Wirtschaftliche Untersuchungen,
Berichte und Sachverhalte

IW-Report 19/2018

Trust and Privacy

How Trust Affects Individuals' Willingness to Disclose Personal Information

Ansprechpartner:
Christina Heldman und Prof. Dr. Dominik H. Enste

Düsseldorf Institute for Competition Economics (DICE)
IW Köln, Kompetenzfeld Verhaltensökonomik und Wirtschaftsethik

Düsseldorf / Köln, 17.05.2018

INSTITUT DER DEUTSCHEN WIRTSCHAFT

Table of Contents

Abstract

Even though people regularly express concern about sharing personal information online and fear a loss of privacy, their behavior seldom matches their opinions – A phenomenon called *Privacy Paradox* and researched for over 20 years. Several influencing factors have been identified. A central one of these is trust, which strongly impacts the relationship between general concerns and actual behavior. This study investigates the impact of trust on the decision to disclose sensitive information online and examines the antecedents of that trust, focusing on the disposition to trust using a computerized laboratory experiment. Results indicate that dispositional trust determines the level of trust placed in the recipient of private data, especially when the person is unfamiliar with this recipient. This knowledge can be useful for business and politics in the design of marketing strategies and consumer protection policies. The study furthermore provides valuable insights on the relatedness between trust measures, which are discussed.

JEL-Classification:

C90 - Design of Experiments, General

D91 - Role and Effects of Psychological, Emotional, Social, and Cognitive Factors on Decision Making

O33 - Technological Change: Choices and Consequences; Diffusion Processes

1 Introduction

The internet has long ceased to be “uncharted territory” as Angela Merkel called it five years ago. The percentage of internet users worldwide has grown rapidly from ten percent in 2006 to 45 in 2016. In Germany, 90 percent of the population have access already (Worldbank, 2018). With the ubiquity of the World Wide Web, the possibilities to communicate increase constantly. Social Networks, blogs and photo- and video-sharing platforms allow people to share personal information anywhere and anytime. Sharing information about oneself is labeled self-disclosure and has many perks: It strengthens relationships, grants access to services and simply makes people happy (Tamir & Mitchell, 2012). Given these benefits, digital platforms that allow for self-disclosure enjoy high popularity and have now become part of our everyday life.

The growing opportunities come with a risk though: the loss of privacy. Over the past years, leading companies have been involved in privacy scandals, most prominently and recently Facebook which had known about the practices of Cambridge Analytica without taking measures to stop them. This negligence has allowed the political consulting firm to collect data of up to 87 million Facebook users and create differentiated personality profiles, while Facebook is now struggling to maintain its reputation. It comes as no surprise that the social media is repeatedly deemed as untrustworthy in user surveys (e.g. Reuters, 2018; vzbv, 2015)

The users' concerns do not translate into behavior though. Social Networks report increasing numbers of registrations. Facebook recorded 1.45 billion daily active users by the end of 2017 (Facebook, 2018a) and the photo-sharing service Instagram, which belongs to the same company, is used by 800 million people worldwide every day (Omnicore, 2018). The discrepancy between privacy attitudes and actual behavior is called Privacy Paradox – a phenomenon first named twelve years ago and investigated ever since (Barnes, 2006). Several explanations have been proposed for this behavior: Some scholars believe in a deliberate Privacy Calculus, which describes the weighting of the costs and benefits of self-disclosure, while others explain the contradictory behavior by a misconception of the advantages and risks. As recent research argues, the paradox most likely stems from a combination of the two and is strongly influenced by personality traits and situational factors (e.g. Kehr et al., 2015).

Trust has been identified as a central one of these factors. Trust comes into play when people are faced with uncertainty and risk and allows to interact, even if one cannot be sure that the other person will not act opportunistically. When disclosing private information online, people are constantly faced with such uncertainty and risk, as they can seldom tell how their data will be stored and processed and who will access it. Trusting the recipient of personal information

helps overcome the fear of an abuse of data and allows for interactions in the presence of general skepticism (Metzger, 2004).

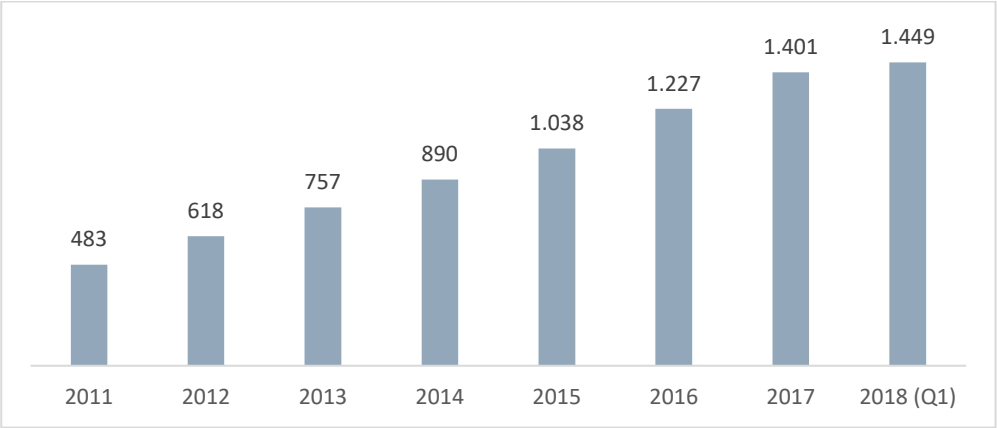
With trust being a central driving force of the willingness to engage online, it is of high interest for businesses and politicians to have knowledge of how this trust is built. This study will explore the antecedents of consumer trust online and investigate how it affects the decision to share private information online using a literature review and an experiment. The antecedent of main interest is the disposition to trust, which has been identified as a central driver when situations are new and people cannot infer from past experience whether another person will likely act in their best interest – An instance that often occurs online, with new businesses opening every day, technologies changing and Social Networks becoming bigger and bigger. To isolate the effect of dispositional trust, further personal characteristics are controlled for.

2 Self-Disclosure

Every day, people share information about themselves, their opinions, thoughts or experiences. This process is called self-disclosure and serves various purposes: It is essential to most communication and increases mutual understanding, which in turn creates intimacy. Self-disclosure is thus necessary to produce social ties and can be seen as the foundation of developing and maintaining social relationships (Altman & Taylor, 1973; Joinson, 2008). By enabling to interact and socialize, people benefit highly from it. Experiments have shown that self-disclosure activates brain regions that are associated with reward and is of such high intrinsic value to humans that they are willing to forego a payment to be allowed to talk about themselves (Tamir & Mitchell, 2012). In addition, sharing personal information with organizations is necessary for authentication or personalization, which can improve product advice and design (Joinson, 2008).

Within the internet, the possibilities to self-disclose increase continuously. The so-called Social Web which includes Social Networks, blogs and picture- and video-sharing platforms allows individuals to share knowledge and private information with a large number of other users instantly (Taddicken, 2014). These offers receive an increasing public reception: The number of daily active Facebook users for example has almost doubled in the last 5 years (see figure 2-1), while Instagram is visited by 500 million people every day, which is five times as much as in 2016 (Facebook 2017, 2018a; TechCrunch, 2017).

