

**Understanding Consumers' Digital Data  
Disclosure Decision-Making:**  
A Focus on Data Sharing Cooperations, Perceived  
Risks and Low-Cognitive-Effort Processing

Dissertation Submitted to Attain the Degree of  
*Doctor rerum politicarum (Dr. rer. pol.)*  
at the School of Business, Economics and Information Systems  
of the University of Passau

Submitted by: Tobias Marcel Steudner, M.Sc.  
First Reviewer: Prof. Dr. Thomas Widjaja  
Second Reviewer: Prof. Dr. Franz Lehner

August 2021



**Accepted as Dissertation**

at the School of Business, Economics and Information Systems of the University of Passau

**Date of the Disputation:** March 14, 2022

**Chair of the Examining Committee:** Prof. Dr. Alena Otto

**First Reviewer:** Prof. Dr. Thomas Widjaja

**Second Reviewer:** Prof. Dr. Franz Lehner

## **Abstract**

Due to the advances of digitalization, firms are able to collect more and more personal consumer data and strive to do so. Moreover, many firms nowadays have a data sharing cooperation with other firms, so consumer data is shared with third parties. Accordingly, consumers are confronted regularly with the decision whether to disclose personal data to such a data sharing cooperation (DSC). Despite privacy research has become highly important, peculiarities of such disclosure settings with a DSC between firms have been neglected until now. To address this gap is the first research objective in this thesis. Another underexplored aspect in privacy research is the impact of low-cognitive-effort decision-making. This is because the privacy calculus, the most dominant theory in privacy research, assumes for consumers a purely cognitive effortful and deliberative disclosure decision-making process. Therefore, to expand this perspective and examine the impact of low-cognitive-effort decision-making is the second research objective in this thesis. Additionally, with the third research objective, this thesis strives to unify and increase the understanding of perceived privacy risks and privacy concerns which are the two major antecedents that reduce consumers' disclosure willingness.

To this end, five studies are conducted: i) essay 1 examines and compares consumers' privacy risk perception in a DSC disclosure setting with disclosure settings that include no DSC, ii) essay 2 examines whether in a DSC disclosure setting consumers rely more strongly on low-cognitive-effort processing for their disclosure decision, iii) essay 3 explores different consumer groups that vary in their perception of how a DSC affects their privacy risks, iv) essay 4 refines the understanding of privacy concerns and privacy risks and examines via meta-analysis the varying effect sizes of privacy concerns and privacy risks on privacy behavior depending on the applied measurement approach, v) essay 5 examines via autobiographical recall the effects of consumers' feelings and arousal on disclosure willingness.

Overall, this thesis shines light on consumers' personal data disclosure decision-making: essay 1 shows that the perceived risk associated with a disclosure in a DSC setting is not necessarily higher than to an identical firm without DSC. Also, essay 3 indicates that only for the smallest share of consumers a DSC has a negative impact on their disclosure willingness and that one third of consumers do not intensively think about consequences for their privacy risks arising through a DSC. Additionally, essay 2 shows that a stronger reliance on low-cognitive-effort processing is prevalent in DSC disclosure settings. Moreover, essay 5 displays that even unrelated feelings of consumers can impact their disclosure willingness, but the effect direction also depends on consumers' arousal level.

This thesis contributes in three ways to theory: i) it shines light on peculiarities of DSC disclosure settings, ii) it suggests mechanisms and results of low-effort processing, and iii) it enhances the understanding of perceived privacy risks and privacy concerns as well as their resulting effect sizes.

Besides theoretical contributions, this thesis offers practical implications as well: it allows firms to adjust the disclosure setting and the communication with their consumers in a way that makes them more successful in data collection. It also shows that firms do not need to be too anxious about a reduced disclosure willingness due to being part of a DSC. However, it also helps consumers themselves by showing in which circumstances they are most vulnerable to disclose personal data. That consumers become conscious of situations in which they are especially vulnerable to disclose data could serve as a countermeasure: this could prevent that consumers disclose too much data and regret it afterwards. Similarly, this thesis serves as a thought-provoking input for regulators as

it emphasizes the importance of low-cognitive-effort processing for consumers' decision-making, thus regulators may be able to consider this in the future.

In sum, this thesis expands knowledge on how consumers decide whether to disclose personal data, especially in DSC settings and regarding low-cognitive-effort processing. It offers a more unified understanding for antecedents of disclosure willingness as well as for consumers' disclosure decision-making processes. This thesis opens up new research avenues and serves as groundwork, in particular for more research on data disclosures in DSC settings.

## Acknowledgements

First of all, I would like to thank Prof. Dr. Thomas Widjaja for giving me the opportunity to do my PhD in Business Informatics and for allowing me to learn something new every day during this time. Furthermore, I would like to thank him for his excellent supervision, valuable advice and the freedom he gave me. I particularly appreciated the supportive work environment, which was challenging but also consistently constructive and a lot of fun. Moreover, I would like to express my sincere thanks to Prof. Dr. Franz Lehner for taking over the second review and for the consistently interesting discussions during my doctorate. I would also like to thank Prof. Dr. Alena Otto for chairing my examination committee with so much enthusiasm.

My special thanks go to all the colleagues and friends who made my time in Passau so exciting and enjoyable. In particular, I would like to thank Andrea, Uschi, Victoria, Basti, Philipp, Muqet, Tobias, and Torben for making me smile so often, for always having an open ear for me, and for providing valuable insights and help. Especially I want to thank Muqet for the fun leisure activities and the consistently good time. I would also like to thank Jan and Daniel and their teams for the great time and their open doors.

Finally, I would like to thank from the bottom of my heart two very special people, who supported me always with unconditional love, patience, and advice:

My father, who sacrificed endless hours to give me a lighthearted childhood and an excellent education. I am fortunate to be your son. I appreciate all you have done for me, thank you Paps.

My partner Anna, who is just always there for me and loves and supports me unconditionally. With you I have already experienced so much, everyday life as well as adventures, and there is nothing more wonderful than being able to share all the moments together with you. Thank you for always making me smile.

Words cannot express my infinite gratitude to you.

In order to also express my great pleasure in the works of Sir Terry Pratchett, which have accompanied me all my life, I would like to reflect on my time during the PhD in his honor with the following statement:

“So much universe, and so little time.” *Terry Pratchett*

# Contents

<b>Introduction.....</b>	<b>1</b>
Motivation and Research Objectives.....	1
Main Concepts .....	5
Privacy Calculus.....	5
Privacy Risk .....	5
Privacy Concerns.....	6
Types of Processing .....	7
Affect as an Umbrella Term .....	8
Emotions and Feelings .....	8
Affect According to the Affect Heuristic .....	9
Data Sharing Cooperation .....	9
Research Methods .....	11
Groundwork .....	11
Samples .....	11
Statistical Analysis .....	12
Summary of the Five Essays and How They are Related .....	13
Essay 1 .....	14
Essay 2 .....	15
Essay 3 .....	16
Essay 4 .....	18
Essay 5 .....	20
Overall Discussion .....	23
Contributions.....	23
Limitations and Avenues for Further Research.....	24
Conclusion.....	25
References .....	26
<b>An Exploratory Study of Risk Perception for Data Disclosure to a Network of Firms .....</b>	<b>34</b>
Introduction .....	35
Theoretical Background on Risks .....	36
Exploratory Survey .....	36
Results, Discussion, and Outlook.....	37
References .....	38

---

<b>The Effect of Data Sharing Between Firms on Low-Cognitive-Effort Processing – An Integrative Approach.....</b>	<b>41</b>
Introduction.....	42
Theoretical Background and Hypotheses Development .....	44
Privacy Calculus and the Base Model.....	44
Low and High Cognitive Effort Processing .....	45
Affective Reaction.....	45
Privacy Calculus from a Reinforcement Learning Perspective.....	46
Sample and Setup.....	50
Results .....	51
Measurement Model Assessment.....	51
Structural Model Assessment.....	51
Group Comparison .....	52
Discussion, Implications and Limitations .....	55
Discussion .....	55
Implications.....	56
Limitations and Future Research.....	56
Appendix.....	58
References .....	63
<b>Consumer Groups and Their Risk Perception in a Data Sharing Cooperation Between Two Firms .....</b>	<b>69</b>
Introduction.....	71
Theoretical Background .....	72
Privacy Concerns.....	72
Privacy Calculus and Perceived Privacy Risks .....	72
Hypotheses Development.....	73
Sample and Setup.....	75
Method and Results.....	76
Discussion .....	79
Implications.....	79
Limitations .....	80
Appendix .....	81
References .....	82

---

<b>The Impact of Abstraction Levels on the Effect Sizes of Privacy Concerns and Privacy Risks – A Quantitative Meta-Analysis .....</b>	<b>87</b>
Introduction .....	89
Theoretical Background and Hypotheses Development .....	90
Abstraction Levels applied in Privacy Studies .....	90
Privacy Concerns.....	90
Privacy Calculus.....	93
Privacy Risks.....	93
Comparison of Privacy Concerns and Privacy Risks on a Situational Abstraction Level .....	94
Method .....	95
Results .....	96
Discussion, Implications and Limitations .....	98
Discussion and Implications.....	98
Limitations .....	100
Appendix .....	102
References .....	113
<b>The Effects of Positive Feelings and Arousal on Privacy Decision-Making.....</b>	<b>117</b>
Introduction .....	119
Theoretical Background and Hypotheses Development .....	120
Privacy Calculus and Privacy Concerns.....	120
Low-Cognitive-Effort Processing .....	121
Sample and Setup.....	124
Results .....	125
Measurement Model Assessment.....	125
Structural Model Assessment.....	126
Discussion .....	128
Limitations .....	130
Implications and Future Research .....	130
Appendix .....	132
References .....	137
<b>Appendix .....</b>	<b>141</b>



## Introduction

### Motivation and Research Objectives

*“I believe people are smart. And some people want to share more data than other people do. Ask them.”* (Jobs, 2010). But what if consumers do not always make smart, meaning thoughtful, decisions regarding personal data disclosure but rather intuitive or affective decisions as indicated by several studies (Wang et al., 2011; Wakefield, 2013; Dinev, McConnell and Smith, 2015). Such emotionally charged situations are situations in which consumers can be especially vulnerable to be willing to disclose personal data (Wang et al., 2011; Wakefield, 2013; Kehr, Kowatsch, Wentzel and Fleisch, 2015). This is particularly problematic since more and more individuals have access to the Internet at almost any time and therefore are able to disclose personal data in any situation (The Sunday Times, 2018), even in emotionally charged situations (cf. Wang et al., 2011). A prediction that an average person in 2025 will produce 4900 data interactions per day (Samad, 2019) emphasizes the importance to understand consumers’ personal data disclosure decision-making in detail (cf. Dinev et al., 2015).

This understanding is highly important for firms, as personal data is necessary to personalize products and services or to be able to target appropriate consumer groups (Rust and Huang, 2014; Gartner, 2019; Österreichische Marketing Gesellschaft and Marketagent, 2019; Hanafizadeh and Harati Nik, 2020). Thus, an increasing number of firms strive to collect more detailed personal data from their consumers (Internet World Business, 2018; Samad, 2019; Brandt, 2020; Hanafizadeh and Harati Nik, 2020). To be successful in data collection it is necessary for firms to understand how their consumers make their disclosure decisions. The increasing importance for firms to understand their consumers’ disclosure decision-making is also reflected in the growing value of the global data market, which is based on the collection and sale of consumer data. In 2016 the global data market was already large with \$18.9 bn, it grew to \$34.6 bn in 2019 and will rise even more with an expected value of \$52.3 bn in 2021 (OnAudience, 2020).

Due to the ever-growing amount of data collection online, consumers nowadays are confronted regularly with the decision whether to disclose personal data (Rust and Huang, 2014; The Sunday Times, 2018; Brandt, 2020; Ovide, 2020). Disclosing personal data can be a requirement for consumers to be able to use certain services at all, to use them more conveniently through personalization, or in order to obtain other benefits by disclosing their personal data (Chellappa and Sin, 2005; Smith, Dinev and Xu, 2011; Schumann, von Wangenheim and Groene, 2014). However, collecting personal data does not only bring benefits for consumers and firms, as personal data collection could deter privacy concerned consumers (Smith et al., 2011; Xu, Luo, Carroll and Rosson, 2011). Indeed, many consumers are highly concerned about their privacy due to the mass amount of personal data collected in the digital environment, as data disclosures entail risks to ones’ privacy, e.g., misuse of personal data (Smith et al., 2011; European Commission, 2016; Pew Research Center, 2019; Bandara, Fernando and Akter, 2020). It is important for consumers themselves as well as legislators to know under which circumstances consumers are most vulnerable to disclose their personal data online. An increased understanding of the disclosure decision-making process could help to protect consumers from disclosing too much personal data, so that consumers will not experience any severe privacy intrusions and regret their disclosure decisions (cf. Wang et al., 2011; Xie and Kang, 2015; Vaidhyanathan, 2018).

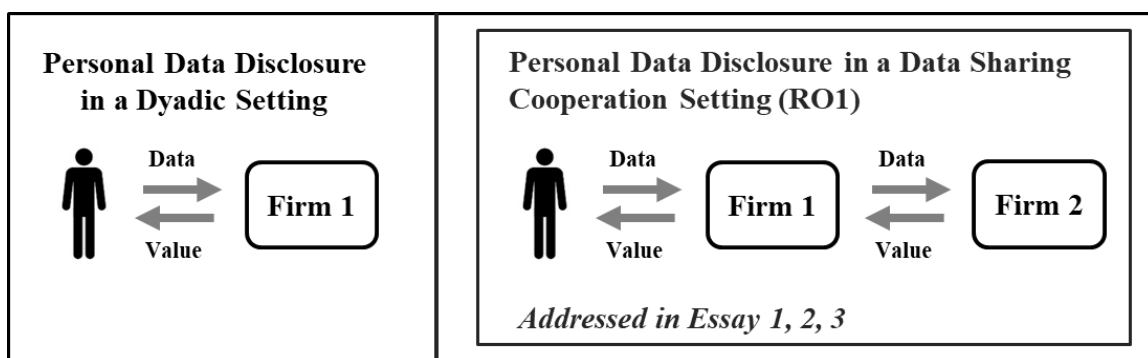
An attempt to protect consumers’ digital privacy was made in the European Union with the General Data Protection Regulation (GDPR) enacted in May 2018 (European Union, 2016). One aspect of

the new regulation, which should help consumers to make better data disclosure decisions, is the increased transparency requirement for data handling procedures of firms and institutions.

