed content. However, the difference of the here-presented results can be due to the current conceptualization of trust. Given that trust relates to assumed task-reliability, the findings could indicate a moderating role of distrust in the trust-concern relation. That is, if individuals are suspicious about the motives of their banks, reliable and competent task execution can turn into something bad. Trust might then decrease error and access concerns, but increase consumers' concerns for 'over-collection' and 'secondary usage'. A similar linkage has been found by Sjöberg (2008).

(H1b) Distrust is positively related to Consumers' Privacy Concerns

Consumers, who distrust their bank more than others, show overall increased privacy concerns and associate more privacy risk with e-banking. This aligns with Cho's (2006) findings, which showed that distrust increases the risk associated with information disclosure and decreases consumers' willingness to disclose personal information.

(H2) Privacy Concerns Increase Consumers' Privacy Risk Perception

The results show that privacy concerns increase consumers' perceived privacy risk. This result builds on prior research that investigated the role of privacy concerns in privacy risk perception (e.g. Malhotra et al., 2004; Van Slyke et al., 2006; Keith et al., 2013).

(H3 & H4) Concern distinction according to responsiveness to task-reliability & value-orientation is not supported by the data

The results do not to support the asymmetric effects proposed in hypotheses 3 and 4. None of the equality constraints indicated a significant decrease in model fit and thus, the impact of trust and distrust – as they are conceptualized in this study – do not differ significantly from each other. Moreover, trust has even a smaller effect on reliability concerns than distrust. It appears therefore unlikely that privacy concerns differ mostly in their responsiveness to perceived task-reliability (i.e. trust) and value-incongruence (i.e. distrust). The formation of these dimensions may instead depend on another underlying variable, which has not been considered in this study. The modification indices, which suggested the inclusion of covariances among the concern dimensions, supports this argument, as it represent one or more common causes affecting these constructs (Tomarken & Waller, 2005).

In fact, neither trust nor distrust impacts reliability concerns significantly, but show instead a higher influence on 'over-collection' and 'secondary usage'. A possible explanation for this limited impact on 'reliability concerns' could lay in the distribution of endogenous and exogenous uncertainty associated with this concern dimension. The uncertainty comprised in access-related and error-related concerns is just partly endogenous. Online transactions involve the use of hardware and software at the final points of the transaction (i.e. electronic devices and desktop systems of the sender and the receiver) and at the data channel (i.e. software and servers of involved operators of the electronic market place) (Grabner-Kräuter & Kaluscha, 2003). Consequently, the occurrence of mistakes and security breaches just partly depends on the receiver's conduct. The other part of the uncertainty is exogenous. It relates to the complex dynamics of many environmental factors, including the functioning of technology components and the decision-making of additional actors. As such, these concerns can hardly be anticipated through judgements of the receiver's trustworthiness alone. Contrary, the concerns 'over-collection' and 'secondary usage' are mainly determined by the receiver and thus contain mostly endogenous uncertainty. They may, therefore, display greater sensitivity to consumers' trust and distrust levels.

Concluding Remarks

In previous research, it was frequently argued that trust reduces consumers' privacy concerns (Luo, 2002). However, the findings raise caution against generalizing this argument, as the impact and the valence might vary across different concern dimensions. Even though trust and distrust did not differ significantly in their absolute magnitude, each concern dimension was affected differently by trust and distrust. Former research has only reported accumulative results for privacy concerns. However, the paper shows that reporting these dimensions separately is useful to deepen the understanding of privacy concern formation and to create comparable and accumulative findings in this regard.

Also, the results indicate that reliability and competence may turn against the information receiver, if he or she is distrusted. While reliable and competent behaviour is certainly important for successful e-commerce, e-vendors might as well want to guide efforts on the display of their sincere value-orientation. Google's formal corporate motto "Don't be evil" could probably be seen as the most famous example of such an attempt.