Figure 2-1: Number of daily Facebook users worldwide (in millions)



Source: Facebook, 2017; 2018a

Not only does the technological advancement create new platforms to communicate, it also multiplies the number of services available, for example in e-commerce. Here, users are asked to share private information such as name, address and credit card details in order to register and order products and information on preferences and tastes can help companies to improve

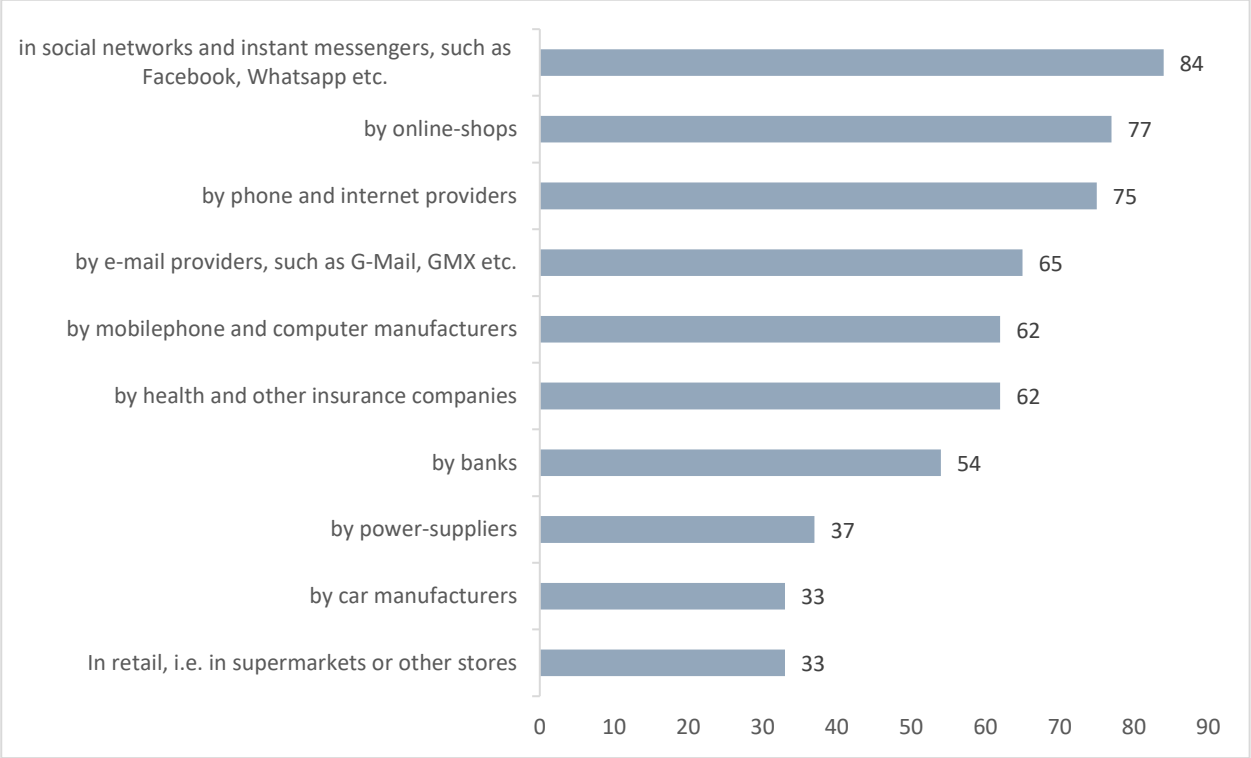
their offers (Lee & Cranage, 2011). Given the advantages of self-disclosure and its high popularity, personal data has become a prime source of income for many companies, such as Facebook, which offers its products without charge and finances itself in part with personalized advertisement based on user data (Facebook, 2018b).

Even though it is beneficial to share private information, users also have to consider the associated risk, namely the loss of privacy. Privacy has been described as "the right to be let alone" (Warren & Brandeis, 1890, p. 193) or the "selective control of access to the self or to one's group" (Altman, 1976, p. 8). It can be clustered into four dimensions: *physical privacy* regarding the territorial surroundings of a person, *social privacy* which relates the decision to interact with or withdraw from other people, *psychological privacy* concerning the ability to control his own feelings and thoughts and *informational privacy* which describes the right to control the collection, storage and use of personal data – a dimension which has gained high regard with the rise of the internet (Burgoon, 1982; Leino-Kilpi et al., 2001). When an individual decides on sharing personal information with other people or an organization, he has to bring his desire for interaction in line with his need for informational privacy (Altman, 1975). While this is already a sensitive task in offline contexts, for example in communicating with other people, it is even more complex in online environments. There, people cannot be sure anymore, who accesses their information, for example when third parties such as advertising companies are integrated into platforms or when the privacy settings of Social Networks are unclear (datenschutz nord, 2015). Elaborate systems make the permanent storage and duplication of data from different sources possible (Papacharissi & Gibson, 2011) and allow to combine and analyze information which compromises the anonymity of users (see for example Kosinksi et al., 2013, who showed that a couple of Facebook-Likes make it possible to draw inferences about sensitive personal information such as sexual orientation or relationship status). These developments are aggravated by the speed at which technologies change and the uncertainty of future use of data (Mayer-Schönberger & Cukier, 2013).

Given these risks, people are more and more afraid of losing control over their data and privacy online and the skepticism regarding digital services is increasing. In a survey among more than 8000 European citizens, only 29 percent say they feel in control over the information gathered about them, 44 percent believe that companies do not respect the privacy of personal data and almost 60 percent do not know where and by whom personal information is collected and stored (Vodafone Institute for Society and Communications, 2016). Another study among 1000 Germans emphasizes the fear that online services gather too much data: 84 percent agree that Social Networks such as Facebook and Whatsapp collect more information than necessary, followed by e-commerce providers (see figure 2-2). The respondents fear that their private data is (mis-)used by unknown entities and that companies, other people or the government have too much knowledge about them (TNS Emnid, 2015).

Figure 2-2: Areas, where too much data is collected (numbers in percent)

Question: "Where do you feel like there is too much data collected from users?"; multiple answers allowed



Source: TNS Emnid, 2015

In the light of these concerns, it is expected that users of online services are cautious and scarcely share private information. However, the attitudes do not translate into behavior, as the previously mentioned statistics and several studies show. In an early experiment, Spiekermann et al. (2001) compare attitudes towards privacy with actual behavior in an e-commerce setting and find that even though participants claimed to put a great value on keeping their information private, they willingly answered highly intimate questions. In another study people had to report their willingness to disclose several information first and were asked to actually provide them a few weeks later. The results confirm that subjects' behavior does not match their originally stated intentions (Norberg et al., 2007). Within the Social Web, Taddicken (2014) reports that out of 2739 survey participants in Germany, more than half provide basic and factual information such as name, birthday and e-mail address. Sensitive information like photos, thoughts and feelings are shared frequently or at least once by over 50 percent as well, with one third not restricting the access to that information. In addition, only a few people read privacy policies even though they consider them important and so most accept the policies without having read them or understood their consequences (Bitkom, 2015; DIVSI, 2015).