With this new regulation, firms are forced to clearly inform their consumers about which data types (e.g., income data, geographical data, etc.) are collected, and with which third-parties this personal data is shared. Nowadays most firms, and even some public institutions, share their consumer data with additional parties (Gesamtverband der Deutschen Versicherungswirtschaft e.V., 2019; LiveRamp, 2021) to create value by selling consumer data or by enabling and improving offered services (Smith et al., 2011; Wharton School, 2019). An example, that shows how prevalent it is nowadays for firms to share consumer data can be found in Apples' iOS app store: most of the available apps share consumer data with third-parties (Dimitrov, 2021). Similarly, Paypal is one of many successful firms that share consumer data with further parties (Paypal, 2018; Wharton School, 2019).

However, the existing privacy literature has not yet examined the effects on consumers' willingness to disclose personal data arising through a data sharing cooperation (DSC) between firms. Previous literature has primarily examined dyadic data disclosures (cf. Figure 1, left) in which consumers disclose their data solely to one firm (e.g., Bansal, Zahedi and Gefen, 2010; H. Li, Sarathy and Xu, 2011). Even when a data sharing cooperation setting was examined, the peculiarities and resulting effects that could occur when firms share personal consumer data to third-parties were mostly ignored (e.g., Angst and Agarwal, 2009). However, this aspect seems to be particularly important with a higher data policy transparency as required by the GDPR, because consumers can exactly see which parties obtain their data. As a first step, this thesis strives to extend knowledge by examining peculiarities of a simple DSC between two firms (cf. Figure 1, right), which is often done in practice (e.g., Beach Majors GmbH, 2019)<sup>1</sup>. Thus, the first research objective (RO1) of this thesis is the following:

*Understanding consumers' data disclosure decision-making in a data disclosure setting in which a data sharing cooperation between two firms exists.*



**Figure 1.** Illustration of the two data disclosure settings. Left side: personal data disclosure in a dyadic setting (without any data sharing between firms). Right side: personal data disclosure in a data sharing cooperation (between two firms) setting. The right side is the focus of research objective 1, which is addressed in essay 1, 2, and 3.

<sup>1</sup> To watch streams of the beach volleyball world championship in 2019 for free, it was necessary to register at the Beachstream.de website, i.e., provide data to the Beach Major GmbH, and allow them to share your personal data with Comdirect (Augsburger Allgemeine, 2019; Beach Majors GmbH, 2019).

Another aspect that is not fully understood regarding consumers' disclosure decision-making is reflected in a so called privacy paradox: even though many individuals state to have high concerns about their privacy in the digital context, they oftentimes willingly disclose their personal data (Pavlou, 2011; Taddicken, 2014; Gerber, Gerber and Volkamer, 2018). One explanation for this surprising observation could lie in the research gap identified by Dinev, McConnell, and Smith (2015): the *privacy calculus* is widely used to explain individuals' disclosure behavior and assumes that individuals base their decision-making solely on thoughtful consideration, i.e., on high-cognitive-effort processing. However, most studies on data disclosures neglect low-cognitive-effort decision-making. Thus, Dinev et al. (2015) call for more research on decision-making based on low-cognitive-effort processing as they expect this processing type to be important. To additionally consider low-cognitive-effort heuristics, such as affective reactions or feelings, could help to understand consumers decision-making in more detail (Dinev et al., 2015; Gerber et al., 2018). In line, qualitative interviews with consumers show that personal data disclosures that lead to unfavorable outcomes are oftentimes associated with decision-making based on low-cognitive-effort processing, e.g., based on feelings or affect (Wang et al., 2011).

So far, only few quantitative studies consider disclosure decision-making based on low-cognitive-effort processing. These studies confirm an indirect or direct effect on disclosure willingness (H. Li et al., 2011; Wakefield, 2013; Kehr et al., 2015; H. Li, Luo, Zhang and Xu, 2017; Aivazpour and Rao, 2020). Despite these studies consider low-cognitive-effort processing, there is still a need for more research to enhance the understanding of consumers' disclosure decision-making process as well as the role of low-cognitive-effort processing in it (Gerber et al., 2018). For example, these studies do not examine direct effects of low-cognitive-effort factors, such as feelings, on disclosure willingness while also considering the privacy calculus including benefits and privacy risks associated with the disclosure. Also, these studies only examine dyadic disclosure settings and therefore, do not consider how a data sharing cooperation between firms affects low-cognitive effort processing. Thus, it motivates to address the research call by Dinev et al. (2015) in this thesis with the following research objective *RO2*:

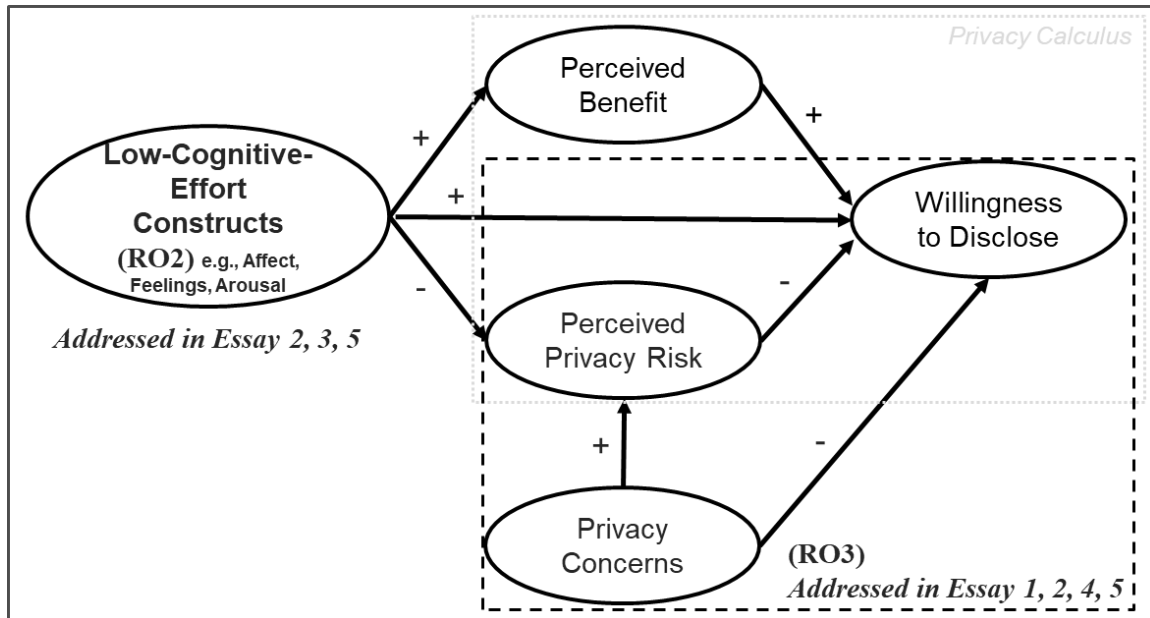
*Understanding the impact of low-cognitive-effort processing, such as affective reactions or feelings, on consumers' data disclosure decision-making.*

A second explanation why consumers generally state high privacy concerns and yet are mostly willing to provide personal data can be found in an ambiguous understanding of commonly used constructs to explain consumers' disclosure decision-making in privacy research (Davazdahemami, Hammer, Luse and Kalgotra, 2018; Gerber et al., 2018). This seems especially problematic for the "cost" side of data disclosures as there are distinct understandings and conceptualizations of privacy concerns (Hong and Thong, 2013; Davazdahemami et al., 2018; Gerber et al., 2018). Additionally, the distinction between privacy concerns and privacy risks remains sometimes blurred (cf. Y. Li, 2012; Hong and Thong, 2013; Davazdahemami et al., 2018). Thus, the last research objective (*RO3*) in this thesis is as follows:

*Understanding privacy risks, privacy concerns, and their effects on consumers' disclosure willingness.*

To address these research objectives and to understand consumers' data disclosure in more detail, this thesis builds on five essays which examine different antecedents. An illustration of the three research objectives in this thesis are provided in Figure 1 and Figure 2. In Figure 1, two distinct personal data disclosure settings are displayed, whereby *RO1* focuses on understanding consumers'

decision-making in the DSC setting (Figure 1, right). Figure 2 provides an overview of RO2 and RO3 in form of a simplified research model. Both figures additionally display which of the five essays contribute to which of the three research objectives. A more detailed overview of the content is provided in the section “summary of the five essays and how they are related”.



**Figure 2.** Illustration of the research objectives RO2 and RO3 in form of a simplified research model based on the studies in this thesis displaying constructs and effects of primary interest. RO2 is addressed in essay 2, 3, and 5. RO3 is addressed in essay 1, 2, 4, and 5.

## Main Concepts

**Privacy Calculus.** The privacy calculus is one of the most dominant theories to understand and predict consumers' personal data disclosure behavior (Smith et al., 2011; Dinev et al., 2015; Gerber et al., 2018). Therefore, the privacy calculus is used as a foundation to extend knowledge in all essays in this thesis.

The privacy calculus is based on the theory of reasoned action (Y. Li, 2012). Thus, one assumption of the privacy calculus is that consumers' disclosure intention does predict their actual disclosure behavior. However, oftentimes there is criticism that this is a weakness of the privacy calculus because intentions do not always predict actual disclosure behavior correctly (Norberg, Horne and Horne, 2007; Pavlou, 2011). Nevertheless, drawing on the privacy calculus and measuring consumers' disclosure intention or willingness is a common research approach (e.g., Al-Natour, Cavusoglu, Benbasat and Aleem, 2020) as these constructs are among the best predictors for actual disclosure behavior (Gerber et al., 2018).

Furthermore, the privacy calculus draws on the utility maximization theory (Awad and Krishnan, 2006; Y. Li, 2012). The privacy calculus assumes that consumers behave like a homo economicus and always choose the option, i.e., to disclose or not to disclose their personal data, that offers the highest utility (Smith et al., 2011; Y. Li, 2012; Gerber et al., 2018). Therefore, the privacy calculus assumes that decision-making is solely built on deliberative and logical thinking. However, this assumption is criticized as the influence of simpler processing heuristics, which require less cognitive effort, is neglected (Dinev et al., 2015). The privacy calculus explains consumers' decision-making with a weighing process where consumers calculate their utility of data disclosure by subtracting the perceived privacy risk from the perceived benefit associated with the respective data disclosure (Awad and Krishnan, 2006; Smith et al., 2011).<sup>2</sup>

Perceived benefits associated with a personal data disclosure can exist in several forms: for example, the possibility for consumers to use a service at all, to get more personalized results respectively to use the service easier or more efficiently, to obtain monetary or social benefits (Chellappa and Sin, 2005; Smith et al., 2011; H. Li, Gupta, Zhang and Sarathy, 2014). The higher consumers' perceived benefits, the more consumers are willing to disclose their personal data (Smith et al., 2011; H. Li et al., 2014).

**Privacy Risk.** In this work, the primary focus is on the privacy risk consumers associate with a personal data disclosure. This focus is chosen as privacy risk is one of the major antecedents that reduce consumers' disclosure willingness (Smith et al., 2011; Y. Li, 2012). It is highly important to understand how consumers assess privacy risks. For instance, in order to adapt the design of firm networks that share consumers' personal data, to adapt the technical data processing procedures, or to adapt privacy policies as well as the communication strategy with consumers (cf. Tsai, Egelman, Cranor and Acquisti, 2011; Bornschein, Schmidt and Maier, 2020). Consumers can become victims of different privacy threats, for example, their personal data can be misused in form of unauthorized data sharing to third parties, unwanted marketing e-mails, blackmailing, or even identity theft (Milne, Pettinico, Hajjat and Markos, 2017; gfs-zürich, 2019).

---

<sup>2</sup> However, to apply the privacy calculus it is necessary that consumers are aware that they are confronted with a data disclosure. The GDPR should help to increase consumers awareness in such disclosure settings due to the higher transparency requirements regarding firms' data handling procedures. Thus, in this thesis the research focus is on data disclosure settings where consumers are aware that they disclose data and whether this data is shared in a DSC.

Based on the privacy calculus and the assumed cognitive effortful evaluation of risks, consumers consider and assess all possible threats they perceive, to make their disclosure decision (Smith et al., 2011; Y. Li, 2012). Thus, these different threats make up the total privacy risk. Based on a “rational” or a high-cognitive-effort perspective, consumers’ total perceived privacy risk is calculated by multiplying the probability of a specific threat with its severity (i.e., the damage caused by the respective threat) and summing up these values over all threats (Peter and Tarpey, 1975).<sup>3</sup> This procedure applies equally to the perceived benefits.

However, additivity of risks respectively benefits as well as the rationality in assessments is challenged, for example, by the *prospect theory* (Kahneman and Tversky, 1979; Tversky and Kahneman, 1992; Mothersbaugh, Foxx, Beatty and Wang, 2012). Therefore, it is interesting to verify whether additivity holds when the privacy risk is stemming from two distinct firms in a data sharing cooperation disclosure setting (cf. essay 1). Privacy risk perception is strongly situation dependent (cf. Dinev, Xu, Smith and Hart, 2013; Kehr et al., 2015; Brakemeier, Wagner and Buxmann, 2017), i.e., situational factors like the firm<sup>4</sup> that collects the data (Pavlou and Gefen, 2004; D. J. Kim, Ferrin and Rao, 2008; H. Li et al., 2014) or the sensitivity of the required personal data, are highly important for consumers’ risk assessment (Dinev et al., 2013; Kehr et al., 2015). Accordingly, in the studies of this thesis, consumers’ perceived privacy risk is conceptualized on a situational level as an antecedent of consumers’ disclosure willingness. Privacy risk is examined in all essays in this thesis, with a focus on it in essay 1, 3, and 4.

**Privacy Concerns.** Besides privacy risk, another important antecedent that decreases consumers’ disclosure willingness is consumers’ privacy concerns. There are several acknowledged measurement instruments for consumers’ online privacy concerns, e.g., the “concerns for information privacy” (CFIP) from Smith, Milberg and Burke (1996), “internet users’ information privacy concerns” (IUIPC) from Malhotra, Kim and Agarwal (2004), “privacy concerns” from Buchanan, Paine, Joinson and Reips (2007), or the privacy concerns measurement instrument from Hong and Thong (2013). These partially different conceptualizations of privacy concerns range from first-order to third-order constructs (Hong and Thong, 2013). Nevertheless, almost all these different privacy concern measurement instruments consider equal aspects that shape consumers’ privacy concerns. These aspects comprise i) the amount of personal data collected, ii) unauthorized data access, iii) use of data for unauthorized purposes, iv) correctness and accuracy of user data, v) missing control over data, and vi) missing transparency (cf. Smith, Milberg and Burke, 1996; Dinev and Hart, 2004; Malhotra, Kim and Agarwal, 2004; Buchanan, Paine, Joinson and Reips, 2007; Hong and Thong, 2013).