Finally, if concern dimensions are mostly associated with exogenous uncertainty, the actor-related constructs distrust and trust may be less effective in governing risk perception. These insights may have important implications for e-vendors, who try to govern consumers' risk perception. For instance, third party privacy certificates, such as 'TRUSTed' (truste.com) or 'eTrust' (privacytrust.org), have been promoted to foster trust between the receiver and consumer (Luo, 2002; Larose & Rifon, 2007). These certificates, however, concern the receivers' conduct (i.e. collection, use, sharing of personal information and security policies) and thus address exclusively the endogenous uncertainty. Drawing from the results, it could be fruitful to address exogenous uncertainty actively (e.g. highlighting standards for technology components and maintenance, providing information about the conjunctive data channel, implementing insurance mechanisms…).

5. Limitations and Future Research Opportunities

The study findings are defined by a number of limitations that are highlighted in this section.

The size and the composition of the sample could limit the power and implications of the results. The sample size is relatively small and the recruiting procedure does not necessarily assure a completely randomized sample population. Especially the small proportion of male respondents is startling. As privacy concerns are of greater concern to women than men (Fogel & Nehmand, 2009), the results might not generalize over other populations. A larger, representative study would, therefore, be a meaningful extension. Moreover, the decision to participate in an online survey may indicate limited privacy concerns. The resulting selection bias implies that the concern and risk levels found in the sample may not necessarily generalize to other populations.

Trust and distrust were conceptualized according to Sitkin & Roth (1993). However, trust and distrust can be specified in many different ways, and scholars have not yet agreed on a common understanding of these concepts. Accordingly, conclusions drawn from the here presented results cannot be generalized for alternative conceptualizations. Hence, the results should be interpreted with their context specificity in mind.

As for all statistical models, SEM is only an approximation of reality, which omits many variables. Variable omissions present a misleading picture of the measurement and/or causal structure and commonly result in biased parameter estimates and inaccurate estimates of standard errors. The later added covariances among the concern dimensions may represent one or more common causes affecting these constructs. Although covariances could be specified to account for omitted variables, this provision does not necessarily solve the problem of biased parameter estimates and inaccurate standard errors. (Tomarken & Waller, 2005)

Further, it is important to recognize, that SEM cannot prove causation. SEM involves the analysis of correlations, which typically indicate association between two events, but do not necessarily imply a cause-effect relationship. Although SEM can be used to show that the correlations found in the data are in accordance with the causation predicted by theory, one should be aware that a large number of alternative, but statistically equivalent models could be supported by the same data. (Gefen et al., 2000)

Another limitation is the merge of two concern dimensions into a single construct called ‘reliability concerns’. The PCA results suggested that the data of ‘error’ and ‘access’ were not sufficiently discriminate. However, it does not necessarily make theoretical sense to combine both privacy concern dimensions into one overall measure (Farrell, 2010). It is up to speculation, whether the insufficient discriminant validity is due to sampling flukes, resemblance of measurement items or actual theoretical similarity of the dimensions ‘error’ and ‘access’ (Farrell, 2010). I indeed suggested that the dependence on consumers’ task-reliability judgement (i.e. trust) represents a communality

of both dimensions. One could argue that these communalities caused respondents' difficulties in differing between the error and access related items. However, various facts cast doubt on such an argument. First, I assumed some shared characteristics between 'access' and 'error', but I still regarded them as theoretically distinct. And so did Smith et al. (1996), who extensively checked and approved discrimination of each concern dimension. Ever since, numerous researchers have successfully applied this scale, without reporting any issues regarding the distinctiveness of 'error' and 'access'. Hence, although the merge was regarded as the most appropriate option in this case, it might not properly reflect the reality. The merge could therefore have affected the interpretation of the data or could have hidden certain aspects of the phenomenon from view. To exclude the rival explanations, a revision of Smith et al.'s (1996) scale could be a venue for future research.

A possible topic for future research might lay in endogenous and exogenous uncertainty associated with the different privacy concern dimensions. It has been speculated that the effectiveness of trust and distrust is related to the fraction of endogenous uncertainty associate with the different privacy concern dimensions. A study design that measures the involved endogenous and exogenous uncertainty and relates it to the efficiency of the trust and distrust mechanisms could represent a valuable extension to this study.