This gap between attitudes and behavior is called *Privacy Paradox*, a term first used by Barnes (2006) to describe the disclosure behavior of young people in Social Networks. Its causes have not been entirely made out, but there are several possible explanations. Some scholars advocate the *Privacy Calculus*, according to which people base their decision to disclose information on a rational weighting of the possible risks against the expected benefits. Self-disclosure is thus a fully rational decision and users are willing to give up some of their privacy if it maximizes the expected payoff and minimizes the potential harm. Within the Privacy Calculus, a discrepancy between general privacy attitudes and actual behavior can therefore be explained by situational factors (Culnan & Armstrong, 1999; Liao et al., 2011; Li et al., 2011).

This model has been challenged by several scholars. Just as in economics in general, a growing body of literature doubts that people are able to fully comprehend the costs and benefits of a decision which is why their behavior differs from that of a fully rational actor. This line of research is called *Behavioral Economics* and states that people try to make rational cost-benefit analyses, but are bound by their limited cognitive resources. In complex environments, such as the online world, it is impossible to collect all information necessary for a fully informed decision. This can cause misjudgments in payoffs, risks and their probabilities of occurrence and consequently behavior inconsistent with a person's long-term interests (Simon, 1959; Tversky & Kahneman, 1974). Within this framework, the Privacy Paradox stems from limited information and a miscalculation of risks, costs and probabilities. This theory is supported by various experiments (Acquisti, 2004; Acquisti & Grossklangs, 2005; Keith et al., 2012; Acquisti et al., 2015).

Furthermore, the literature has identified several personal characteristics that influence users' decision to self-disclose, such as general privacy concerns, which affect the assessment of risks and benefits (Xu et al., 2008), and the closely related general willingness to share (Taddicken, 2014). Online experience has also been identified as a predictor of self-disclosure, as for example Metzger (2004) finds, as well as gender with women being more concerned about their privacy than men (Youn & Hall, 2008). Cultural influences are investigated by Wu and Lu (2013), who report that users who live in individualistic countries such as Germans or Americans share more information than those from collectivist societies like China. The *Big Five* personality traits have also been subject to empirical analyses: Lee et al. (2014) for example report that extraverts and narcissists share more information in Social Networks while neuroticism and conscientiousness have a negative influence.

The perspectives and results on self-disclosure are not mutually exclusive but most likely interact. The assessment of risks and benefits in the Privacy Calculus is expected to be strongly influenced by individual characteristics and cognitive limitations. Several authors have therefore proposed an extension to the Privacy Calculus model, such as Wilson and Valacich (2012), who expand it by situational factors, factors that contribute to irrational behavior and general privacy

concerns. Kehr et al. (2015) define privacy-related decisions as a “situation-specific trade-off of privacy-related risk and benefit perceptions, bounded by dispositional tendencies and irrational behavior” (p. 608). Both extensions not only take personal characteristics into account, but also highlight the importance of situational factors. One of the most central individual and personal factor influencing self-disclosure is trust, which is the focus of the present study and will be described in the following sub-chapter.

3 Trust

Human interaction is a complex process. It is often impossible to fully predict each other's behavior and one cannot always be certain, that the other party will act in one's own best interest. Without means to reduce that complexity, people would have to consider and take precautions for all possible reactions of everybody involved in a decision, which would lead to prohibitive transaction costs. Laws and rules govern situations to a large extent, but still one can never be certain that they will be abided. One of the most important methods to reduce complexity apart from rules is trust. Relying on other people without being certain that they won't behave opportunistically requires the trust in the other party (Gefen, 2000; Fukuyama, 1995; Rousseau, 1998). Trust can thus be defined as a voluntary investment of resources in somebody without being able to enforce his cooperation (Coleman, 1990). Mayer et al. (1995) define trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action […], irrespective of the ability to monitor or control that other party" (p. 712) and similarly, Rousseau et al. (1998) describe trust as a "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (p. 395). Since people depend on others in many aspects of life, trust plays a significant role in the economic system by greatly facilitating or even making transactions possible (Arrow, 1972).

There are many more definitions, depending on the disciplinary lens it is seen though, e.g. psychology, sociology or economics (Rousseau et al., 1998). In order to unify the different conceptions, several scholars have proposed composite conceptualizations of trust. These include Mayer et al. (1995) with their model of Organizational Trust, where trust, its antecedents in terms of characteristics of the *trustor*, i.e. the person who relies on somebody else, the *trustee* who is relied upon, the environment and the outcomes are distinguished. McKnight et al. (1998) developed an interdisciplinary model in which they define trust-related behavior as a result of the concepts trust in general, trust in the institutional environment and trust in a specific other. Another way to model trust is to view it as a process over time, such as Kenning (2002), who argues that trust in a vendor is based on different aspects depending on the length of the relationship. While at first reputation exerts a dominant impact, individual experiences become more important over time. Personal characteristics of the trustor and trustee are said to influence the process permanently and independent of time.

3.1 Trust in the Online Environment

Trust comes into play when a decision is associated with uncertainty and risk and so it might be even more important in online interactions than offline. Predicting another person's behavior is harder, the more distant he or she is physically and psychologically. On the internet, people do

not interact face to face and additionally online transactions are technologically complex and hard to comprehend, partly because computers and not humans conduct most actions – a development that adds to the uncertainty of a situation (McKnight & Chervany, 2001; Kim et al., 2008; Rusk, 2014). Examples for these uncertainties are found in e-commerce, where vendors and products cannot be personally examined and consumers face the risk of receiving low quality or being scammed altogether. They might be even more present when disclosing information, where a person can often not be sure about what will happen to his or her data now or in the future.

Trust allows overcoming the feeling of insecurity and has therefore been identified as one of the most important factors in the decision to engage in online actions and transactions. Several studies investigate the role of trust in the online environment. The majority focuses on e-commerce and the decision to interact with an online-shop. One of the first and most influential studies in this domain was conducted by Gefen (2000), who investigates attitudes towards Amazon and reports that trust in the homepage exerts a positive influence on the willingness to inquire information and products from the shop. Metzger (2004) analyzes the behavior of students in a fictitious online-shop for posters where orderings could be made after providing several, partly highly sensitive information and finds that amongst other factors, trust in the website predicted disclosure. Kim et al. (2008) followed online consumers through an actual shopping process and also identify trust in an online-shop as a strong positive impact on the intention to purchase a product. The previously described model of trust developed by McKnight et al. (2002) was applied to online-shopping as well, where the hypothesized relationships between different types of trust and the intention to interact with an online service provider are proven to be significant.

Online-shopping is a well-established part of everyday life now, and so the focus of more recent studies has shifted to the disclosure of information as a main act itself rather than a byproduct of purchasing products and services. Mesch (2012) for example interviewed 2253 adults regarding the disclosure of personal information using real names, usernames or anonymously on the internet. He reports that the disclosure of identifiable information is closely related to the degree of trust on news websites and Social Networks. Joinson et al. (2010) conducted an online experiment where they confronted participants from 17 countries with intimate web surveys that differed in the strength of the privacy policy and the level of trustworthiness which was manipulated using language, the host of the survey and the use of incorporated advertisement. They show that high levels of perceived trustworthiness increase perceived privacy and lead to self-disclosure even when the actual privacy is low.

Based on these and related findings, trust can be recognized as a central variable in understanding the Privacy Paradox, i.e. why peoples' attitudes towards privacy often do not match their

actual behavior. Even if a person is generally skeptical and scared of misuse of their personal data, he can overcome these feelings and provide personal information when faced with a counterpart he trusts.