Despite these similarities of the measurement instruments and although most of them clearly describe these privacy concerns as a general construct that is an antecedent of privacy risk (cf. Smith et al., 1996; Malhotra et al., 2004; Hong and Thong, 2013; Kehr et al., 2015), there is a certain ambiguity in the understanding of privacy concerns. Some other researchers understand them as the privacy costs of a specific personal data disclosure (cf. Mothersbaugh et al., 2012;

<sup>3</sup> Commonly, the consumers can neither identify all possible threats, nor the objective severity and probability of the threats due to, e.g., incomplete information or bounded rationality (Acquisti and Grossklags, 2005). Thus, in this thesis the focus does not lie on objective privacy risks, probabilities, severities, or benefits but on consumers perception of these constructs as this is what consumers use in their decision-making (cf. Acquisti and Grossklags, 2005; Brakemeier et al., 2017).

<sup>4</sup> In this regard, consumers’ trust in the firms can be important for the privacy risk assessment in disclosure settings when consumers had experience or are familiar with the firm they disclose to (Gefen, Karahanna and Straub, 2003; M.-S. Kim and Ahn, 2007; Ozturk, Nusair, Okumus and Singh, 2017). It must be noted that all essays in this thesis draw on hypothetical, unknown firms making effects of trust in these studies less important (cf. Gefen et al., 2003; M.-S. Kim and Ahn, 2007). However, trust is considered for control purposes in essay 2.

Y. Li, 2012; Davazdahemami et al., 2018) similar to the interpretation of privacy risks in this thesis. Another ambiguity is about the wording of the measurement items, e.g., several instruments include some items that measure consumers' expectation of firms' data processing behavior and some items that measure their own tendency to be concerned regarding firms' handling of their data (cf. Hong and Thong, 2013). This could lead to problems when measuring privacy concerns, as these distinct wording types do not reflect the same construct (Hong and Thong, 2013). To reduce such problems, the conceptualization of privacy concerns in this work is based mainly on the conceptualization perspective of Hong and Thong (2013): privacy concerns reflect consumers' self-assessment of one's general tendency to develop concerns regarding one's privacy (cf. Malhotra, Kim and Agarwal, 2004; Hong and Thong, 2013). Followingly, in this work privacy concerns are conceptualized on a general instead of a situational level and are interpreted as a general antecedent of consumers' perceived privacy risk (cf. Malhotra et al., 2004; Hong and Thong, 2013; Kehr et al., 2015). The impact of the applied abstraction levels for privacy concerns as well as privacy risks on the resulting effect sizes are examined in more detail in essay 4. For the empirical studies in essay 2 and 3, rather short measurement instruments in form of the CFIP (Smith et al., 1996) and the privacy concerns measurement instrument from Dinev et al. (2006) are used to reduce the length of the questionnaires. Similarly, in essay 5 a shortened conceptualization based on the measurement instrument from Hong and Thong (2013) is used.

**Types of Processing.** One of the main points of criticism regarding the privacy calculus is that only high-cognitive-effort processing is considered to explain consumers' data disclosure decision-making whereas the influence of low-cognitive-effort processing is mostly ignored (Dinev et al., 2015). This is in contrast to more psychological research streams where it is commonly accepted that individuals do not purely base their decision-making on high-cognitive-effort processing and that individuals do not always act "rationally" (Epstein, 1994; Stanovich and West, 2000; Kahneman, 2012; Evans and Stanovich, 2013). These theories assume individuals to base their decision on two processing types, which are also called processing systems (Epstein, 1994; Slovic, Finucane, Peters and MacGregor, 2004; Kahneman, 2012; Evans and Stanovich, 2013). Most of these dual processing theories describe the two processing systems in a very similar way: i) processing system 1 is intuitive and can be used even subconsciously. This type can be used to process several inputs simultaneously, is very fast and requires only low cognitive effort. Factors like vividness, immediacy, and individuals' feeling states are important information for processing with system 1 (Epstein, 1994; Loewenstein, Weber, Hsee and Welch, 2001; Slovic et al., 2004; Kahneman, 2012; Evans and Stanovich, 2013). From now on this processing type is simply referred to as low-effort processing (cf. Dinev et al., 2015); ii) processing system 2 can be described as a more conscious reasoning and deliberative thinking procedure in order to process the inputs in a sequential order. This processing type is cognitively very demanding and time-consuming. Especially inputs like probabilities and severities are important for processing with system 2 (Epstein, 1994; Slovic et al., 2004; Kahneman, 2012; Evans and Stanovich, 2013). From now on this processing type is simply referred to as high-effort processing (cf. Dinev et al., 2015). When individuals base their decision-making only on system 2 it should lead to a decision-making that resembles the one of a homo economicus under the assumption that all relevant information is accessible (and processable) by the individuals. Thus, deliberative weighing of benefits against risks for a data disclosure according to the privacy calculus can clearly be attributed to system 2 processing (cf. Kahneman, 2012; Dinev et al., 2015). Decision-making based on system 1 processing is the focus in several publications. For instance, the feelings-as-information theory (Schwarz and Clore, 1983, 2003), the risks-as-feelings theory (Loewenstein et al., 2001), or the affect heuristic (Finucane, Alhakami, Slovic and Johnson, 2000; Slovic, Finucane, Peters and MacGregor, 2002, 2007) discuss the impact of affective states on decision-making.

According to these theories, individuals can rely on both processing systems to make their decision respectively to solve a certain task. However, the degree of influence of the respective processing type on a decision can vary depending on the person, the situation, and the decision to be made (Daw, Niv and Dayan, 2005; Kahneman, 2012). Also, the two processing systems can interact with each other during decision-making (Loewenstein et al., 2001; Daw et al., 2005; Slovic et al., 2007; Kahneman, 2012). For instance, system 1 can make suggestions for system 2 (e.g., regarding the privacy risk assessment associated with a data disclosure), which can be adopted, modified, or completely rejected and overruled by system 2 (Kahneman, 2012).

***Affect as an Umbrella Term.*** The term affect is tightly linked to system 1, i.e., low-effort processing (Slovic et al., 2007). However, affect is an umbrella term which is used differently depending on the research streams (Zhang, 2013). This chapter introduces some of the most important concepts regarding affect drawing mainly on the work of Russell (2003, 2009), Zhang (2013) and Finucane, Alhakami, Slovic and Johnson (2000). However, this is not intended to be a comprehensive overview of these concepts (for more details, cf. Russell, 2003, 2009; Slovic et al., 2007; Zhang, 2013).

To discuss the more abstract meaning of affect, Zhang (2013) and Russell (2003, 2009) use the term *core affect*: according to their more general designed frameworks, core affect is always present in every individual. Core affect is a neurophysiological state experienced as raw feelings (Russell, 2003, 2009). This state can vary between individuals as well as it can vary over time or due to stimuli. Nevertheless, core affect is always present, i.e., time unconstrained. Core affect must not be directed or attributable to a certain object or stimulus, nevertheless it can be directed or attributable to something (Russell, 2003, 2009; Zhang, 2013). Core affect consists of two dimensions that describe the current core affect of an individual: i) the valence direction, i.e., does an individual feel good or bad; and ii) the arousal level, i.e., how activated (excited) or deactivated (sleepy) is an individual (Russell, 2003, 2009; Zhang, 2013). “Core affect is a fundamental concept that is the basis to all other affective concepts [such as affective reactions, feelings, emotions, and mood] making them affective in nature” (Zhang, 2013, p. 254). Therefore, drawing on these constructs for decision-making is clearly attributable to system 1, i.e., low-effort processing. This common nature between affective reactions, emotions, and mood explains why there are many different definitions and understandings of these concepts and why affect serves as an umbrella term (Russell, 2009; Zhang, 2013). In the following, a short distinction between the more specific manifestations of affective states, such as emotions, feelings, mood, and affect according to the affect heuristic is provided as a basis for this thesis.

***Emotions and Feelings.*** Emotions and feelings are often used as interchangeable synonyms (cf. Zhang, 2013). For the sake of uniformity, this thesis draws on the term feelings. Feelings are evoked by a specific and attributable stimulus. This is in contrast to individuals’ mood, for which there is usually no attributable reason or stimulus (Russell, 2009; Zhang, 2013). Feelings also have a shorter lifespan than moods (Russell, 2009; Zhang, 2013). Feelings exist only as long as the supporting perceptions or other elicitors are present (Russell, 2003; Scherer, 2005). When examining individuals’ decisions or assessments, individuals can be confronted with a decision-unrelated stimulus, for example, the weather being currently sunny or rainy. This stimulus is unrelated to individuals’ assessments of their general life-satisfaction. With the sunny stimulus, individuals are more satisfied with their lives in general than under the rainy condition (Schwarz and Clore, 1983). Thus, even affective states evoked by a stimulus that is completely unrelated to a specific decision can influence this specific decision (Schwarz and Clore, 1983, 2003). Therefore, another distinction of evoked feelings is possible: feelings evoked by a decision-related or unrelated stimulus (cf. Schwarz and Clore, 2003; Dunn and Schweitzer, 2005). Feelings can also be subdivided into more



fine-granular distinct affective states, such as fear, anger, and happiness (Russell, 2003). In essay 5, the focus is on the impact of positive feelings, evoked by a disclosure-decision unrelated stimulus, on consumers' personal data disclosure willingness.

***Affect According to the Affect Heuristic.*** Another similar concept to emotions that influences decision-making based on affective states is the affect heuristic examined in essay 2 (Finucane et al., 2000; Slovic et al., 2002, 2007). Slovic et al. (2007) define affect in their framework as “the specific quality of “goodness” or “badness” (i) experienced as a feeling state (with or without consciousness) and (ii) demarcating a positive or negative quality of a stimulus. Affective responses occur rapidly and automatically” (Slovic et al., 2007). These affective responses can impact assessments and decisions, for example privacy risk assessments and the decision to disclose personal data (cf. Slovic et al., 2007).

Decision-making based on affect according to the affect heuristic (cf. Finucane et al., 2000; Slovic et al., 2002, 2007) is similar to decision-making based on feelings (cf. Schwarz and Clore, 1983, 2003) and was not explicitly distinguished in the more generally designed frameworks of Zhang (2013) and Russell (2003, 2009). This section shortly provides a fine-granular distinction applied in this thesis between the concept of affect according to the affect heuristic (from now on simply referred to as affect) and emotions. First, affect is the very first intuitive association of goodness/badness towards a certain stimulus experienced as an affective state. Therefore, affect mainly focuses on the perceived valence of a certain stimulus while the concept of emotions focuses on both, the valence and arousal that is present in an individual (Russell, 2003; Zhang, 2013). Second, the concept of affect is always focused on a certain stimulus and due to the very short-lived and intuitive character of affect, it is always related to the disclosure-decision in this thesis (cf. essay 2). Although present feelings are evoked by a certain stimulus, in contrast to the concept of affect, the concept of emotions does not necessarily focus on the stimulus but rather on the feeling states of individuals. Feelings are also not necessarily related to a certain disclosure decision as feelings can be evoked by a stimulus unrelated to the decision (cf. essay 5). However, such evoked feelings can similarly impact unrelated decision-making (Schwarz and Clore, 1983).

***Data Sharing Cooperation.*** A factor that could alter the impact of low-effort processing heuristics, e.g., relying on affect or feelings for consumers' disclosure decision-making, could be the existence of a data sharing cooperation (DSC). In this thesis a DSC refers to the procedure that a firm shares consumers' personal data with further firms or organizations. Therefore, consumers in a disclosure setting with a DSC disclose their data to a firm which subsequently shares their data with further parties (cf. Figure 1, right). The reason for a DSC could be to create more value by enabling or improving services, or simply by monetizing the data (Smith et al., 2011; Wharton School, 2019). In contrast, in a dyadic data disclosure setting consumers disclose their data only to one firm which does not share their data with further parties (cf. Figure 1, left). There are several differences between these two disclosure settings which could impact consumers' disclosure decision-making.

For instance, the assessment of privacy risks in a deliberative manner, as assumed in the privacy calculus, could seem too difficult for consumers in a DSC setting due to the increased number of parties obtaining personal data. Therefore, they might rely more strongly on low-effort-processing in disclosure settings with a DSC compared to dyadic disclosure settings (cf. Daw et al., 2005; Pezzulo, Rigoli and Chersi, 2013; Maglio and Reich, 2019). This is examined in essay 2.

Also, the privacy risk perception associated with a data disclosure setting with a DSC could vary between consumers. For instance, some consumers could perceive that a DSC i) increases their

privacy risks, e.g., due to additional firms obtaining the data (cf. Peter and Tarpey, 1975; van den Braak, Choenni, Meijer and Zuiderwijk, 2012; Gartner, 2018), ii) reduces their privacy risks, e.g., due to exchange of security know-how (cf. Lei and Slocum Jr., 1992; Mason, 1993), or iii) does not affect their privacy risks at all, e.g., as consumers may avoid to think about consequences (cf. Kool, McGuire, Rosen and Botvinick, 2010). Consequences of a DSC regarding consumers risk perception are examined in essay 1 and 3.

Similarly, it could be possible that one of the firms in the DSC outshines all other firms and is the dominant, i.e., the most relevant, firm for the decision-making process (similar to a dominant firm in a strategic alliance, e.g., British Airways compared to their franchise partners, cf. Netzer, 1999). For example, this could be the firm with the biggest revenue, the one with the best reputation, or the touchpoint firm, i.e., the one the consumers disclose their data to. Therefore, the firm order in the DSC could be a characteristic that impacts consumers' disclosure decision. Another effect of a dominant firm could be that it might serve as an anchor: for instance, when the other firms in the DSC are associated with less privacy risk than the anchor, this could lead to an increased willingness to disclose (cf. Tversky and Kahneman, 1974). An additional influential aspect in a DSC setting for consumers disclosure decision could be whether consumers perceive the data sharing between firms as necessary to enable or improve the service for consumers, or if the DSC exists only for data monetization purposes (cf. European Commission, 2021a, 2021b).

## Research Methods

**Groundwork.** To give an overview of the current state of research regarding DSCs between firms and low-cognitive-effort decision-making in personal data disclosure situations, a broad and structured literature review for the topic of personal data disclosure was conducted. The procedure for the structured literature review was based on Webster and Watson (2002) and Tranfield, Denyer and Smart (2003). This review considered literature between 1991 and early 2017. This review was not only used as a basis for the essays presented in this thesis but also for a research proposal approved by the *Deutsche Forschungsgemeinschaft* (DFG) as well as for a published book contribution (cf. Specht-Riemenschneider et al., 2019).<sup>5</sup> A brief overview of the structured literature review is attached in the appendix.

Due to the scarce literature on data sharing cooperations between firms, 14 comprehensive interviews with consumers as well as researchers in the context of personal data and information systems (IS) were conducted based on Meuser and Nagel (1989) as well as Myers and Newman (2007). This was done to refine the planned research projects for this thesis on the consumers' perspective on data sharing cooperations. The obtained knowledge was the first input for the five essays.