As previously discussed, the positive effect of trust on privacy concerns indicates a moderating role of distrust, where reliability is no longer perceived as beneficial. If the distrust level is high, reliability increases receivers' efficiency in conducting undesired actions and thus, increases privacy concerns. In the past, latent interaction modeling using structural equation modeling has been proposed to test such interaction effects. Future research should check for these effects. Steinmetz et al. (2011) provide an excellent overview of the existing approaches using structural equation modeling.

This study has assumed that their influence on privacy risk perception is mediated by privacy concerns. Previous research, however, has suggested that individuals might use trust and distrust as social heuristic for decision-making. Individuals might decide to cooperate or refrain from so-doing intuitively and in absence of formal monitoring (Kramer, 1999). Hence, using heuristics, consumers would probably abandon in-depth processing of specific privacy concerns and form their risk perception intuitively. A future study may provide a comprehensive theoretical and empirical account of these direct effects of trust and distrust on privacy risk perception.

References

Acquisti, A., Grossklags, J., (2003). Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. *Proceedings of the 2nd Annual Workshop on "Economics and Information Security"*, UC Berkeley.

Adams, J.E., Highhouse, S., Zickar, M.J. (2010). Understanding General Distrust of Corporations. *Corporate Reputation Review*, 13 (1), 38-51.

Anderson, J.C., Gerbing, D.W. (1988). Structural Equation Modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103 (3), 411-423.

Awad, N.F., Krishnan, M.S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, 30 (1), 13-28.

Baier, A.C. (1994). *Moral prejudices: Essays on ethics*. Cambridge: Harvard University Press.

Barber, B. (1983). *The Logic and Limits of Trust*. New Jersey: Rutgers University Press.

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems*, 19 (1), 211-241.

Bergen, M., Shantanu, D., Walker Jr., O.C. (1992). Agency Relationships in Marketing: A Review of the Implications and Applications of the Agency and Related Theories. *Journal of Marketing*, 56, 1-24.

Boyd, D., Crawford, B. (2012). Critical Questions for Big Data. Information, *Communication & Society*, 15 (5), 662-679.

Bravo, R., Montaner, T., Pina, P.M. (2012). Corporate brand image of financial institutions: a consumer approach. *Journal of Product & Brand Management*, 21 (4), 232-245.

Cho, J. (2006). The mechanism of trust and distrust formation and their relational outcomes. *Journal of Retailing*, 82 (1), 25-35.

Culnan, M.J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*, 17 (3), 341-363.

Culnan, M.J., Armstrong, P.K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science*, 10 (1), 104-115.

Deutsch, M. (1960). The effect of motivational orientation upon trust and suspicion. *Human Relations*, 13, 123-140.

Dinev, T., Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, 23 (6), 413-422.

Dinev T., Hart P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17 (1), 61-80.

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

epp.eurostat.ec.europa.eu, "Internet use statistics - individuals", online available at: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Internet_use_statistics_-_individuals (visited: 17.09.2014).

etrust.org, “Privacy Certification“, online available at: http://www.privacytrust.org/certification/privacy/index.html (visited: 15.11.2014)

Farrell, A.M. (2010). Insufficient discriminant validity: A comment on Bove, Pervan, Beatty, and Shiu (2009). *Journal of Business Research*, 63, 324-327.

Featherman, M.S., Miyazaki, A.D., Sprott, D.E. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal for Service Marketing*, 24 (3), 219-229.

Field, A. (2009). *Discovering Statistics Using SPSS* (3rd Edition). London: Sage.

Fishbein, M., Ajzen, I. (1957). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Massachusetts: Addison Wesley.

Fogel, J, Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25, 153-160.

Frewer, L. (1999). Risk Perception, Social Trust, and Public Participation in Strategic Decision Making: Implications for Emerging Technologies. Ambio, 28 (6), 569-574.

Gabarro, J. J. (1978). The Development of Trust, Influence, and Expectations. In A. G. Athos, Gabarro, J. J. (Eds.) *Interpersonal Behavior: Communication and Understanding in Relationships* (pp. 290-303). New Jersey: Engle-wood Cliffs.

Garcia-Retamero, R., Müller, S.M., Rousseau, D.L. (2012). The Impact of Value Similarity and Power on the Perception of Threat. *Political Psychology*, 33 (2), 179-193.