3.2 The Disposition to Trust

With trust being a key factor in most interactions, understanding its antecedents is of high interest for practitioners and research. As mentioned before, there are a lot of different approaches to model trust, but there is one aspect most of them have in common: the importance they attribute to the initial trust level of an individual, which is also referred to as *generalized trust* (Ripperger, 2003)*, disposition to trust* (McKnight et al., 1998) or *trust propensity* (Mayer et al., 1995). It is a stable individual characteristic based on lifelong experience and socialization and describes the general willingness to trust another party independently of situational cues or information about the trustee (Michalski & Schupp, 2009; Gefen, 2000 resp. Fukuyama, 1995; Rotter, 1971). The propensity to trust has for example been incorporated in the model of Mayer et al. (1995), who argue that it strongly influences the perceptions of another person's trustworthiness – a hypothesis supported by a meta-study of 119 articles that empirically analyze trust (Colquitt et al., 2007). The disposition to trust "colors our interpretation of situations and actors" (McKnight & Chervany, 2001, p. 45) which makes it especially influential in novel situations. When a person has not been able to gather information or experience, it is difficult to form an opinion on the counterpart's characteristics and whether he will act in the trustee's best interest. It is the general expectancy of trustworthiness that impacts the decision on how much a person is willing to rely on another party then (Mayer et al., 1995; Rotter, 1971).

When engaging online, people are constantly faced with unknown counterparts, such as new e-commerce sites or the undefined audience of Social Network activity, and there is often no experience or historical evidence to base the assessment of trustworthiness on. The trust they place in these offers and platforms is therefore strongly driven by their dispositional trust. The previously mentioned Kim et al. (2008) report that dispositional trust is a central component of trust in a vendor, as well as Liao et al. (2011) who experimentally show that trust in the internet in general is positively affected by the participant's initial tendency to trust. Christofides et al. (2009) analyze students' disclosure and control of personal information on Facebook and search for influencing personality factors. The majority of the participants had posted information like their birthday and relationship status and were very likely to post private pictures. The use of privacy settings was negatively related to individual trust attitudes, as the authors discovered.

After a trustor has engaged in several interactions with a trustee and becomes more familiar with him, he will place higher weight on actual information than on his general tendency when

deciding to trust him (McKnight et al., 1998). This relationship has also been analyzed empirically. Gefen (2000) finds that both familiarity and the disposition to trust are strong predictors of trust in a specific web vendor. He argues that familiarity works two ways: If people are familiar with a homepage and its procedures and technology, complexity is reduced which increases the willingness to use that service. Familiarity also asserts and impact on trust by allowing people to anchor their expectations on specific past behavior. It can thus either strengthen trust or destroy it, depending on how the trustee has behaved in the past. Schoenbachler and Gordon (2002) show that past experience with a company positively affects trust, because if people made the experience that their data is used responsibly they are more willing to keep up or deepen their relationship. A similar finding has been made van Slyke et al. (2006), who argue that when an individual is familiar with a web merchant and the way he protects personal data, this knowledge will dominate the impact of general attitudes.

Besides familiarity with a certain provider, familiarity with the institutional environment also encourages trust and trusting behavior. According to McKnight et al. (2002), experience with an institutional environment in terms of general experience with the web, strongly influences trust in that environment, because it gives users an impression of normality and safety. This *institution-based trust* in turn impacts the level of trust in the specific web vendor, who is situated in that institutional environment. An analysis of the Oxford Internet Survey showed that confidence in the internet increases while the perception of risk decreases with the frequency it is used (Dutton & Shepherd, 2006). In a telephone survey of 1200 US-citizens, people with higher online skills stated to be less afraid of sharing personal information. The authors presume that this confidence stems from the belief that their skills will help them to avoid dubious organizations (Turow & Hennesy, 2007). Metzger (2004), reports that participants who had spent more time online and had shared more information in the past, disclosed more private information to an unknown web vendor. She explains that relationship with the truism “that the best predictor of future behavior is past behavior” (p. 4). A further explanation is that people who have experience with self-disclosure e.g. for personalized marketing are more likely to have experienced its benefits before and are thus more willing to share private information. Another reason might be that people who have already shared information might feel like “the damage has already been done” (Metzger, 2004, p. 4).

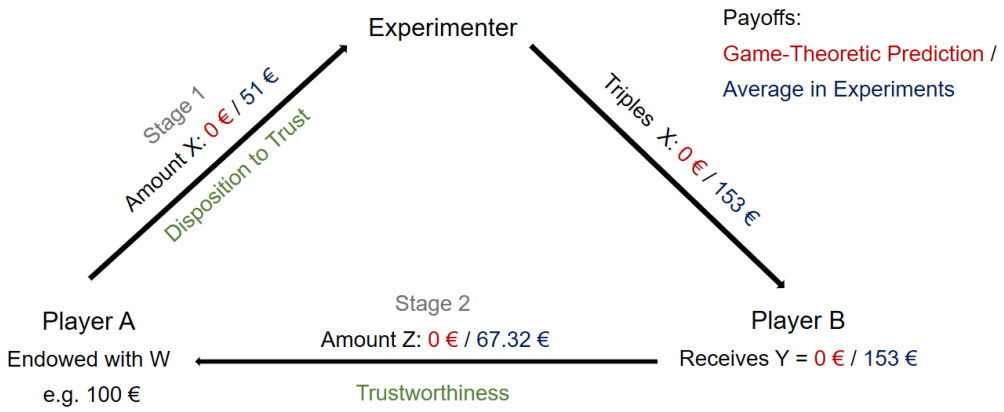
4 The Experiment

To gain further insight into how trust affects self-disclosure and how the disposition to trust alongside familiarity with the recipient of personal information and experience with the institutional environment determine that trust, a laboratory experiment was run at the DICE Lab for Experimental Economics. In the first stage, the *disposition to trust* was measured in an interactive game. In the second stage, the data for the remaining variables *familiarity, experience, trust in recipient* and *self-disclosure* was collected using a questionnaire

4.1 The Setup

The disposition to trust was measured in two ways: The Trust Game and a questionnaire. The Trust Game, developed by Berg et al. (1995), is an interactive game, which is aimed at measuring peoples' willingness to trust and their trustworthiness. In the classic setup, one player A (the trustor or investor) can transfer money to another anonymous player B. This amount is tripled, so the second player gets three times what Player A sent him. In the second stage, Player B has the option to send money back to Player A. The first stage indicates how trusting Player A is, since he shares money without knowing whether he will get anything in return. The second stage sheds light on the trustworthiness of Player B, who can decide whether to comply with A's positive expectations or to exploit his trust. In the unique Nash equilibrium prediction, Player A does not send any money, since a fully rational and self-interested Player B would keep it all to himself (Berg et al., 1995). In practice, however, most people do send money and get something in return, as a meta-study of 15 Trust Games in Germany illustrates. On average, Players A send 51 percent of their endowment, while Players B return 44 percent. This deviation from the game-theoretic prediction has been recorded in 34 other countries, but regional differences prevail (Johnson & Mislin, 2011). Figure 4-1 depicts the sequence of the experiment and contrasts the game theoretic prediction with the observations in reality.