**Samples.** In order to examine the research questions in essays 1-3 as well as in essay 5, three scenario-based experimental online surveys were created with Questback Enterprise Feedback Suite. The surveys were based on hypothetical scenarios as this is a common approach in IS privacy research (e.g., Brakemeier, Wagner and Buxmann, 2017). All samples were collected in cooperation with ResponDi, a German market research firm which is well-established in scientific research. All surveys included only established measurement instruments which were identified via several literature reviews. These measurement instruments were adapted to the research context if necessary. The questionnaires and scenarios in all surveys were checked for comprehensibility by means of interviews with potential participants as well as experts in the field of privacy before the surveys were launched.

The first survey conducted for essay 1 included four scenarios and led to a sample size of 61.

In the second survey, 364 completed questionnaires were obtained in total. The sample consisted of two groups with different scenarios. The complete sample was used for essay 2, whereas for essay 3 only a smaller subsample was used due to a narrower research focus that only was applicable to one of the two groups. Thus, one group was removed for data analysis in essay 3, leading to a sample size of 182 participants in essay 3.

The third survey was conducted for essay 5, which had a total sample size of 368 participants. The sample consisted of two groups. However, this time the groups obtained the same scenario but differed only regarding their positively valenced feelings which were manipulated via an autobiographic recall at the very beginning of the survey (cf. Martin, 1990; Jallais and Gilet, 2010).

For the quantitative meta-analysis in essay 4, the privacy paradox literature review of Kokolakis (2017) was used as foundation and was complemented with recent publications from 2015-2020 based on the same procedure. Of these publications only studies that quantitatively examine an effect of privacy concerns or privacy risks on disclosure or protection willingness were further examined via meta-analysis.

---

<sup>5</sup> Due to copyright restrictions from the publisher, this article was not allowed to be part of this thesis.

**Statistical Analysis.** The data was prepared and analyzed with *R studio version 1.2*. For Fisher's randomization test, the R package *EnvStats* (Millard, 2013) was used. The mediation test in essay 3 was conducted with the R package *mediation* (Tingley et al., 2014). The procedure of the quantitative meta-analysis in essay 4 was based on Del Re (2015), Quintana (2015), and Balduzzi, Rucker and Schwarzer (2019). For the meta-analysis, the R packages *MAd* (Del Re and Hoyt, 2018), *metafor* (Viechtbauer, 2020) and *compute.es* (Del Re, 2020) were applied. In order to compare the resulting effect sizes in essay 4, the R package *cocor* (Diedenhofen, 2016) was used. For survey-based studies, Cronbach's alpha and factor loadings were calculated with *SmartPLS 3* if *structural equation modeling* (SEM) (Hair, Hult, Ringle and Sarstedt, 2016) was applied, otherwise the R package *psych* (Revelle, 2021) was used.

To test the hypothesized research models in essay 2 and 5, the prepared data were analyzed via SEM. To be precise, *partial least squares SEM* (PLS-SEM) was applied and conducted in *SmartPLS 3*. It should be noted that there is an ongoing discussion about the advantages and disadvantages of PLS-SEM compared to *covariance-based SEM* (CB-SEM) (e.g., Rönkkö and Evermann, 2013; Hair Jr et al., 2017). CB-SEM and PLS-SEM differ in several ways. One of the fundamental differences is in the statistical objective of these two SEM methods: the aim of CB-SEM is to minimize differences between the observed sample covariance matrix and the estimated theoretical covariance matrix. Unlike in CB-SEM, in PLS-SEM the statistical objective is to maximize the explained variance for the dependent variables (Hair Jr et al., 2017). In essay 2, the research focus is on comparing the effect sizes of affect on disclosure willingness between two different disclosure settings. The aim is to investigate in which disclosure setting affect explains more variance in the dependent variables. Thus, the appropriate SEM method for such a research aim is PLS-SEM. Also, for essay 5, this is the adequate method as PLS-SEM is suited to be applied when a theoretical model is expanded, and PLS-SEM is also designed to work with continuous moderators as well as with complex models. Additionally, in both models some variables are non-normally distributed, which make the selection of PLS-SEM even more appropriate as there are no distributional requirements for this method (Hair Jr et al., 2017).

## Summary of the Five Essays and How They are Related

The first essay “An Exploratory Study of Risk Perception for Data Disclosure to a Network of Firms” co-authored with Thomas Widjaja and Jan H. Schumann was published as a short paper in the *Proceedings of the 14<sup>th</sup> International Conference on Wirtschaftsinformatik 2019*. The second essay “The Effect of Data Sharing Between Firms on Low-Cognitive-Effort Processing – An Integrative Approach” has not yet been submitted to a conference or journal. The third essay “Consumer Groups and Their Risk Perception in a Data Sharing Cooperation Between Two Firms” was published in the *Proceedings of the International Telecommunications Society 2020*. The version in this thesis is a slightly revised version of that essay which can also be found via the *Proceedings of the International Telecommunications Society 2020*. The fourth essay “The Impact of Abstraction Levels on the Effect Sizes of Privacy Concerns and Privacy Risks – A Quantitative Meta-Analysis” was submitted to the *29<sup>th</sup> European Conference on Information Systems 2021*. The fifth essay “The Effects of Positive Feelings and Arousal on Privacy Decision-Making” was published in the *Proceedings of the 23<sup>rd</sup> Biennial Conference of the International Telecommunications Society 2021*. Essay 5 was additionally awarded with the Student Paper Award at the *23<sup>rd</sup> Biennial Conference of the International Telecommunications Society 2021*. Except for the first essay, all essays are single author contributions.

A brief overview of the primary research focus and disclosure settings applied in the essays are displayed in Figure 3. A more detailed description of the essays and their contribution to the research objectives are provided in the following sections.

		Low-Cognitive-Effort Processing (RO: 2)			Privacy „Costs“ (RO: 3)	
Object of Investigation		Affect	Feelings + Arousal	Cognitive Effort	Privacy Risks	Privacy Concerns
Variable						
Setting	<b>Dyade</b>	Essay 2: Comparison of affect's effect sizes between dyadic and data sharing cooperation settings	Essay 5: Examining the effect of positive unrelated feelings and arousal on willingness to disclose		Essay 4: Examining differences between privacy concerns, privacy risks and their effect sizes	
	<b>Data Sharing Cooperation (RO: 1)</b>				Essay 1: Comparison of perceived privacy risks	
				Essay 3: Examining distinct consumer groups based on implications of a data sharing collaboration		

Figure 3. Overview and content of the five essays.

**Essay 1.** Generally, research on DSCs between firms is scarce.<sup>6</sup> One unexplored aspect of DSCs is how additional firms in a DSC impact consumers' risk perception for a personal data disclosure. In order to address this research gap, consumers' privacy risk perception in a disclosure setting with a DSC between two firms is compared with the risk perceptions regarding dyadic disclosures to the identical firms.

There are two possible outcomes for the privacy risk perception in this scenario: i) the privacy risk in the DSC setting is perceived to be higher compared to the maximum perceived privacy risks of the two respective dyadic settings. This could be the case as the privacy risks perceived when disclosing to the two firms in a dyadic setting should contribute to the total privacy risk in the DSC disclosure setting. This should increase the total perceived privacy risk in the DSC setting above the maximum perceived privacy risk of the two dyadic settings, e.g.,  $Risk_{DSC} > Risk_{Dyad1\_Max} > Risk_{Dyad2\_Min}$  (cf. for simple additivity: Peter and Tarpey, 1975; for a function with diminishing marginal value cf. Kahneman and Tversky, 1979; Tversky and Kahneman, 1992). ii) consumers could perceive less privacy risk in the DSC disclosure setting than the maximum of the two dyadic settings, e.g.,  $Risk_{Dyad1\_Max} > Risk_{DSC} > Risk_{Dyad2\_Min}$  or  $Risk_{Dyad1\_Max} > Risk_{Dyad2\_Min} > Risk_{DSC}$ . This could be due to increased data protection through technical know-how or mutual control between the firms in the DSC setting (cf. Hamel, Doz and Prahalad, 1989; Mason, 1993). This leads to the following research question:

*Is consumers' privacy risk perception in a disclosure setting with a DSC between two firms higher or lower than the maximum perceived privacy risk of the two respective dyadic settings?*

Based on a within-subject design (n=61), the results show that participants perceive the disclosure in the DSC setting as significantly less risky than the riskiest of the two dyadic data disclosures ( $Risk_{Dyad1\_Max} > Risk_{DSC} > Risk_{Dyad2\_Min}$ ). Therefore, this essay contributes to an increased understanding of privacy risks (RO3) in DSC disclosure settings (RO1).

This work offers first insights for theory as well as practitioners: research should examine the exact reasons and mechanisms that lead to this observation as a DSC setting has new aspects that are not existent in dyadic disclosure settings. For instance, research could focus on consumers' expectancy that firms in a DSC decrease the privacy risk due to mutual control that leads to less data mishandling, or due to an increase in data protection through technical know-how exchange. However, research should also focus on "non-rational" explanations that could explain the observed results (Dinev et al., 2015). For example, low-effort processing draws on different information than high-effort processing (Loewenstein et al., 2001). A stronger reliance on low-effort processing in a DSC setting could be another explanation for the resulting low risk perception in a DSC setting (cf. Dinev et al., 2015).

For firms that are associated with a very high privacy risk, these results indicate that it is possible to lower consumers' total perceived privacy risk via a data sharing cooperation with a firm, that is associated with less privacy risk in the mind of consumers. This could reduce consumers' perceived privacy risk to an acceptable level and in turn, make data collection for the firms more successful in total. Especially, the privacy risky firm is clearly more successful regarding data collection in such a DSC than without being in a DSC. However, the privacy unrisky firm would be even more successful regarding data collection on its own, i.e., without being in a DSC with a privacy risky

---

<sup>6</sup> In essay 1 and essay 2, the term *Business Network Data Exchange* (BNDE) is used synonymously to describe a *Data Sharing Cooperation* (DSC) between firms.

firm. This could make redistribution mechanisms necessary to balance cooperation benefits between privacy risky and unrisky firms in a DSC.

These results are subject to some limitations, such as the small sample size, or that the within-subject design misses an order randomization for the different disclosure settings. Also, the simplest form of a data sharing cooperation consisting of only two firms was used. Further studies could use a bigger sample size and a more complex DSC network to verify the observed results.

**Essay 2.** This essay follows the call of Dinev et al. (2015) for more research on low-effort processing in the context of data disclosures. Based on first insights from essay 1, this work focuses on differences between dyadic and DSC disclosure settings (RO1) regarding low-effort processing (RO2). In particular, this essay examines the following research question:

*Is consumers' reliance on low-effort processing for their decision-making stronger in a personal data disclosure setting with a DSC between two firms, or in an identical dyadic disclosure setting (without data sharing between the two firms)?*

Only few studies have examined low-effort processing in the context of data disclosures before (e.g., H. Li et al., 2011; Wakefield, 2013), but research on DSC disclosure settings is even more scarce. Thus, interdisciplinary dual-processing literature is used in this essay to develop hypotheses on whether a stronger reliance on low-effort processing in DSC settings is prevalent. The hypotheses development is especially based on reinforcement learning literature (e.g., Daw et al., 2005; Gläscher, Daw, Dayan and O'Doherty, 2010), and cognitive effort studies (e.g., Garbarino and Edell, 1997; Pezzulo, Rigoli and Chersi, 2013). According to these studies, a certain decision can be made by using both processing types, high-effort and low-effort processing. The degree of reliance on these processing systems can vary depending on the situation and the individual (Garbarino and Edell, 1997; Pezzulo et al., 2013). Based upon the knowledge of these interdisciplinary research streams, a simplified consumers' disclosure decision-making process is developed. Applying this decision-making perspective, a DSC setting signals consumers increased cognitive requirements for high-effort processing via the statement that the firms share consumer data. Particularly, this statement signals consumers that their disclosure decision-making is more complex under high-effort processing due to the increased number of firms that obtain their personal data in a DSC. Thus, to reduce cognitive requirements and to enable a higher decision-certainty, a stronger reliance of consumers on low-effort processing for their decision-making in DSC settings is hypothesized (cf. Garbarino and Edell, 1997; Daw et al., 2005; Pezzulo et al., 2013). When consumers rely more strongly on low-effort processing in a DSC setting compared to an identical dyadic setting, the following is hypothesized: consumers perceive their decision-making in retrospect, i.e., *after* the decision-making process, to be less complex and perceive a lower decision uncertainty in the DSC setting than in the dyadic setting (Garbarino and Edell, 1997; Pezzulo et al., 2013).

In order to examine the degree of reliance on low-effort processing between the two disclosure setting types, the privacy calculus is used as a base-model (Smith et al., 2011) and is extended with affect as an instance of low-effort processing (Slovic et al., 2007). The effects of affect on consumers' perceived benefit, perceived privacy risk, and their willingness to disclose is examined (H. Li et al., 2011; Wakefield, 2013) and compared between dyadic and DSC disclosure settings.

To this end, a hypothetical online survey with two groups, i.e., dyadic (n=172) and DSC (n=165) disclosure setting, is used. In the resulting SEMs for both disclosure settings, affect increases participants' perceived benefit, decreases perceived privacy risk, and increases participants' disclosure willingness. Participants' privacy concerns and trust do not impact their disclosure

willingness directly but indirectly via perceived privacy risk in both settings. As hypothesized, affect exerts a stronger effect, i.e., participants rely more strongly on affect for their perceived benefit and for their willingness to disclose in the DSC setting. Contrary to the initial expectation, affect does not have a stronger effect on perceived privacy risk in the DSC setting. As furthermore hypothesized, participants in the DSC setting perceive decision-making to be less complex and were more certain regarding their decision in retrospect.

This study offers important theoretical implications: First, dual-processing knowledge of reinforcement learning, and cognitive effort studies are used to develop a simplified decision-making process. This new perspective enables new hypotheses regarding consumers' decision-making and their reliance on low-effort processing for data disclosures. This is particularly helpful for the almost unexplored field of DSC disclosure settings. This perspective could also help to understand whether consumers' reliance on low-effort processing is increased when they are asked to disclose more data types.

Second, this study emphasizes that consumers' disclosure decision-making is not solely based on high-effort weighing of perceived benefits against perceived privacy risks. Therefore, it could explain behavior that deviates from decision-making purely based on high-effort processing. Especially in DSC settings, consumers rely more strongly on low-effort processing and thus, researchers need to explicitly consider this when examining DSC contexts.

Besides, this study offers implications for practitioners as well. It may help firms and regulators to adapt their consumer communication strategy in DSC settings to the increased low-effort processing reliance of consumers. An easier processable information format, such as simple privacy icons in addition to long and complex privacy policies, could help consumers to include more information when relying more strongly on low-effort processing in DSC settings. In turn, this could help firms to increase disclosure willingness of their consumers. Moreover, this essay could help legislators to improve protection of consumers' privacy, especially in DSC settings.