Gefen, D., Straub, D.W., Boudreau, M. (2000). Structural Equation Modeling Techniques and Regression: Guidelines For Research Practice. *Communications of Association for Information Systems*, 4 (7), 1-79.

Grabner-Kräuter, S., Kaluscha, E.A. (2003). Empirical research in on-line trust: a review and critical assessment. *Human-Computer Science*, 58, 783-812.

Herzig, C., Moon, J. (2013). Discourses on corporate social ir/responsibility in the financial sector. *Journal of Business Research*, 66, 1870-1880.

Hiranandani, V. (2011). Privacy and security in the digital age: contemporary challenges and future directions. *The International Journal of Human Rights*, 15 (7), 1091-1106.

Hoffman, D.L., Novak, T.P., Peralta, M.A. (1999). Information privacy in the marketspace: implications for the commercial uses of anonymity on the web. The Information Society, 15 (2), 129-139.

Hsiao, R.L. (2003). Technology fears: distrust and cultural persistence in electronic marketplace adoption. *Journal of Strategic Information Systems*, 12, 169-199.

Jagadish, H.V. (2012). Challenges and Opportunities with Big Data - A community white paper developed by leading researchers across the United States.

Junglas, I.A., Johnson, N.A., Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17, 387-402.

Kee, H. W., Knox, R. E. (1970). Conceptual and Methodological Considerations in the Study of Trust and Suspicion. Journal of Conflict Resolution, 14, 357-366.

Keith, M.J., Babb Jr., J.S., Furner, C.P., Abdullat, A. (2010). Privacy Assurance and Network Effects in the Adoption of Location-based Services: an Iphone Experiment. *International Conference on Information Systems 2010 Proceedings*. Paper 237.

Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, 71, 1163-1173.

Kline, R. B. (2010). *Principles and Practices of Structural Equation Modeling*. New York: The Guilford Press.

Kramer, R.M. (1999). Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. *Annual Review of Psychology*, 50, 569-598.

Larose, R., Rifon, N.J. (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *The Journal of Consumer Affairs*, 41 (1), 127-149.

Lee, S.M., Park, S.H., Yoon, S.N., Yeon, S.J. (2007). RFID based ubiquitous commerce and consumer trust. *Industrial Management & Data Systems*, 107 (5/6), 605-617.

Lewicki, R.J., McAllister, D.J., Bies, R. (1998). Trust and Distrust: New Relationships and Realities. *Academy of Management Review*, 23 (3), 438-458.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54, 471-481.

Liao, C., Liu, C.C., Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, 10, 702-715.

Lim, N. (2003). Consumers' perceived risk: sources versus consequences. *Electronic Commerce Research and Applications*, 2, 216-228.

Luhmann, N. (1989). *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität* (3rd Edition). Stuttgart: Enke.

Lui, S.S., Ngo H. (2004). The role of trust and contractual safeguards on cooperation in non-equity alliances. *Journal of Management*, 30, 471-485.

Luo, X. (2002). Trust production and privacy concerns on the Internet - A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, 31, 111-118.

Malhotra, N.K., Kim, S.S., Agarwal, J. (2004). Internet Users' Information Privacy (IUIPC). The Construct, the Scale and a Causal Model. *Information System Research*, 15 (4), 336-355.

Marsh, S., Dibben, M.R. (2005). Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side. In P. Herrmann, Issarny, V., Shiu, S. (Eds.), *Trust Management, Third International Conference Proceedings,* iTrust 2005 (pp. 17-33). Paris: Springer.

McKnight, D.H., Chervany N.L. (2001). Trust and Distrust Definitions: One Bite at a Time. In R. Falcone, Singh, M., Tan, Y.H. (Eds.), *Trust in Cyber-societies: Integrating the Human and Artificial Perspectives* (pp. 27-54). Berlin: Springer.

Mendez, F. (2005). The European Union and cybercrime: insights from comparative federalism. *Journal of European Public Policy*, 12 (3), 509-527.

Möller, N., Hansson, S.O., Peterson, M. (2006). Safety is more than the antonym of risk. *Journal of Applied Philosophy*, 23 (4), 419-432.