Figure 4-1: The Trust Game



Source: Enste et al., 2016

Another way to measure the disposition to trust are questionnaires. In surveys like the World Values Survey (WVS) or the European Social Survey (ESS), subjects have to reply to the question "Generally speaking, would you say that most people can be trusted, or that you could not be too careful in dealing with people?" (ESS, 2014; WVS, 2017). Others ask more detailed questions like the previously mentioned McKnight et al. (2002), who measure the disposition to trust with a total of 12 questions. Answers are usually given on a scale, for example from 0 to 10, where 0 indicates that "you can't be too careful" and 10 means that "most people can be trusted" (ESS, 2014). As both measures are commonly used and it is unclear, which captures dispositional trust more accurately, they are both implemented in this study. This method can also provide insights on the relatedness between survey and experimental measures.

The remaining antecedents of trust *familiarity* and *experience* and also *trust in the recipient* were measured using a questionnaire. The questions were later condensed into one variable each. For better identification of trust and familiarity, two treatments were introduced which consisted of different recipients of the information shared. Half of the subjects were informed that the data was processed by the Düsseldorf Institute for Competition Economics (DICE), an institution located at the university and hosting the experiment. The other half of the subjects was told that their data was transferred to the Institute of Economic Research Cologne (IW Köln), an institution that is assumed to be less known, especially by students without an economic background. Introducing two recipients, a higher variation in familiarity and trust in the recipient is expected which can help in identifying effects.

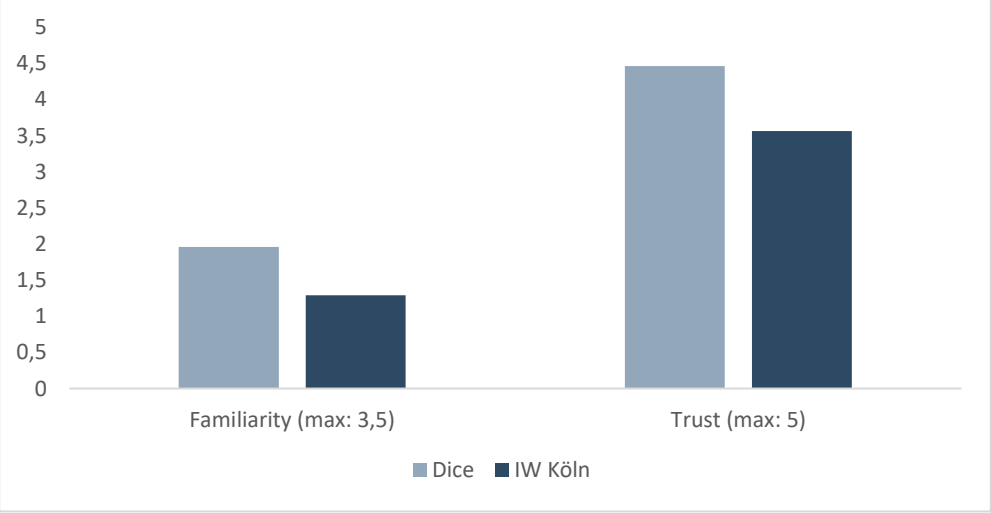
To measure self-disclosure, participants were presented with a survey developed by Joinson et al. (2008), which consisted of highly sensitive questions, such as the number of sexual partners, the monthly income or political party affiliation. Subjects had the choice to reply to the questions or click the button “I prefer not to say”. The number of questions answered was then used as an indicator for self-disclosure. As the focus of this study was online self-disclosure, the questions were posed and had to be answered on a computer screen, in order to bring the decision-making closer to the online environment.

4.2 Results and Discussion

A total of 48 students participated- 24 per treatment. In the first treatment, participants were given the information that the questionnaire was later processed by the DICE. This group consisted 15 female and 9 male participants. The second group, who was told that their data was given to the IW Köln, consisted of 7 females and 17 males. The majority of students in both treatments were in their bachelor-studies (13 in each group) and the average age was 24 years (SD=4.44).

Descriptive analysis shows that participants were more familiar with the DICE than the IW Köln and placed more trust in it (see figure 4-2), which was already expected as the DICE is located at the university and hosts all economic experiments in Düsseldorf, while the IW Köln is likely unknown to students with no economic background. This impression was confirmed by non-parametrical tests.

Figure 4-2: Average familiarity and trust in the recipient of personal information



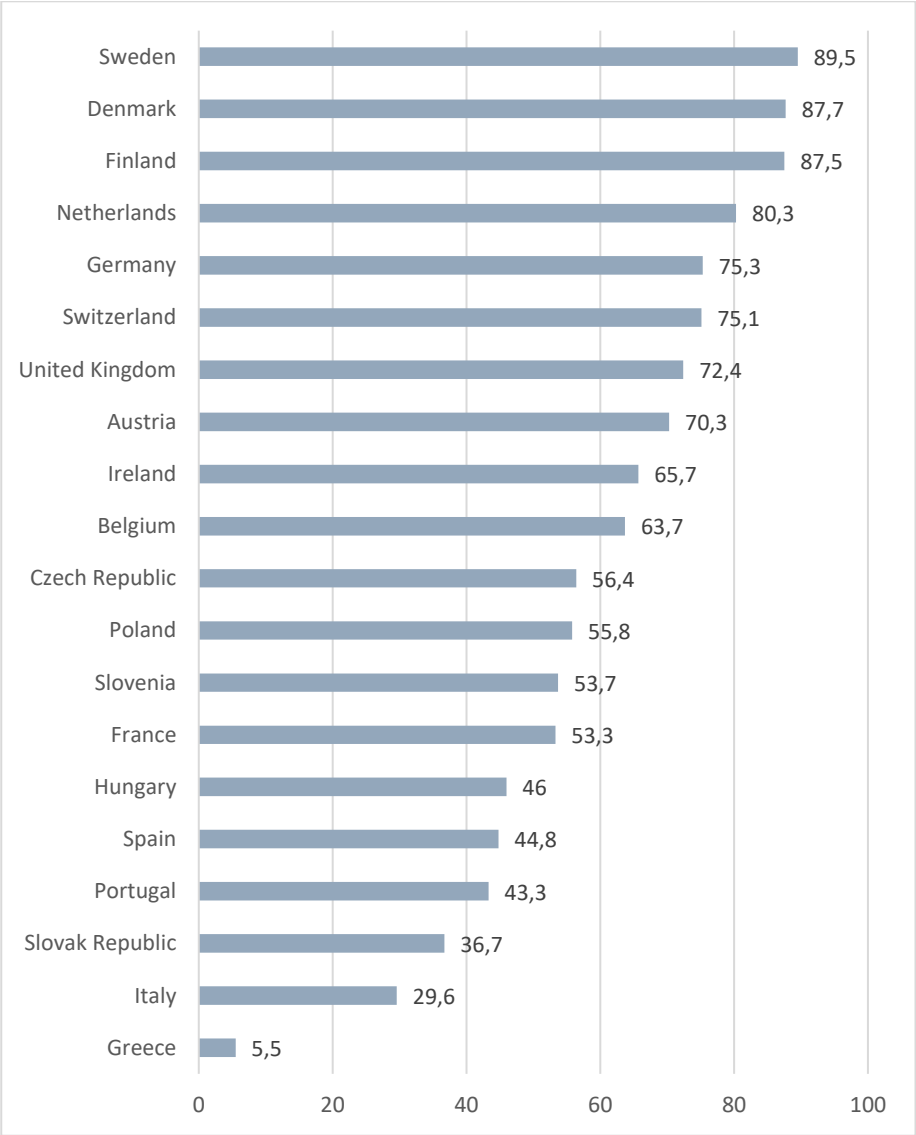
The tests also show that within the IW Köln-group, the disposition to trust significantly affects the level of trust placed in this recipient of personal information. A possible explanation has been given before: Dispositional trust is of special importance when dealing with rather unknown partners, while it loses its impact when the trustor becomes more familiar with the trustee. The participants in the IW-treatment showed significantly lower familiarity than the other group, so this argument possibly applies here.