However, this study must be viewed in light of its limitations, which could open further research avenues. Although the hypotheses build on established insights of the dual-process literature and are mostly confirmed in the study, the applied method is not suited to verify if the assumed mechanism of the decision-making process is correct. Therefore, to examine what is exactly happening in the mind of consumers, neurological methods could be more adequate. Also, only the affect heuristic was used as a proxy for low-effort processing. Thus, other low-effort constructs and heuristics could be examined to confirm these results in future research. Future studies could also examine more complex DSC disclosure settings, i.e., settings with a DSC between more than just two firms. Last, consumers are not always completely aware of the data sharing practice between firms, which is why in these specific DSC situations the obtained results of this study are probably not applicable.

**Essay 3.** Based on the first interviews conducted and due to insights from essay 1, this work examines consumers' perspectives on implications for their perceived privacy risks due to the data sharing process of firms in a disclosure setting with a DSC between two firms. Thus, essay 3 contributes primarily to a more detailed understanding of consumers' privacy risk perception (RO3) by considering new aspects existent in the context of DSC (RO1). Consumers can assess a DSC between firms as either i) risks are increasing ("risks increasing"-group), e.g., because additional data transfers could be necessary (cf. Peter and Tarpey, 1975; Gartner, 2018); ii) risks are decreasing ("risks decreasing"-group), e.g., because firms exert mutual control or exchange technical data protection know-how (Hamel et al., 1989; Mason, 1993); or iii) risks are unaffected



(“unreflected”-group), e.g., because consumers do not think intensively about the impact of such a data sharing practice on their risks (cf. Kool, McGuire, Rosen and Botvinick, 2010) or simply see neither a positive nor a negative impact due to it.

The first research question relates to whether these consumer groups really exist:

*Are there consumer groups with distinct perceptions of a data sharing cooperation between two firms?*

Besides verification of the groups’ existence and their distribution, the differences between the groups especially regarding privacy risk perception and disclosure willingness is examined. The expectation for the “risks increase”-group is that these consumers perceive a rather high level of risks and have a rather low willingness to disclose personal data. In contrast, the “risks decrease”-group is expected to perceive a rather low level of risks and is rather willing to disclose personal data. However, the characteristics of the third group, i.e., the “unreflected”-group are hard to predict. This leads to the second research question:

*What are the differences between consumers who see their privacy risks not affected due to a data sharing cooperation and consumers who see their privacy risks affected?*

The “unreflected”-group that does not see any influence on privacy risks due to data sharing between firms are hypothesized to have this perspective simply because it can be easily obtained without thinking about risk consequences of a DSC. Thus, the “unreflected”-group is hypothesized to spend less cognitive effort in assessing their privacy risks and to deal less intensively with privacy relevant aspects of a disclosure situation than the other two groups. This is expected due to less privacy intrusion experiences of consumers in the “unreflected”-group compared to the other groups, which is why for these consumers intensive thinking about detailed privacy risk implications of a certain data sharing practice is not dominant or necessary in their mind (Osberg and Shrauger, 1986; Kahneman, 2012). When consumers have less privacy intrusion experiences, they mostly have less privacy concerns in general (Smith et al., 1996; Cranor, Reagle, Joseph, and Ackerman, M. S., 1999; Awad and Krishnan, 2006). This, in turn, leads usually to a lower privacy risk perception and to an increased willingness to disclose personal data (Awad and Krishnan, 2006; Smith et al., 2011; Dinev et al., 2015). Accordingly, the “unreflected”-group is hypothesized to have less privacy intrusion experiences, less privacy concerns, less perceived privacy risks and a higher willingness to disclose personal data compared to the other two groups. It is also hypothesized that the “unreflected”-groups’ perspective on data sharing procedures between firms, i.e., that this does not affect their risks, increases their disclosure willingness. This effect is expected to be fully mediated by their privacy risk perception.

In order to address these research questions and hypotheses, this study draws on a subsample of essay 2, i.e., it only examines participants with the hypothetical DSC setting (n=182). Participants are asked in retrospect how this data sharing procedure between firms affects their privacy risks. Based on this answer, participants are split into the three aforementioned groups. Participants are almost equally distributed between the three groups with a slight dominance of the “risks increase”-group. This answers RQ1 as all perspectives regarding the impact of DSCs on privacy risks exist among consumers.

Regarding the differences in RQ2, the hypotheses are confirmed via Fishers’ randomization test and via mediation test: participants in the “unreflected”-group have used less cognitive effort for their privacy risk assessment and for dealing with privacy relevant aspects in the situation compared to the other two groups. Also, they have less privacy intrusion experiences, less privacy concerns,

less perceived privacy risks and a higher willingness to disclose personal data compared to the other two groups. Moreover, the perspective that such a data sharing procedure between firms does not impact privacy risks has an effect on disclosure willingness. As hypothesized, this effect is fully mediated by consumers' privacy risk perception while it was controlled for the effects of perceived benefits and privacy concerns.

This work provides several theoretical implications, such as a refined understanding of consumers' risk perception in a DSC context (RO1+3). Thus, this essay contributes to a *theory for analyzing* (cf. Gregor, 2006) as new consumer groups were explored and compared. This work also provides initial insights into the group differences. Also, it displays a first way to identify consumers who do not effortlessly assess privacy relevant details in a DSC disclosure situation without asking them directly. This is especially helpful for future cognitive effort studies in DSC disclosure settings, as it could prevent to trigger participants to the topic of cognitive effort.

This study offers implications for practitioners as well. Two-thirds of the participants do not think that a DSC would have a negative impact on their privacy risks. Thus, the results are a first indication that firms do not need to be too anxious about being part of a DSC. Also, one-third of the consumers do not intensively think about consequences for their privacy risks due to data sharing procedures between firms. These consumers have a relatively high disclosure willingness. However, it also displays that two-thirds of the consumers do think about consequences for their privacy risks due to data sharing between firms. Thus, these consumers eventually could be convinced to disclose data with logical arguments, for instance, the application of high encryption standards (cf. Tsai et al., 2011). Similarly, emphasizing the benefits arising through a data sharing cooperation, such as personalization or time savings, could finally increase consumers' disclosure willingness (Smith et al., 2011).

However, this study has some limitations. The distribution of the consumer groups may vary for different firm constellations or for a higher number of firms in the DSC. Furthermore, the results could be dependent on cultural or regulatory differences (cf. Miltgen and Peyrat-Guillard, 2014).

**Essay 4.** Privacy concerns and privacy risks are two of the most important factors that reduce consumers' disclosure willingness (Smith et al., 2011; Y. Li, 2012). Despite extensive research in this field, there is still some ambiguity regarding the concepts of privacy concerns and privacy risks, which became clearer through the literature reviews conducted for the previous essays in this thesis.

Sometimes researchers do not differentiate sufficiently between privacy risks and privacy concerns and use them ambiguously (e.g., Y. Li, 2012). Furthermore, some studies find a significant effect of privacy concerns on disclosure or protection decisions (e.g., Aivazpour and Rao, 2020), while other studies find only small or even non-significant effects (e.g., Zafeiropoulou, Millard, Webber and O'Hara, 2013). The phenomenon that this effect is sometimes not significant, i.e., that consumers' privacy concerns are not in line with their privacy behavior, is also known as *privacy paradox* (Norberg et al., 2007; Pavlou, 2011).<sup>7</sup> These mixed findings make it unclear when and why significant effects exist.

In order to better interpret such mixed findings, this essay strives to increase the understanding and differences of privacy concerns and privacy risks. Thus, this essay addresses RO3. In particular, the varying effect sizes of privacy concerns and privacy risks among different studies are investigated using meta-analysis by additionally considering the applied abstraction levels.

---

<sup>7</sup> The term privacy paradox is used for even more phenomena (for details cf. Kokolakis, 2017; Risius, Baumann and Krasnova, 2020). However, these are not within the scope of this work.

According to Davazdahemami et al. (2018), a construct such as privacy concerns can be measured on three abstraction levels: on a general, contextual, or a situation-specific abstraction level. They show that measuring privacy concerns (independent variable) and disclosure willingness (dependent variable) on different abstraction levels, i.e., unaligned, leads to weaker or even non-significant effects (Davazdahemami et al., 2018). However, this study goes a step further and seeks to understand which combinations of aligned abstraction levels are likely to have the strongest effect sizes of privacy concerns and privacy risks based on a sharpened conceptualization of the constructs. Thus, this leads to the following research aim:

*Distinguishing the constructs privacy concerns and privacy risks and understanding differences in the resulting effect sizes based on abstraction level combinations.*

Therefore, a meta-analysis is conducted whereby only literature is considered that quantitatively examines an effect of privacy concerns or privacy risks on disclosure or protection behavior<sup>8</sup> and additionally considers itself as a privacy paradox study. The latter is done to reduce publication bias. This leads to a final sample size of 27 publications.

Drawing on literature that developed privacy concerns measurement instruments (Smith et al., 1996; Malhotra et al., 2004; Hong and Thong, 2013) and based on knowledge of self-schemata literature (Markus, 1977; Sheeran and Orbell, 2000), this essay defines privacy concerns as a “generalized self-assessment regarding the disposition to develop concerns due to privacy issues” (essay 4, p. 5). Due to the general nature of privacy concerns, the strongest effect size is hypothesized for the aligned abstraction level combination where privacy concerns and the dependent variable (disclosure/protection behavior) are measured on a general level.

Consumers’ perceived privacy risks reflect the privacy costs that are associated with a specific disclosure decision (Malhotra et al., 2004; Smith et al., 2011; Kehr et al., 2015). Thus, this construct is the situational manifestation of the general tendency to develop privacy concerns. In line, in this essay privacy concerns are seen as the general antecedent of the situation specific privacy risks (Malhotra et al., 2004; Kehr et al., 2015). Accordingly, the strongest effect size is hypothesized for the abstraction level combination where privacy risks as well as the dependent variable are measured on a more specific, i.e., situational level. Furthermore, privacy risks are hypothesized to exert a stronger effect on disclosure behavior compared to privacy concerns when the variables are measured on a situational level. This is expected because privacy concerns were not initially designed to reflect situational privacy cost while this was the intended aim for privacy risks.

The results verify that privacy concerns exert the strongest effect on protection behavior when the variables are measured on a general level. The effect of privacy risks on disclosure behavior is the strongest when both variables are measured aligned on a contextual or a situational level. When all variables are measured on a situational level, the effect size for privacy risks on disclosure behavior compared to the effect size of privacy concerns on disclosure behavior is significantly stronger.

This study offers several theoretical contributions, such as a refined understanding of privacy concerns as a general self-schema to develop privacy concerns. Similarly, it provides a sharpened understanding of privacy risks as the situational privacy cost manifestation of consumers’ general tendency to develop privacy concerns. This understanding allows to explain even paradoxical seeming findings (e.g., Mothersbaugh et al., 2012; Zafeiropoulou et al., 2013). It also helps to build

---

<sup>8</sup> The considered studies did not have to examine actual behavior. Measurements of disclosure intention, willingness, and self-reported as well as actual behavior were considered and not separately examined in this study to not further reduce the publication sample size. The same procedure was applied to protection behavior.

a more common understanding and differentiation of the constructs in future research. This enables a better comparability across different studies. Furthermore, the refined understanding helps to explain and predict effect sizes even for aligned abstraction level effects, which was not addressed in the study of Davazdahemami et al. (2018). Based on the obtained Pearson's  $r$  estimates, a better assessment and comparison of the effect sizes in previous privacy studies is possible. Also, the obtained Pearson's  $r$  estimates could help future researchers to plan their required study sample size more detailed in advance (Anderson, Baskerville and Kaul, 2017).

The limitations of the results must be taken into account, which could help future research to address the weaknesses. The structured literature review covers only privacy paradox studies that examined the discussed effects quantitatively but is far from covering all studies that examine such effects. Also, the number of publications in the subsamples is relatively small and heterogeneity of effect sizes is still high due to different covariates or different measurement instruments between the studies. A higher sample size in future research would enable a more detailed splitting of the publications to reduce heterogeneity and still achieve a sufficient number of publications in each subsample. Also, there is sometimes a huge difference between the number of observations in the subsamples and the subsamples are sometimes overlapping which could distort the applied effect size comparison test.

**Essay 5.** This essay extends essay 2 by considering the influence of positive feelings as well as by considering arousal levels on disclosure behavior instead of examining the affect heuristic. In particular, the positive feelings are evoked by a disclosure decision-unrelated stimulus. Such feelings are expected to influence even unrelated assessments and decisions. This expectation is based on dual-process literature such as the *feelings-as-information theory* (Schwarz and Clore, 1983, 2003). According to this theory, even unrelated positive feelings can decrease privacy risk perception and increase benefit perception. In this study, the research focus is on feelings evoked by an unrelated stimulus, which complements the research on the decision-related affect heuristic examined in essay 2. Furthermore, the influence of consumers' arousal level and not only the valence of the feeling state is examined. To consider both constructs together is rather rare in IS privacy research (there are few studies that examine arousal, for instance, Coker and McGill, 2020). However, this could be helpful as arousal is expected to increase individuals' reliance on low-cognitive-effort processing (cf. Svenson and Maule, 1993; Finucane et al., 2000; Ariely and Loewenstein, 2006; Ditto et al., 2006; Coker and McGill, 2020; Y. Kim et al., 2020). Therefore, an interaction effect of consumers' feelings and arousal levels on privacy related assessments is hypothesized to address the research question of this study:

*How do positively valenced unrelated feelings and arousal levels impact individuals' willingness to disclose personal data?*

Thus, this essay contributes primarily to RO2. To answer the research question, an online survey with a hypothetical disclosure setting placed in a social media context is conducted. The participants are asked to share personal data, such as a photo of them, with an Instagram account of a firm which operates in the field of soccer. Thus, this setting corresponds to a DSC disclosure setting. However, to examine special characteristics of such a DSC setting is not in the scope of this work. A similar research base model as in essay 2 is applied. Consumers' privacy concerns as well as the privacy calculus including consumers' willingness to disclose personal data as well as their benefit and privacy risk perceptions are included in the research model. To understand the effect of consumers' feelings and arousal on perceived (total) privacy risk in more detail, the following two privacy risk antecedents are considered besides privacy concerns: perceived risk

severity as well as perceived risk probability (cf. Howard and Gengler, 2001). Thus, this study contributes to RO3 as well.

The structural equation model results (n=368) confirm the influence of positively valenced unrelated feelings and arousal on disclosure willingness and its antecedents. Both, unrelated positively valenced feelings and arousal levels directly increase benefit perception without any significant interaction effect.

For the effects of feelings and arousal on perceived risk severity, neither significant direct effects nor a significant interaction effect is observable. In contrast, the interaction effect of positively valenced unrelated feelings and arousal on disclosure willingness, perceived (total) privacy risk, and perceived risk severity is significant, while the direct effects are not significant. This is due to a special type of interaction effect called crossover interaction (Loftus, 1978; Williams, 2015): arousal serves as a “switch” for the effects of unrelated positive feelings on perceived privacy risk, perceived severity and disclosure willingness. Under high arousal levels, stronger positive feelings decrease perceived privacy risk and risk severity, while disclosure willingness is increased. Whereas under low arousal levels, more positively valenced feelings have the opposite effect: they increase perceived privacy risk and risk severity, while disclosure willingness is decreased. Therefore, to correctly predict and understand the effects of more positively valenced unrelated feelings it is necessary to also consider the arousal level.