Nickel, P.J., Vaesen, K. (2012). Risk and Trust. In S. Roeser, Hillerbrand, R., Sandin, P., Peterson, M. (Eds.), *Handbook of Risk Theory* (pp. 858-873). New York: Springer Science + Business Media.

Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron?. *Boston University Law Review*, 81, 101-131.

Omariba, Z.B., Masese N.B., Wanyembi, G. (2012). Security and privacy of electronic banking. *International Journal of Computer Science Issues*, 9 (4), 432-446.

oxforddictionaries.com, "concern", online available at: http://www.oxforddictionaries.com/definition/english/concern (visited: 05.05.2014).

oxforddictionaries.com, "privacy", online available at: http://www.oxforddictionaries.com/definition/english/privacy (visited: 22.04.2014).

Patton, J.W. (2000). Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places. *Ethics and Information Technology*, 2, 181-187.

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

Poortinga, W., Pidgeon, N.F. (2005). Trust in Risk Regulation: Cause or Consequence of the Acceptability of GM Food?. *Risk Analysis*, 25 (1), 199-209.

Raithel, S., Wilczynski, P., Schloderer, M.P., Schwaiger, M. (2010). The value-relevance of corporate reputation during the financial crisis. *Journal of Product & Brand Management*, 19 (6), 389-400.

Schoorman, F.D., Mayer, R.C., Davis J.H. (2007). An integrative model of organizational trust: Past present and future. *Academy of Management Review*, 32 (2), 344-354.

Siegrist, M., Cvetkovich, G., Roth, C. (2000). Salient Value Similarity, Social Trust, and Risk/Benefit Perception. *Risk Analysis*, 20 (3), 353-362.

Sitkin, S.B., Roth, N. (1993). Explaining the Limited Effectiveness of Legalistic Remedies for Trust/Distrust. *Organization Science*, 4 (3), 367-392.

Sjöberg, L. (2000). Factors in Risk Perception. *Risk Analysis*, 20 (1), 1-11.

Sjöberg, L., Fromm, J. (2001). Information Technology Risks as Seen by the Public. *Risk Analysis*, 21 (3), 427-441.

Sjöberg, L., Wester Herber, M. (2008). Too much trust in (social) trust? The importance of epistemic concerns and perceived and antagonism. *International Journal of Global Environmental Issues*, 8 (1/2), 30-44.

Smith, H.J., Milberg, S.J., Bruke, S.J. (1996). Information Privacy: Measuring Individual's Concerns About Organizational Practices. *Mis Quarterly*, 20 (2), 167-196.

Steinmetz, H., Davidov, E., Schmidt P. (2011). Three Approaches to Estimate Latent Interaction Effects: Intention and Perceived Behavioral Control in the Theory of Planned Behavior. *Methodological Innovations Online*, 6 (1), 95-110.

Stone, E.F., Gardner, D.G., Gueutal, H.G., McCLure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 68 (3), 459-468.

Tomarken, A.J., Waller, N.G. (2005). STRUCTURAL QUATION MODELING: Strengths, Limitations, and Misconceptions. Annual Review of Clinical Psychology, 1, 31-65.

truste.com, "TRUSTed Data Privacy Certification", online available at: http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-data (visited: 15.11.2014)

Udo, J.G. (2001). Privacy and security concerns as major barriers for e-commerce: a survey study. *Information Management & Computer Security*, 9 (4), 165-174.

Van Slyke, C., Shim, J.T., Johnson, R., Jiang, J. (2006). Concern for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems*, 7 (6), 415-444.

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

Whipple, J.M., Frankel, R (2000). Strategic alliance success factors. *Journal of Supply Chain Management*, 36 (3), 21–28.

Xu, H., Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, 19, 137-149.

Xu, H., Teo, H.H. (2004). Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective. 25th *International Conference on Information Systems 2004 Proceedings*, Paper 64.

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, 111 (2), 212-226.

Zimmer, M. (2008). More on the "Anonymity" of the Facebook dataset – it's Harvard College, MichaelZimmer.org Blog, Online available at: http://www.michaelzimmer.org/2008/10/03/more-on-the-anonymity-of-the-facebook-dataset-its-harvard-college (visited: 02.04.2014).