This result was supported by a regression analysis, but there an interesting contradiction occurred: While the survey measure of dispositional trust showed to positively determine the level of trust in the recipient, which is in accordance with the literature, the experimental measure exerted a negative influence. Further investigation of the two variables indicated that they are not correlated and thus appear to measure different concepts. This adds to the ongoing debate, whether experiments and surveys capture the same facet of trust and whether they are adequate altogether. Glaeser et al. (2000) for example compared sender behavior in the trust game with the answers to the commonly used question “Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with people”. They did not find a correlation, claiming that the question does not measure trust, but rather trustworthiness. Gächter et al. (2004) support the finding by also not sustaining a significant correlation between experimental and survey behavior. On the other hand, several studies contradict these results by identifying a significant relationship between the behavior of Player A in the Trust Game and survey measures of trust, such as Fehr et al. (2003) and Bellemare and Kröger (2007). Sapienza et al. (2013) investigate the contradictory findings with an experiment as well. They argue that answers to common survey questions mainly measure the expectation of others' trustworthiness. Reviewing the definitions of trust shows that expectation of other people's trustworthiness is a central component of trust, as trust is “based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer et al., 1995, p.712). It thus appears that survey methods are indeed a good measure of trust. They do however suffer from general weaknesses, as mentioned before. The sender behavior in the Trust Game appears to capture more than trust: Sapienza and her colleagues (2013) show that it depends on the expectation of other people's trustworthiness and additionally on personal preferences, such as risk- and inequality aversion or altruism. These insights can help explain the results of the present study. The Trust Game was intended to capture the disposition to trust, but the results from the regression analyses were inconsistent with the literature. The negative relationship between the behavior in the Trust Game and trust in the recipient might stem from factors that are not controlled for, but positively influence the amount sent as Player A, while possibly reducing the trust in the recipient. Further research should aim at identifying these determinants by measuring personal preferences and traits additionally.

The analyses did not provide support for the remaining relationships presented by the literature in the previous chapter, which can be explained by the relative small sample size and flaws in the variables. Especially the measurement of self-disclosure needs revision: The majority of subjects replied to all sensitive questions, which leaves little variance and makes it hard to identify effects. One possible explanation proposed by Joinson et al. (2010) and also in related studies (Korzaan et al., 2009; Norberg et al., 2007) is that participants felt protected by the environment they were placed in: a lab in the university, where most of them had been before. This might have given them the confidence, that their personal data is safe, no matter who received it in the end and so a lot of information was given. In addition, the data was said to be used for academic research, which probably added to the positive effect. Further research should therefore aim at increasing the variance in self-disclosure, for example by changing the environment or asking even more sensitive questions.

The study still provides valuable insights on the formation of trust. If trust in another party – in this case the requester and recipient of personal information – is strongly determined by the general willingness to trust, businesses and politics should expect different levels of trust amongst different population groups. As the disposition to trust depends on relatively stable personality traits and is influenced by experiences throughout life, it partly depends on socio-demographic and cultural factors. A survey of the experimental literature on gender differences for example shows that men are generally more trusting than women, even though this result was not obtained in this study (Croson and Gneezy, 2009). The general tendency to trust also differs between education levels, as an evaluation of the data from the German-based Socioeconomic Panel (SOEP) reports. People who have an academic education trust twice as much as people without it (Michalski and Schupp, 2009). Regarding culture, Guiso et al. (2003) analyzed data from the European Values Survey and the World Values Survey and shows that religious people are 20 percent more trusting than atheists. Within Europe, general trust in others also differs, as a study by Enste and Grunewald (2017) illustrates: While Scandinavian countries enjoy high levels of general trust in the political system, the economic system and society, southern European countries such as Greece and Italy reach very low scores. Germany reaches a level amongst the top third (see figure 4-3).

Figure 4-3: IW Trust Index 2017



Source: Enste / Grunewald, 2017

These findings should not be viewed isolated, as they interact and depend on numerous other personal traits such as life experience or the Big Five and also societal influences. Additionally, there is most likely simultaneity between trust and the contributing factors (Michalski and Schupp, 2009). Knowledge of the formation of trust can however still be interesting and should not be disregarded in the design of strategies to establish trust, which is of special relevance in the anonymous, fast and ever-changing online environment. Businesses should consider differences in their customers' general trust levels in the design of their processes communication strategies. When faced with population groups that are generally less trusting, they should expect lower levels of trust in their company and might want to focus on trust enhancing signals or increasing familiarity. Most importantly though, businesses should meet their users' need for safety online and design their processes accordingly. Only if users are sure that their data is

handled confidently, they are willing to build and sustain a relationship with an online provider. This in turn is crucial for the long-term success of an online-business.

Politics also wants to create an environment, where citizens feel and are safe. People with high initial trust levels might be more likely to trust a specific vendor, even if he might exploit that trust. Insights on the formation of trust can help identifying consumer types which can in turn be addressed individually, depending on their need for protection. Not only do politicians want to protect consumers from untrustworthy offers, they also aim at a successful digital transition. In order for online services to work and develop further, people need to feel safe to use them. Users who exhibit low general trust levels and thus possibly lower levels of trust in specific internet providers might be reluctant to use online services in general. To help overcome their distrust, educational programs to increase their knowledge of these systems can be implemented. Additionally, officially certified and easily understood seals need to be provided so that consumers do not have to rely on their gut feeling when faced with an unknown service, but can quickly assess its trustworthiness. Differentiated policies that take the consumers' individual needs into account are a valuable addition to existing laws, since they decrease the vulnerability of users and increases their confidence. This can help to reduce the number of untrustworthy online-services, as they have lower opportunity to exploit users. At the same time, such policies can support serious offers which might face a higher willingness to engage with them.

5 Conclusion

Expressing themselves and sharing thoughts, tastes and other personal information is of high value for individuals, as it strengthens relationships, enhances experiences and improves well-being altogether. With the rise of the internet, the possibilities to self-disclose have multiplied, as services are accessible everywhere and anytime. While they do enjoy high popularity, they are also viewed with growing skepticism. People are more and more afraid of losing control over their data and feel at unease when sharing information online. These concerns however only marginally translate into behavior. A broad body of research has aimed at explaining this discrepancy and several personal and situational factors have been identified which moderate the relationship between skepticism and self-disclosure.

The aim of this study was to add to the existing literature by investigating one of the central factors in the decision to share personal information, namely trust. A computerized laboratory experiment was conducted to measure how trust in a recipient of personal information impacts the willingness to self-disclose and what drives the formation of that trust. Even though no significant relationship between trust and self-disclosure was sustained, the study provides valuable insights on the positive impact of dispositional trust on trust in a specific other party. This knowledge can be used by politics and businesses in the design of rules and communication strategies regarding different consumer types.