Additionally, this essay provides a first explanation for the switch function of arousal. The feelings-as-information theory (Schwarz and Clore, 1983, 2003) is dominant for the high arousal level case, as it explains and predicts the effects correctly for high arousal levels: consumers rely on their positive feelings for privacy related assessments and thus, perceive less privacy risk and are more willing to disclose their data. Whereas under low arousal levels, the *affect regulation theory* (Andrade, 2005) seems to be dominant as it is suitable to explain and predict consumers’ privacy related assessments: consumers want to maintain their positive feeling state and do not want to risk their positive feelings by disclosing personal data which is associated with a potential loss of privacy. Therefore, they perceive more risk and are less willing to disclose their personal data.

This study provides several important theoretical contributions: it addresses the field of positively valenced unrelated feelings and arousal levels, which is underexamined in IS privacy research. The study shows that the effect mechanism of these two constructs is different for the effect on the benefit side compared to the risk side of the privacy calculus. Furthermore, the influence of unrelated positive feelings and arousal on the privacy risk assessment is examined in detail. This essay also provides an explanation for the observed crossover interaction, which displays the feelings-as-information theory applicable for privacy assessments under high arousal while under low arousal levels the affect regulation theory should be able to explain privacy assessments best.

Similarly, this study offers insights for practitioners as well. It emphasizes that it is possible to alter disclosure willingness of consumers by using stimuli that evoke certain feelings. In this study, it was demonstrated that this is even valid when only positively valenced feelings are evoked that are decision-unrelated. However, this insight is also important for lawmakers: it indicates that it could be helpful to not only regulate the content of a disclosure consent form but also the degree to which an organization is allowed to evoke positive feelings or high arousal levels while consumers are asked for their consent (cf. Schaub, Balebako, Durity and Cranor, 2015; Y. Kim et al., 2020).

However, this study must be viewed in light of its limitations. For survey participation, participants needed to be interested in soccer and must have had an existing Instagram account. Thus, this sample may not reflect the whole population. Also, the interaction effect sizes are rather weak when

applying the standards of Cohen (1988) for direct effects. However, compared to published interaction effect sizes, the interaction effect sizes observed in this essay have to be interpreted as medium to large (Aguinis, Beaty, Boik and Pierce, 2005; Kenny, 2015). Furthermore, the arousal level is not manipulated in isolation (e.g., a recalled positive experience could either be a thrilling bungee jump experience with high arousal levels, or a relaxing sauna visit with low arousal levels). Therefore, future research could draw on a more representative sample and apply a 2x2 factorial design to examine the effects of feelings and arousal in more detail.

## Overall Discussion

The five essays in this thesis deepen the understanding of consumers' personal data disclosure decision-making. To this end, various research methods are performed, including i) multiple literature reviews on data disclosure decision-making, ii) quantitative meta-analysis, iii) empirical group-comparisons, and iv) regression analysis as well as structural equation modeling. Considering all essays as a whole, this thesis offers three main contributions to IS privacy research.

**Contributions.** The *first* contribution is primarily associated with RO1, i.e., to understand peculiarities of consumers' data disclosure decision-making in a DSC setting. In this thesis, new phenomena and factors are identified that play a crucial role for understanding consumers' decision-making in personal data disclosure settings with a DSC between firms. Especially three peculiarities of DSC settings are examined in this thesis, that could serve as a starting point for the scarce research in this context: i) a lower risk perception in DSC settings than expected based on traditional risk theory (Peter and Tarpey, 1975) or prospect theory (Kahneman and Tversky, 1979; Tversky and Kahneman, 1992) is observed in essay 1. This observation can be partially explained with the next two peculiarities of DSC settings examined in this thesis: ii) the impact of a DSC between two firms on consumers' perceived privacy risks, as examined in essay 3. Roughly one third of the participants think a DSC between two firms reduces their privacy risks while another third assumes that their privacy risks are not affected. Therefore, consumers' assessment of a DSC can be indeed positive, which could plausibly explain the results in essay 1. iii) an overall stronger reliance on low-effort processing for consumers' disclosure decision-making in a DSC setting compared to a dyadic setting is confirmed in essay 2. This is also strongly connected to the next contribution.

*Second*, this thesis contributes to RO2, i.e., to understand the impact of low-effort processing on personal data disclosure decision-making in more detail. In particular, in essay 2 perspectives of interdisciplinary dual-process literature (e.g., Daw et al., 2005; Pezzulo et al., 2013) are transferred to the field of privacy disclosure settings to explain consumers' decision-making. In this thesis, different constructs and stimuli are used to verify that affective states do influence benefit and risk perception as well as consumers' willingness to disclose. In contrast to previous research, this thesis does not only confirm that consumers depend on low-effort processing in their disclosure decision-making. The results in this thesis rather indicate that the impact strength of low-effort processing can depend on the situation, e.g., the disclosure setting (essay 2), and individual characteristics (essay 3). Also, previous research assumed positive affective states to generally increase consumers' willingness to disclose (e.g., H. Li et al., 2011; Wakefield, 2013). This is also observed in essay 2 in which the affect heuristic with the disclosure situation itself as decision-related stimulus is examined. However, essay 5 indicates that this is not as simple: the effect direction of positively valenced unrelated feelings can depend on the arousal level. This may even help to explain why some studies find non-significant effects of positively valenced feelings on disclosure willingness or privacy risk perception (e.g., Kehr et al., 2015; Kordzadeh, Warren and Seifi, 2016). As indicated by the results of previous studies (e.g., Kehr et al., 2015; Kordzadeh, Warren and Seifi, 2016), essay 2 and 5 show that low-effort processing affects benefit and privacy risk perception differently. This thesis additionally offers initial insights to understand this difference. For risk perception, a crossover interaction of arousal and positively valenced feelings is observed in essay 5 while arousal and feelings have a direct effect on benefit perception.

*Third*, in line with RO3, a more fine-granular differentiation of privacy risk and privacy concerns is provided in essay 4. This work emphasizes that privacy concerns are a general antecedent of privacy risk. In line, privacy concerns primarily exert an indirect effect via privacy risks on disclosure

willingness. This is confirmed by means of structural equation modeling in essay 2 and 5. This interpretation helps to establish a more unified conceptualization of privacy concerns and privacy risks (Malhotra et al., 2004; Hong and Thong, 2013). It also helps to better understand why some previous studies find only weak or non-significant direct effects of privacy concerns on disclosure willingness (e.g., Zafeiropoulou et al., 2013). Overall, this refined understanding helps to compare different studies, allows the interpretation of seemingly paradoxical results, and supports future privacy research in their study design (Davazdahemami et al., 2018).

Besides theoretical contributions, this thesis offers *practical implications*. Firms that want to increase their consumers' willingness to disclose personal data can do more than objectively providing more benefits for consumers or reducing privacy risks as suggested by previous research (cf. Smith et al., 2011; Keith, Thompson and Greer, 2012). Firms additionally could adapt the data disclosure situation itself in a way that increases consumers' positively valenced feelings and their arousal levels, which in turn lead to a higher benefit perception, a lower risk perception, and a higher willingness to disclose (cf. essay 2; essay 5; Wakefield, 2013; Kehr et al., 2015; Coker and McGill, 2020). Even unrelated stimuli can help to achieve this goal (cf. essay 5; Schwarz and Clore, 1983, 2003). Furthermore, firms do not need to worry too much about having a data sharing cooperation with other firms as most consumers see their privacy risk not negatively impacted by a DSC (cf. essay 3). In addition to that, firms may use a DSC disclosure setting to increase consumers' reliance on low-effort processing (cf. essay 2), which could sometimes, i.e., depending on the situation, be beneficial for firms (cf. essay 1 and 5).

Although drawing on this knowledge could help firms to be more successful in collecting personal data, it carries some disadvantages for consumers at the same time. Consumers are most vulnerable to disclose personal data in very positively valenced and highly aroused affective states. This is especially critical for DSC disclosure settings where low-effort processing is even more important. Therefore, this thesis indicates that regulators may need to protect consumers in particular when they are in such affective states and when confronted with a DSC disclosure setting. Also, this thesis could help consumers themselves as it displays their weak spots for personal data disclosures. When consumers know when they are most vulnerable to disclose personal data, they can try to counter their weak spot in these situations by becoming conscious of the reasons for their affective state and its' consequences (cf. Schwarz and Clore, 1983; Ciarrochi, Caputi and Mayer, 2003).

***Limitations and Avenues for Further Research.*** In addition to the limitations already discussed for each individual essay, the overall thesis has limitations that could open new avenues for further research.

This thesis solely draws on consumers' willingness to disclose and its antecedents such as privacy risk to examine consumers' privacy decision-making which is a common approach in IS privacy research (cf. Smith et al., 2011; Kehr et al., 2015; Al-Natour et al., 2020). Nevertheless, this is a limitation as actual disclosure behavior is not considered in this thesis and there can be a gap between intended and actual disclosure behavior (Norberg et al., 2007). Therefore, to measure actual behavior instead of self-reported behavior or intentions would be the best measurement approach for future studies (cf. Junco, 2013; Gerber et al., 2018). But still, disclosure intention and willingness to disclose are together with perceived benefits and privacy risks among the best predictors for actual disclosure behavior (cf. Ajzen and Fishbein, 1980; Keith et al., 2012; Gerber et al., 2018). In this regard, studies confirmed that privacy risks can not only impact consumers' actual disclosure behavior indirectly via disclosure intention (Keith et al., 2012), but can also exert a direct effect on disclosure behavior (Keith et al., 2015). Additionally, privacy risks impact consumers' self-reported data protection behavior (Miltgen and



Smith, 2015). Thus, perceived privacy risk should also be considered in future studies that measure actual behavior whenever possible.

Also, this thesis mostly draws on scenarios with hypothetical firms, i.e., unknown firms. But for firms, consumers had already experience with, trust is of high importance (Gefen, Karahanna and Straub, 2003; M.-S. Kim and Ahn, 2007). In essay 2, effects of trust are considered in the SEM (cf. Ozturk, Nusair, Okumus and Singh, 2017), resulting only in an indirect effect on disclosure willingness via perceived privacy risk. Nevertheless, to examine the role of trust in DSC disclosure settings including familiar firms as well as the role of trust regarding low-effort processing is important to expand knowledge and should therefore be considered in future studies.

Besides not examining known firms, this thesis neither examines how the order of the firms in the DSC setting (e.g., which firm is the touchpoint for consumers), or the single characteristics of each firm in a DSC disclosure setting (e.g., which firm is the largest, which creates the most value for consumers, or which is the best-known firm) affects consumers' decision-making. This is an almost unexplored research field that could include several, maybe opposing effects to explore in future research.

Similarly, the essays in this thesis examine only hypothetical settings where consumers are asked directly for their personal data. Depending on the regulation of the country and the situation, consumers are not always asked in an easily understandable and transparent way for their data in everyday life (Gindin, 2009; Tuunainen, Pitkänen and Hovi, 2009), or are not willing to read the privacy policies carefully (LINK Institut and SRG SSR, 2018; Latzer, Büchi and Festic, 2019). Thus, maybe they are not fully aware that they are about to disclose data and that this data is shared in a DSC. Thus, consumers probably behave differently in such situations compared to the observations in this thesis. To examine consumers' decision-making in such situations could be a new avenue for further research.

Also, in this thesis, the privacy risk and benefit levels are not manipulated specifically, for instance, by splitting participants into groups that must disclose more or less sensitive personal data (cf. Mothersbaugh et al., 2012) and obtaining more or less benefits. It could be helpful for future research to examine how varying benefit and privacy risk levels affect consumers' reliance on low-effort processing. Also, this thesis only examines how consumers perceive their privacy risk to be affected by a DSC between firms. However, benefits such as improved personalization or time-savings could also be affected by a DSC. Future research on the impact of a DSC could distinguish between offered benefits that can be affected by a DSC between firms in the eyes of consumers and offered benefits that are unlikely to be affected by such a DSC. Future research in this field may even help to better understand differences for effects of low-effort processing on benefit and privacy risk perceptions as observable in essay 2 and 5.

**Conclusion.** In conclusion, this thesis examines and provides initial explanations for peculiarities of DSC disclosure settings such as an unexpected privacy risk perception as well as a stronger reliance on low-effort processing in DSC disclosure settings compared to dyadic settings. Besides, this thesis indicates that the benefits and risks associated with a data disclosure are affected differently by low-effort processing. Furthermore, this thesis focuses on the cost side of a data disclosure and increases the understanding of the concepts privacy concerns and privacy risks as well as their disclosure willingness reducing effects. This thesis also emphasizes the need for more research in the context of data disclosures regarding low-effort processing in DSC disclosure settings to understand the mechanisms in detail. It displays that the privacy research field offers many unexplored peculiarities in DSC settings that are just waiting to be examined: for instance, there could be unique effects resulting from different value contributions of firms to their DSC, or from different firm orders, or from different anchors.