The question why people decide to share private information is highly relevant today, as the internet penetrates more and more areas of life and the value of personal data is growing. Understanding the driving forces behind self-disclosure is therefore important for the digital transition to reach its full potential. Future research should aim at identifying further factors that determine the level of trust a person places into an online-service and investigate how that trust translates into behavior.

6 References

Acquisti, Alessandro (2004), „Privacy in Electronic Commerce and the Economics of Immediate Gratification“, *Proceedings of the 5th ACM Conference on Electronic Commerce*, S. 21-29.

Acquisti, Alessandro; Brandimarte, Laura & Loewenstein, George (2015), „Privacy and Human Behavior in the Age of Information“, *Science* 347 (6221), S. 509-514.

Acquisti, Alessandro & Grossklags, Jens (2005), „Privacy and Rationality in Individual Decision Making“, *IEEE Security & Privacy* 3 (1), S. 26-33.

Altman, Irwin (1976), „Privacy- A Conceptual Analysis“, *Environment and Behavior* 8 (1), S. 7-29.

Altman, Irwin (1975), *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Publications: Monterey.

Altman, Irwin & Taylor, Dalmas (1973), *Social Penetration: The Development of Interpersonal Relationships*. Holt, Rinehart & Winston: New York.

Arrow, Kenneth (1972), „Gifts and Exchanges“, *Philosophy & Public Affairs* 1 (4), S. 343-362.

Barnes, Susan (2006), „A Privacy Paradox: Social Networking in the United States“, *First Monday* 11 (9).

Bellemare, Charles & Kröger, Sabine (2007), „On Representative Social Capital“, *European Economic Review* 51 (1), S. 183-202.

Berg, Joyce; Dickhaut, John & McCabe, Kevin (1995), „Trust, Reciprocity, and Social History“, *Games and Economic Behavior* 10 (1), S. 122-142.

Bitkom (2015), „Datenschutz in der digitalen Welt“, Berlin.

Burgoon, Judee (1982), „Privacy and Communication“, *Annals of the International Communication Association* 6 (1), S. 206-249.

Christofides, Emilily; Muise, Amy & Desmarais, Serge (2009), „Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?“, *Cyberpsychology & Behavior* 12 (3), S. 341-345.

Coleman, James (1990), *Foundations of Social Theory*. Harvard University Press: Cambridge, London.

Colquitt, Jason; Scott, Brent & LePine, Jeffery (2007), „Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships with Risk Taking and Job Performance“, *Journal of Applied Psychology* 92 (4), S. 909-927.

Croson, Rachel & Gneezy, Uri (2009), „Gender Differences in Preferences“, *Journal of Economic Literature* 47 (2), S. 448-474.

Culnan, Mary & Armstrong, Pamela (1999), „Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation“, *Organization Science* 10 (1), S. 104-115.

Datenschutz Nord (2015), „Umgang mit Verbraucherdaten durch Online-Shops“, Berlin.

DIVSI – Deutsches Institut für Vertrauen und Sicherheit im Internet (2015), „Allgemeine Geschäftsbedingungen (AGB) von Kommunikationsdienstleistern“, Hamburg.

Dutton, William & Shepherd, Adrian (2006), „Trust in the Internet as an Experience Technology“, *Information, Communication & Society* 9 (4), S. 433-451.

Enste, Dominik; Ewers, Mara; Heldman, Christina & Schneider, Regina (2016), „Verbraucherschutz und Verhaltensökonomik: Zur Psychologie von Vertrauen und Kontrolle“, *IW-Analysen* 106, Köln.

Enste, Dominik & Grunewald, Mara (2017), „IW-Vertrauensindex 2017 – Vertrauen in Wirtschaft, Politik und Gesellschaft im europäischen Vergleich“, Köln.

ESS – European Social Survey (2014), „Variable ppltrst: Most people can be trusted or you can't be too careful“, http://nesstar.ess.nsd.uib.no/webview/ [Stand: 05.10.2017].

Facebook (2018a), „ Facebook Q1 2018 Results “.

Facebook (2018b), „Erste Schritte mit Werbeanzeigen“, https://www.facebook.com/business/learn/facebook-ads-basics [Stand: 27.02.2018].

Facebook (2017a), „Facebook Q4 2017 Results”.

Fehr, Ernst; Fischbacher, Urs; von Rosenbladt, Bernhard; Schupp, Jürgen & Wagner, Gert (2003), „A Nation-Wide Laboratory: Examining Trust and Trustworthiness by Integrating Behavioral Experiments into Representative Surveys“, *IZA Discussion Papers*, No. 715, Bonn.

Fukuyama, Francis (1995), „Trust: The Social Virtues and the Creation of Prosperity“, Free Press Paperback: New York.

Gächter, Simon; Herrmann, Benedikt & Thöni, Christian (2004), „Trust, Voluntary Cooperation, and Socio-Economic Background: Survey and Experimental Evidence“, *Journal of Economic Behavior & Organization* 55 (4), S. 505-531.

Gefen, David (2000), „E-Commerce: The Role of Familiarity and Trust“, *Omega* 28 (6), S. 725-737.

Glaeser, Edward; Laibson, David; Scheinkamn, Jose & Soutter, Christine (2000), „Measuring Trust“, *The Quarterly Journal of Economics* 115 (3), S. 811-846.

Guiso, Luigi; Sapienza, Paola & Zingales, Luigi (2003), „People's Opium? Religion and Economic Attitudes“, *Journal of Monetary Economics* 50 (1), S. 255-282.

Joinson, Adam; Paine, Carina; Buchanan, Tom & Reips, Ulf-Dietrich (2008), „Measuring Self-Disclosure Online: Blurring and Non-Response to Sensitive Items in Web-Based Surveys“, *Computers in Human Behavior* 24 (5), S. 2158-2171.

Joinson, Adam; Reips, Ulf-Dietrich; Buchanan, Tom & Paine Schofield, Carina (2010), „Privacy, Trust and Self-Disclosure Online“, *Human–Computer Interaction* 25 (1), S. 1-24.

Kehr, Flavius; Kowatsch, Tobias; Wentzel, Daniel & Fleisch, Elgar (2015), „Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus“*, Information Systems Journal* 25 (6), S. 607-635.

Keith, Mark; Thompson, Samuel; Hale, Joanne & Greer, Chapman (2012), „Examining the Rationality of Information Disclosure Through Mobile Devices“, *International Conference on Information Systems* 201 (2).

Kenning, Peter (2002), *Customer Trust Management. Ein Beitrag zum Vertrauensmanagement im Lebensmittelhandel*. Dissertation Universität Münster, Deutscher Universtitäts-Verlag GmbH: Wiesbaden.

Kim, Dan; Ferrin, Donald & Rao, Raghav (2008), „A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents“, *Decision Support Systems* 44 (2), S. 544-564.

Korzaan, Melinda; Brooks, Nita & Greer, Timothy (2009), „Demystifying Personality and Privacy: An Empirical Investigation into Antecedents of Concerns for Information Privacy“, *Journal of Behavioral Studies in Business* 1, S. 1-17.

Kosinski, Michal; Stillwell, David & Graepel, Thore (2013), „Private Traits and Attributes Are Predictable from Digital Records of Human Behavior”, *Proceedings of the National Academy of Sciences* 110 (15), S. 5802-5805.