## References

- Acquisti, A. and J. Grossklags. (2005). "Privacy and rationality in individual decision making." *IEEE Security Privacy*, 3(1), 26–33.
- Aguinis, H., J. C. Beaty, R. J. Boik and C. A. Pierce. (2005). "Effect Size and Power in Assessing Moderating Effects of Categorical Variables Using Multiple Regression: A 30-Year Review." *Journal of Applied Psychology*, 90(1), 94–107.
- Aivazpour, Z. and V. S. (Chino) Rao. (2020). "Information Disclosure and Privacy Paradox: The Role of Impulsivity." *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 51(1), 14–36.
- Ajzen, I. and M. Fishbein. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs.
- Al-Natour, S., H. Cavusoglu, I. Benbasat and U. Aleem. (2020). "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps." *Information Systems Research*, 31(4), 1037–1063.
- Anderson, C., R. L. Baskerville and M. Kaul. (2017). "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information." *Journal of Management Information Systems*, 34(4), 1082–1112.
- Andrade, E. B. (2005). "Behavioral Consequences of Affect: Combining Evaluative and Regulatory Mechanisms." *Journal of Consumer Research*, 32(3), 355–362.
- Angst, C. M. and R. Agarwal. (2009). "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion." *MIS Quarterly*, 33(2), 339–370.
- Ariely, D. and G. Loewenstein. (2006). "The heat of the moment: the effect of sexual arousal on sexual decision making." *Journal of Behavioral Decision Making*, 19(2), 87–98.
- Augsburger Allgemeine. (2019). "Beachvolleyball-WM 2019: Finale, Teams, Duelle live im TV und Stream." URL: <https://www.augsburger-allgemeine.de/sport/Beachvolleyball-WM-2019-Finale-Teams-Duelle-live-im-TV-und-Stream-id54711401.html> (accessed on 11/29/2019)
- Awad, N. F. and M. S. Krishnan. (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.
- Balduzzi, S., G. Rücker and G. Schwarzer. (2019). "How to perform a meta-analysis with R: a practical tutorial." *Evidence Based Mental Health*, 22(4), 153–160.
- Bandara, R., M. Fernando and S. Akter. (2020). "Explicating the privacy paradox: A qualitative inquiry of online shopping consumers." *Journal of Retailing and Consumer Services*, 52, 101947.
- Bansal, G., F. "Mariam" Zahedi and D. Gefen. (2010). "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online." *Decision Support Systems*, 49(2), 138–150.
- Beach Majors GmbH. (2019). "Beachstream." URL: [https://de.beachmajorseries.com/en/users/beach\\_stream](https://de.beachmajorseries.com/en/users/beach_stream) (accessed on 07/05/2019)
- Bornschein, R., L. Schmidt and E. Maier. (2020). "The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices." *Journal of Public Policy & Marketing*, 39(2), 135–154.
- Brakemeier, H., A. Wagner and P. Buxmann. (2017). "When Risk Perceptions Are Nothing but Guesses – An Evaluability Perspective on Privacy Risks." In: *Proceedings of the 38th International Conference on Information Systems*. Seoul.
- Brandt, M. (2020). "Facebook hat den größten Datenhunger." URL: <https://de-statista-com.docweb.rz.uni-passau.de:2443/infografik/23501/anteil-der-durch-apps-getrackten-persoelichen-daten/> (accessed on 04/12/2021)
- Buchanan, T., C. Paine, A. N. Joinson and U.-D. Reips. (2007). "Development of measures of online privacy concern and protection for use on the Internet." *Journal of the American Society for Information Science and Technology*, 58(2), 157–165.

- Chellappa, R. K. and R. G. Sin. (2005). "Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology & Management. Information & Management*, 705–719.
- Ciarrochi, J., P. Caputi and J. D. Mayer. (2003). "The distinctiveness and utility of a measure of trait emotional awareness." *Personality and Individual Differences*, 34(8), 1477–1490.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, N.J: L. Erlbaum Associates.
- Coker, B. and A. L. McGill. (2020). "Arousal increases self-disclosure." *Journal of Experimental Social Psychology*, 87.
- Cranor, L. F., Reagle, Joseph, and Ackerman, M. S. (1999). "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy." *AT&T Labs Research Technical Report TR 99.4.3*.
- Davazdahemami, B., B. Hammer, A. Luse and P. Kalgotra. (2018). "The Role of Parallelism in Resolving the Privacy Paradox of Information Disclosure in Social Networks." In: *Proceedings of the 39th International Conference on Information Systems*. San Francisco.
- Daw, N. D., Y. Niv and P. Dayan. (2005). "Uncertainty-based competition between prefrontal and dorsolateral striatal systems for behavioral control." *Nature Neuroscience*, 8(12), 1704–1711.
- Del Re, A. C. (2015). "A Practical Tutorial on Conducting Meta-Analysis in R." *The Quantitative Methods for Psychology*, 11(1), 37–50.
- Del Re, A. C. (2020). compute.es: Compute Effect Sizes. URL: <https://cran.r-project.org/web/packages/compute.es/compute.es.pdf>
- Del Re, A. C. and W. T. Hoyt. (2018). "MAde: Meta-Analysis with Mean Differences." URL: <https://CRAN.R-project.org/package=MAde> (accessed on 05/12/2021)
- Diedenhofen, B. (2016). "Package "cocor."" URL: <https://cran.uni-muenster.de/web/packages/cocor/cocor.pdf> (accessed on 11/18/2020)
- Dimitrov, I. (2021). "Invasive apps." URL: <https://blog.pcloud.com/invasive-apps/> (accessed on 07/08/2021)
- Dinev, T., M. Bellotto, P. Hart, V. Russo and I. Serra. (2006). "Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States." *Journal of Global Information Management (JGIM)*, 14(4), 57–93.
- Dinev, T. and P. Hart. (2004). "Internet privacy concerns and their antecedents - measurement validity and a regression model." *Behaviour & Information Technology*, 23(6), 413–422.
- Dinev, T., A. R. McConnell and H. J. Smith. (2015). "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box." *Information Systems Research*, 26(4), 639–655.
- Dinev, T., H. Xu, J. H. Smith and P. Hart. (2013). "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts." *European Journal of Information Systems*, 22(3), 295–316.
- Ditto, P. H., D. A. Pizarro, E. B. Epstein, J. A. Jacobson and T. K. MacDonald. (2006). "Visceral influences on risk-taking behavior." *Journal of Behavioral Decision Making*, 19(2), 99–113.
- Dunn, J. R. and M. E. Schweitzer. (2005). "Feeling and Believing: The Influence of Emotion on Trust." *Journal of Personality and Social Psychology*, 88(5), 736–748.
- Epstein, S. (1994). "Integration of the Cognitive and the Psychodynamic Unconscious." *American Psychologist*, 49(8), 709–724.
- European Commission. (2016). "Special Eurobarometer 447 - Online platforms." URL: <https://www-statista-com.docweb.rz.uni-passau.de:2443/statistics/602885/distribution-of-concerns-over-online-data-collection-in-the-european-union/> (accessed on 04/13/2021)
- European Commission. (2021a). "Can data received from a third party be used for marketing?" URL: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/can-data-received-third-party-be-used-marketing\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/can-data-received-third-party-be-used-marketing_en) (accessed on 07/13/2021)
- European Commission. (2021b). "When can personal data be processed?" URL: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and->

- organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed\_en (accessed on 07/13/2021)
- European Union. (2016) “General Data Protection Regulation (GDPR),” Official Journal of the European Union. Regulation (EU) 2016/679
- Evans, J. S. B. and K. E. Stanovich. (2013). “Dual-Process Theories of Higher Cognition: Advancing the Debate.” *Perspectives on Psychological Science*, 8(3), 223–241.
- Finucane, M. L., A. Alhakami, P. Slovic and S. M. Johnson. (2000). “The Affect Heuristic in Judgments of Risks and Benefits.” *Journal of Behavioral Decision Making*, 13(1), 1–17.
- Garbarino, E. C. and J. A. Edell. (1997). “Cognitive Effort, Affect, and Choice.” *Journal of Consumer Research*, 24(2), 147–158.
- Gartner. (2018). “Gartner Says Data and Analytics Risks Are Audit Executives’ Prime Concerns for 2019.” URL: <https://www.gartner.com/en/newsroom/press-releases/2018-10-25-gartner-says-data-and-analytics-risks-are-audit-executives-prime-concerns-for-2019> (accessed on 11/29/2019)
- Gartner. (2019). “How to Balance Personalization With Data Privacy.” URL: <https://www.gartner.com/smarterwithgartner/how-to-balance-personalization-with-data-privacy/> (accessed on 11/29/2019)
- Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2019). “Cyberisiken bei Ärzten und Apotheken.” URL: <https://de-statista-com.docweb.rz.uni-passau.de:2443/statistik/daten/studie/1065657/umfrage/weitergabe-von-nutzerdaten-von-apotheken-klinik-websites-an-dritte/> (accessed on 04/15/2021)
- Gefen, D., E. Karahanna and D. W. Straub. (2003). “Inexperience and experience with online stores: The importance of tam and trust.” *IEEE Transactions on Engineering Management*, 50(3), 307–321.
- Gerber, N., P. Gerber and M. Volkamer. (2018). “Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior.” *Computers & Security*, 77, 226–261.
- gfs-zürich. (2019). “Sicherheit im Internet.” URL: <https://de-statista-com.docweb.rz.uni-passau.de:2443/statistik/daten/studie/992380/umfrage/umfrage-zu-befuerchtungen-beim-umgang-mit-dem-internet-in-der-schweiz/> (accessed on 04/13/2021)
- Gindin, S. E. (2009). “Nobody Reads Your Privacy Policy or Online Contract: Lessons Learned and Questions Raised by the FTC’s Action against Sears.” *Northwestern Journal of Technology and Intellectual Property*, 8(1), 1–37.
- Gläscher, J., N. Daw, P. Dayan and J. P. O’Doherty. (2010). “States versus Rewards: Dissociable Neural Prediction Error Signals Underlying Model-Based and Model-Free Reinforcement Learning.” *Neuron*, 66(4), 585–595.
- Gregor, S. (2006). “The Nature of Theory in Information Systems.” *MIS Quarterly*, 30(3), 611.
- Hair, J. F., G. T. M. Hult, C. Ringle and M. Sarstedt. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications.
- Hair Jr, J. F., L. M. Matthews, R. L. Matthews and M. Sarstedt. (2017). “PLS-SEM or CB-SEM: updated guidelines on which method to use.” *International Journal of Multivariate Data Analysis*, 1(2), 107–123.
- Hamel, G., Y. L. Doz and C. K. Prahalad. (1989). “Collaborate with Your Competitors and Win.” *Harvard Business Review*.
- Hanafizadeh, P. and M. R. Harati Nik. (2020). “Configuration of Data Monetization: A Review of Literature with Thematic Analysis.” *Global Journal of Flexible Systems Management*, 21(1), 17–34.
- Hong, W. and J. Y. L. Thong. (2013). “Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies.” *MIS Quarterly*, 37(1), 275–298.
- Howard, D. J. and C. Gengler. (2001). “Emotional Contagion Effects on Product Attitudes.” *Journal of Consumer Research*, 28, 189–201.
- Internet World Business. (2018). “Ist Personalisierung, also die Anpassung Ihrer Website oder Ihrer Online-Werbung an die individuellen Vorlieben der Kunden, für Sie ein Thema?” URL: <https://de-statista-com.docweb.rz.uni->

- passau.de:2443/statistik/daten/studie/921812/umfrage/interesse-an-personalisierungsstrategien-im-e-commerce-in-deutschland/ (accessed on 04/12/2021)
- Jallais, C. and A.-L. Gilet. (2010). "Inducing changes in arousal and valence: Comparison of two mood induction procedures." *Behavior Research Methods*, 42(1), 318–325.
- Jobs, S. (2010). "Steve Jobs warned about privacy issues in 2010 at a Wall Street Journal conference" [CNN Money] URL: <https://cnnvfox.com/cnn/cnn-apple-co-founder-steve-jobs-warned-about-privacy-issues-in-tech-at-a-conference-in-2010-facebooks-mark-zuckerberg-was-in-the-audience-https-t-co-fosm5kxpvx-https-t-co-plcdauvkgo/>. (accessed on 07/07/2021)
- Junco, R. (2013). "Comparing actual and self-reported measures of Facebook use." *Computers in Human Behavior*, 29(3), 626–631.
- Kahneman, D. (2012). *Thinking, fast and slow*. Penguin Books.
- Kahneman, D. and A. Tversky. (1979). "Prospect Theory: An Analysis of Decision under Risk." *Econometrica*, 47(2), 263–291.
- Kehr, F., T. Kowatsch, D. Wentzel and E. Fleisch. (2015). "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus." *Information Systems Journal*, 25(6), 607–635.
- Keith, M. J., J. S. Babb, P. B. Lowry, C. P. Furner and A. Abdullat. (2015). "The role of mobile-computing self-efficacy in consumer information disclosure." *Information Systems Journal*, 25(6), 637–667.
- Keith, Thompson and Greer. (2012). "Examining the Rationality of Information Disclosure through Mobile Devices." Presented at the Thirty Third International Conference on Information Systems, Orlando.
- Kenny, D. A. (2015). "Moderator Variables." URL: <http://davidakenny.net/cm/moderation.htm> (accessed on 05/31/2021)
- Kim, D. J., D. L. Ferrin and H. R. Rao. (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), 544–564.
- Kim, M.-S. and J.-H. Ahn. (2007). "Management of Trust in the E-Marketplace: The Role of the Buyer's Experience in Building Trust." *Journal of Information Technology*, 22(2), 119–132.
- Kim, Y., K. Park, Y. Kim, W. Yang, D. Han and W.-S. Kim. (2020). "The Impact of Visual Art and High Affective Arousal on Heuristic Decision-Making in Consumers." *Frontiers in Psychology*, 11, Article 565829.
- Kokolakis, S. (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon." *Computers & Security*, 64, 122–134.
- Kool, W., J. T. McGuire, Z. B. Rosen and M. M. Botvinick. (2010). "Decision Making and the Avoidance of Cognitive Demand." *Journal of Experimental Psychology. General*, 139(4), 665–682.
- Kordzadeh, N., J. Warren and A. Seifi. (2016). "Antecedents of privacy calculus components in virtual health communities." *International Journal of Information Management*, 36(5), 724–734.
- Latzer, M., M. Büchi and N. Festic. (2019). *Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2019*. Universität Zürich. URL: <https://de-statista-com.docweb.rz.uni-passau.de:2443/statistik/daten/studie/307584/umfrage/privatsphaere-im-internet-in-der-schweiz/> (accessed on 08/13/2021)
- Lei, D. and J. W. Slocum Jr. (1992). "Global Strategy, Competence-Building and Strategic Alliances." *California Management Review*, 35(1), 81–97.
- Li, H., A. Gupta, J. Zhang and R. Sarathy. (2014). "Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract." *Decision Support Systems*, 57, 376–386.
- Li, H., X. (Robert) Luo, J. Zhang and H. Xu. (2017). "Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors." *Information & Management*.
- Li, H., R. Sarathy and H. Xu. (2011). "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors." *Decision Support Systems*, 51(3), 434–445.