Lee, Chung Hun & Cranage, David (2011), „Personalisation– Privacy Paradox: The Effects of Personalisation and Privacy Assurance on Customer Responses to Travel Web Sites“, *Tourism Management* 32 (5), S. 987-994.

Lee, Eunsun; Ahn, Jungsun & Kim, Yeo Jung (2014), „Personality Taits and Self-Presentation at Facebook“, *Personality and Individual Differences* 69, S. 162-167.

Leino-Kilpi, Helena; Välimäki; Maritta; Dassen, Theo; Gasull, Maria; Lemonidou, Chryssoula; Scott, Allison & Arndt, Marianne (2001), „Privacy: A Review of the Literature“, *International Journal of Nursing Studies* 38 (6), S. 663-671.

Li, Han; Sarathy, Rathindra & Xu, Heng (2011), „The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors“, *Decision Support Systems* 51 (3), S. 434-445.

Liao, Chechen; Liu, Chuang-Chun & Chen, Kuanchin (2011), „Examining the Impact of Privacy, Trust and Risk Perceptions beyond Monetary Transactions: An Integrated Model“, *Electronic Commerce Research and Applications* 10 (6), S. 702-715.

Mayer, Roger; Davis, James & Schoorman, David (1995), „An Integrative Model of Organizational Trust“, *The Academy of Management Review* 20 (3), S. 709-734.

Mayer-Schönberger, Viktor & Cukier, Kenneth (2013), *Big Data. Die Revolution, die unser Leben verändern wird*. 2. Auflage, Redline Verlag: München.

McKnight, Harrison & Chervany, Norman (2001), „What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology“, *International Journal of Electronic Commerce* 6 (2), S. 35-59.

McKnight, Harrison; Chodhury, Vivek & Kacmar, Charles (2002), „Developing and Validating Trust Measures for E-Commerce: An Integrative Typology“, *Information Systems Research* 13 (3), S. 332-359.

McKnight, Harrison; Cummings, Larry & Chervany, Norman (1998), „Initial Trust Formation in New Organizational Relationships“, *The Academy of Management Review* 23 (3), S. 473-490.

Metzger, Miriam (2004), „Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce“, *Journal of Computer-Mediated Communication* 9 (4).

Mesch, Gustavo (2012), „Is Online Trust and Trust in Social Institutions Associated with Online Disclosure of Identifiable Information Online?“, *Computers in Human Behavior* 28 (4), S. 1471-1477.

Michalski, Niels & Schupp, Jürgen (2009), „Sozialer Rohstoff: Den meisten Menschen kann man vertrauen“, *DIW Wochenbericht* 34/2009, Berlin.

Norberg, Patricia; Horne, Daniel & Horne, David (2007), „The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors“, *Journal of Consumer Affairs* 41 (1), S. 100-126.

Reuters (2018), „Who trusts Facebook?”, http://ngfx.thomsonreuters.com/gfx/rngs/USAFACEBOOK-POLL/0100619Q2Q6/index.html [Stand: 2018-04-13].

Ripperger, Tanja (2003), *Ökonomik des Vertrauens: Analyse eines Organisationsprinzips*. 2. Auflage, Mohr Siebeck: Tübingen.

Rotter, Julian (1971), „Generalized Expectancies for Interpersonal Trust“, *American Psychologist* 26 (5), S. 443-452.

Rousseau, Denise; Sitkin, Sim; Burt, Ronald & Camerer, Colin (1998), „Not so Different after All: A Cross-Discipline View of Trust“, *The Academy of Management Review* 23 (3), S. 393-404.

Rusk, John (2014), „The Privacy Paradox: Trust and Distrust as Separate Variables“, *Proceedings of the Southern Association for Information Systems Conference (SAIS),* Macon.

Sapienza, Paola; Toldra-Simats, Anna & Zingales, Luigi (2013), „Understanding Trust“, *The Economic Journal* 123 (573), S. 1313-1332.

Schoenbachler, Denise & Gordon, Geoffrey (2002), „Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing“, *Journal of Interactive Marketing* 16 (3), S. 2-16.

Simon, Herbert (1959), „Theories of Decision-Making in Economics and Behavioral Science“, *The American Economic Review* 49 (3), S. 253-283.

Spiekermann, Sarah; Grossklags, Jens & Berendt, Bettina (2001), „E-Privacy in 2nd Generation E-commerce: Privacy Preferences versus Actual Behavior“, *Proceedings of the 3rd ACM Conference on Electronic Commerce*.

Statista (2017). Digital Market Outlook.

Taddicken, Monika (2014), „The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure“, *Journal of Computer-Mediated Communication* 19 (2), S. 248-273.

Tamir, Diana & Mitchell, Jason (2012), „Disclosing Information about the Self is Intrinsically Rewarding“, *Proceedings of the National Academy of Sciences* 109 (21), S. 8038-8043.

TechCrunch (2017), „Instagram now has 800 million monthly and 500 million daily active users”, https://techcrunch.com/2017/09/25/instagram-now-has-800-million-monthly-and-500-million-daily-active-users/ [Stand: 02.05.2018]

TNS Emnid (2015), „Datenschutz. Die Sicht der Verbraucherinnen und Verbraucher in Deutschland“, Studie im Auftrag des Verbraucherzentrale Bundesverbands, Bielefeld.

Van Slyke, Craig; Shim, J.T.; Johnson, Richard & Jiang, James (2006), „Concern for Information Privacy and Online Consumer Purchasing“, *Journal of the Association for Information Systems* 7 (6), S. 415-444.

Vodafone Institute for Society and Communications (2016), „Big Data. A European Survey on the Opportunities and Risks of Data Analytics“, Berlin.

vzbv – Verbraucherzentrale Bundesverband (2015), „Big Data: Verbraucher befürchten Nachteile durch Profilbildung“, http://www.vzbv.de/pressemitteilung/big-data-verbrau-cher-befuerchten-nachteile-durch-profilbildung [Stand: 05.03.2018].

Warren, Samuel & Brandeis, Louis (1890), „The Right to Privacy“, *Harvard Law Review* 4 (5), S. 193-220.

Wilson, David & Valacich, Joseph (2012), „Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus“, *Proceedings of the Thirty Third International Conference on Information Systems (ICIS 2012)*, S. 1-11.

Worldbank (2018), „Individuals Using the Internet (% of Population) “, https://data.worldbank.org/indicator/IT.NET.USER.ZS [01.03.2018].

Wu, Jingwei & Lu, Heng (2013), „Cultural and Gender Differences in Self-Disclosure on Social Networking Sites“, in: Petley, Julian (Hrsg.), *Media and Public Shaming*. London, New York: I.B. Tauris, S. 97-115.

WVS – World Values Survey (2017), „World Values Survey Wave 6: 2010-2014: V24.- Most People Can be Trusted“, http://www.worldvaluessurvey.org/WVSOnline.jsp [Stand: 05.10.2017].

Youn, Seounmi & Hall, Kimberly (2008), „Gender and Online Privacy among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors“, *Cyberpsychology & Behavior* 11 (6), S. 763-765.

Xu, Heng; Dinev, Tamara; Smith, Jeff & Hart, Paul (2008), „Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View“, *International Conference on Information Systems (ICIS) 2008 Proceedings*, S. 1-16.

Table of Figures