- Li, Y. (2012). "Theories in online information privacy research: A critical review and an integrated framework." *Decision Support Systems*, 54(1), 471–481.
- LINK Institut und SRG SSR. (2018). "Dataland." URL: <https://de-statista-com.docweb.rz.uni-passau.de:2443/statistik/daten/studie/977771/umfrage/umfrage-zum-lesen-der-agbs-von-apps-in-der-schweiz/> (accessed on 04/13/2021)
- LiveRamp. (2021). "Collaborative Data Solutions: Data and Identity in the Era of Permission." URL: <https://www-statista-com.docweb.rz.uni-passau.de:2443/statistics/1206477/popularity-first-party-data-sharing-usa/> (accessed on 04/09/2021)
- Loewenstein, G. F., E. U. Weber, C. K. Hsee and N. Welch. (2001). "Risk as feelings." *Psychological Bulletin*, 127(2), 267–286.
- Loftus, G. R. (1978). "On interpretation of interactions." *Memory & Cognition*, 6(3), 312–319.
- Maglio, S. J. and T. Reich. (2019). "Feeling certain: Gut choice, the true self, and attitude certainty." *Emotion*, 19(5), 876–888.
- Malhotra, N. K., S. S. Kim and J. Agarwal. (2004). "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research*, 15(4), 336–355.
- Markus, H. (1977). "Self-schemata and processing information about the self." *Journal of Personality and Social Psychology*, 35(2), 63–78.
- Martin, M. (1990). "On the induction of mood." *Clinical Psychology Review*, 10(6), 669–697.
- Mason, J. C. (1993). "Strategic alliances: Partnering for Success." *Management Review*, 82(5).
- Meuser, M. and U. Nagel. (1989). *Experteninterviews - vielfach erprobt, wenig bedacht: Ein Beitrag zur qualitativen Methodendiskussion*.
- Millard, S. P. (2013). *EnvStats: An R package for environmental statistics*. New York: Springer.
- Milne, G. R., G. Pettinico, F. M. Hajjat and E. Markos. (2017). "Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing." *Journal of Consumer Affairs*, 51(1), 133–161.
- Miltgen, C. L. and D. Peyrat-Guillard. (2014). "Cultural and generational influences on privacy concerns: a qualitative study in seven European countries." *European Journal of Information Systems*, 23(2), 103–125.
- Miltgen, C. L. and H. J. Smith. (2015). "Exploring information privacy regulation, risks, trust, and behavior." *Information & Management*, 52(6), 741–759.
- Mothersbaugh, D. L., W. K. Foxx, S. E. Beatty and S. Wang. (2012). "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information." *Journal of Service Research*, 15(1), 76–98.
- Myers, M. D. and M. Newman. (2007). "The qualitative interview in IS research: Examining the craft." *Information and Organization*, 17(1), 2–26.
- Netzer, F. (1999). *Strategische Allianzen im Luftverkehr*. Peter Lang International Academic Publishers.
- Norberg, P. A., D. R. Horne and D. A. Horne. (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs*, 41(1), 100–126.
- Österreichische Marketing Gesellschaft and Marketagent. (2019). "Digital Trend Report 2019." URL: <https://de-statista-com.docweb.rz.uni-passau.de:2443/statistik/daten/studie/435852/umfrage/innovationspotenzial-von-marketing-trends-laut-werbungtreibenden-in-oesterreich/> (accessed on 04/12/2021)
- OnAudience. (2020). "Size of the marketing related data market worldwide from 2017 to 2021." URL: <https://www.statista.com/statistics/818754/global-marketing-data-market-size/> (accessed on 04/12/2021)
- Osberg, T. M. and J. S. Shrauger. (1986). "Self-prediction: Exploring the parameters of accuracy." *Journal of Personality and Social Psychology*, 51(5), 1044–1057.
- Ovide, S. (2020). "Just Collect Less Data, Period." *The New York Times*. URL: <https://www.nytimes.com/2020/07/15/technology/just-collect-less-data-period.html> (accessed on 07/15/2021)

- Ozturk, A. B., K. Nusair, F. Okumus and D. Singh. (2017). "Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework." *Information Systems Frontiers*, 19(4), 753–767.
- Pavlou, P. A. (2011). "State of the Information Privacy Literature: Where are We Now and Where Should We Go?" *MIS Quarterly*, 35(4), 977–988.
- Pavlou, P. A. and D. Gefen. (2004). "Building Effective Online Marketplaces with Institution-Based Trust." *Information Systems Research*, 15(1), 37–59.
- Paypal. (2018). "Paypal's Third-Party List." URL: <https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list> (accessed on 07/09/2018)
- Peter, J. P. and L. X. Tarpey. (1975). "A Comparative Analysis of Three Consumer Decision Strategies." *Journal of Consumer Research*, 2(1), 29–37.
- Pew Research Center. (2019). "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." URL: <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> (accessed on 04/12/2021)
- Pezzulo, G., F. Rigoli and F. Chersi. (2013). "The Mixed Instrumental Controller: Using Value of Information to Combine Habitual Choice and Mental Simulation." *Frontiers in Psychology*, 4, Article 92.
- Quintana, D. S. (2015). "From pre-registration to publication: a non-technical primer for conducting a meta-analysis to synthesize correlational data." *Frontiers in Psychology*, 6.
- Revelle, W. (2021). "Procedures for Psychological, Psychometric, and Personality Research [R package psych version 2.1.3]." URL: <https://CRAN.R-project.org/package=psych> (accessed on 05/12/2021)
- Risius, M., A. Baumann and H. Krasnova. (2020). "Developing a New Paradigm: Introducing the Intention-Behaviour Gap to the Privacy Paradox Phenomenon." In: *Proceedings of the 28th European Conference on Information Systems*. Online.
- Rönkkö, M. and J. Evermann. (2013). "A Critical Examination of Common Beliefs About Partial Least Squares Path Modeling." *Organizational Research Methods*, 16(3), 425–448.
- Russell, J. A. (2003). "Core affect and the psychological construction of emotion." *Psychological Review*, 110(1), 145–172.
- Russell, J. A. (2009). "Emotion, core affect, and psychological construction." *Cognition & Emotion*, 23(7), 1259–1283.
- Rust, R. T. and M.-H. Huang. (2014). "The Service Revolution and the Transformation of Marketing Science." *Marketing Science*, 33(2), 206–221.
- Samad, F. G., Pierre Péladeau, and Rawia Abdel. (2019). "Tomorrow's data heroes." URL: <https://www.strategy-business.com/article/Tomorrows-Data-Heroes> (accessed on 07/06/2021)
- Schaub, F., R. Balebako, A. L. Durity and L. F. Cranor. (2015). "A Design Space for Effective Privacy Notices\*." In: E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (1st ed., pp. 365–393). Cambridge University Press.
- Scherer, K. R. (2005). "What are emotions? And how can they be measured?" *Social Science Information*, 44(4), 695–729.
- Schumann, J. H., F. von Wangenheim and N. Groene. (2014). "Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance among Users of Free Web Services." *Journal of Marketing*, 78(1), 59–75.
- Schwarz, N. and G. L. Clore. (1983). "Mood, misattribution, and judgments of well-being: Informative and directive functions of affective states." *Journal of Personality and Social Psychology*, 45(3), 513–523.
- Schwarz, N. and G. L. Clore. (2003). "Mood as Information: 20 Years Later." *Psychological Inquiry*, 14(3–4), 296–303.
- Sheeran, P. and S. Orbell. (2000). "Self-schemas and the theory of planned behaviour." *European Journal of Social Psychology*, 30(4), 533–550.
- Slovic, P., M. L. Finucane, E. Peters and D. G. MacGregor. (2004). "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality." *Risk Analysis*, 24(2), 311–322.

- Slovic, P., M. L. Finucane, E. Peters and D. G. MacGregor. (2007). "The affect heuristic." *European Journal of Operational Research*, 177(3), 1333–1352.
- Slovic, P., M. Finucane, E. Peters and D. G. MacGregor. (2002). "Rational actors or rational fools: implications of the affect heuristic for behavioral economics." *The Journal of Socio-Economics*, 31(4), 329–342.
- Smith, H. J., T. Dinev and H. Xu. (2011). "Information privacy research: an interdisciplinary review." *MIS Quarterly*, 35(4), 989–1016.
- Smith, H. J., S. J. Milberg and S. J. Burke. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly*, 20(2), 167–196.
- Specht-Riemenschneider, P. D. L., N. Werry, S. Werry, D. S. Apel, D. jur M. Beyer-Katzenberger, M. Bidler, ... P. D. L. Yu. (2019). *Datenrecht in der Digitalisierung* (1st ed.). Erich Schmidt Verlag GmbH & Co.
- Stanovich and West. (2000). "Behavioral and Brain Sciences 23:5," 23(5), 645–665.
- Svenson, O. and A. J. Maule. (1993). *Time Pressure and Stress in Human Judgment and Decision Making*. Springer Science & Business Media.
- Taddicken, M. (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), 248–273.
- The Sunday Times. (2018). "A day in the life of your data: here's how much information you give away." URL: <https://www.thetimes.co.uk/static/connected-families/how-much-data-are-you-sharing-in-a-typical-day/> (accessed on 07/06/2021)
- Tingley, D., T. Yamamoto, K. Hirose, L. Keele and K. Imai. (2014). "mediation: R Package for Causal Mediation Analysis." *Journal of Statistical Software*, 59(5).
- Tranfield, D., D. Denyer and P. Smart. (2003). "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review." *British Journal of Management*, 14(3), 207–222.
- Tsai, J. Y., S. Egelman, L. Cranor and A. Acquisti. (2011). "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research*, 22(2), 254–268.
- Tuunainen, V. K., O. Pitkänen and M. Hovi. (2009). "Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook." In: *BLED 2009 Proceedings* (Vol. 42). Bled, Slovenia.
- Tversky, A. and D. Kahneman. (1974). "Judgment under Uncertainty: Heuristics and Biases." *Science*, 185(4157), 1124–1131.
- Tversky, A. and D. Kahneman. (1992). "Advances in prospect theory: Cumulative representation of uncertainty." *Journal of Risk and Uncertainty*, 5(4), 297–323.
- Vaidhyanathan, S. (2018). "Violating our privacy is in Facebook's DNA." *The Guardian*. URL: <https://www.theguardian.com/commentisfree/2018/dec/20/facebook-violating-privacy-mark-zuckerberg> (accessed on 07/31/2019)
- van den Braak, S. W., S. Choenni, R. Meijer and A. Zuiderwijk. (2012). "Trusted third parties for secure and privacy-preserving data integration and sharing in the public sector." In: *Proceedings of the 13th Annual International Conference on Digital Government Research* (pp. 135–144). College Park, Maryland.
- Viechtbauer, W. (2020). "Meta-Analysis Package for R [R package metafor version 2.4-0]." URL: <https://CRAN.R-project.org/package=metafor> (accessed on 03/19/2020)
- Wakefield, R. (2013). "The influence of user affect in online information disclosure." *The Journal of Strategic Information Systems*, 22(2), 157–174.
- Wang, Y., G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon and L. F. Cranor. (2011). "'I regretted the minute I pressed share": a qualitative study of regrets on Facebook." In: *Proceedings of the seventh symposium on usable privacy and security* (pp. 1–16). Pittsburgh.
- Webster, J. and R. T. Watson. (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review." *MIS Quarterly*, 26(2), xiii–xxiii.



- Wharton School. (2019). "Your Data Is Shared and Sold...What's Being Done About It?" URL: <https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/> (accessed on 07/13/2021)
- Williams, R. (2015). "Interpreting Interaction Effects; Interaction Effects and Centering."
- Xie, W. and C. Kang. (2015). "See you, see me: Teenagers' self-disclosure and regret of posting on social network site." *Computers in Human Behavior*, (52), 398–407.
- Xu, H., X. (Robert) Luo, J. M. Carroll and M. B. Rosson. (2011). "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing." *Decision Support Systems*, 51(1), 42–52.
- Zafeiropoulou, A. M., D. E. Millard, C. Webber and K. O'Hara. (2013). "Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?" In: *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 463–472). Paris.
- Zhang, P. (2013). "The Affective Response Model: A Theoretical Framework of Affective Concepts and Their Relationships in the ICT Context." *MIS Quarterly*, 37(1), 247–274.

# **An Exploratory Study of Risk Perception for Data Disclosure to a Network of Firms**

**Authors:** Tobias Steudner, University of Passau, Germany  
Thomas Widjaja, University of Passau, Germany  
Jan H. Schumann, University of Passau, Germany

**Presented at:** Information Systems Brown-Bag Seminar, 2018, Passau Germany  
14th International Conference on Wirtschaftsinformatik, 2019, Siegen, Germany

**Published in:** Proceedings of the 14<sup>th</sup> International Conference on Wirtschaftsinformatik, 2019

## **Abstract**

Research on the Privacy Calculus, which explains individuals' intention to disclose personal data, mostly focuses on dyadic disclosures in which individuals disclose data to a single firm. So far, little attention has been paid to understand the characteristics of data disclosures to a network of firms. We refer to data sharing of firms in a network as "Business Network Data Exchange" (BNDE). We explore risk perception for data disclosures in a BNDE context based on an exploratory survey. Our results indicate that risk perception for data disclosures in the BNDE context deviates from rational risk perception theory. In particular, individuals perceive the risk to disclose data to a network of two firms as lower than the maximum risk of the separate dyadic data disclosures. These results portend the need for an adapted and nuanced view on perceived risks in this context and have important practical implications for data-sharing among firms.

## **An Exploratory Study of Risk Perception for Data Disclosure to a Network of Firms**

Tobias Steudner<sup>1</sup>, Thomas Widjaja<sup>1</sup> and Jan H. Schumann<sup>2</sup>

<sup>1</sup> University of Passau, Chair of Business Information Systems, Passau, Germany  
{tobias.steudner,thomas.widjaja}@uni-passau.de

<sup>2</sup> University of Passau, Chair of Marketing and Innovation, Passau, Germany  
jan.schumann@uni-passau.de

**Abstract.** Research on the Privacy Calculus, which explains individuals' intention to disclose personal data, mostly focuses on dyadic disclosures in which individuals disclose data to a single firm. So far, little attention has been paid to understand the characteristics of data disclosures to a network of firms. We refer to data sharing of firms in a network as "Business Network Data Exchange" (BNDE). We explore risk perception for data disclosures in a BNDE context based on an exploratory survey. Our results indicate that risk perception for data disclosures in the BNDE context deviates from rational risk perception theory. In particular, individuals perceive the risk to disclose data to a network of two firms as lower than the maximum risk of the separate dyadic data disclosures. These results portend the need for an adapted and nuanced view on perceived risks in this context and have important practical implications for data-sharing among firms.

**Keywords:** Privacy Calculus, Risk Perception, Business Network Data Exchange

### **1 Introduction**

Most research in the privacy context focuses on situations in which individuals disclose data only to a single firm (e.g., [1]). However, recently more and more firms started to depart from this dyadic consumer-firm relationship and began to share consumer data within a network of firms [2, 3]. In accordance with Bidler et al., we will refer to such procedures as Business Network Data Exchange (BNDE) [4]. An example for BNDE is the music streaming service Spotify: Consumers' data is shared among a network of artists, record labels, and further third parties [5]. Potential differences between dyadic data disclosures and data disclosures in the BNDE context have rarely been examined in the literature. One difference could be the complexity or non-transparency of BNDE situations, which could promote irrational behavior [4, 6–8]. However, the Privacy Calculus, as the dominant theory to explain individuals' intention to disclose personal data by weighing their benefits against their risks, assumes rational behavior [3, 9–11]. As perceived privacy risks are the main factor reducing individuals' intention to disclose in the Privacy Calculus [11–13], we will focus on perceived risks as a key factor in this first approach. We argue that in BNDE data disclosures individuals' risk perception

14<sup>th</sup> International Conference on Wirtschaftsinformatik,  
February 24-27, 2019, Siegen, Germany

differ from dyadic data disclosures. As a starting point for future research in the BNDE context, we first focus on the question: *Is individuals' risk perception of a data disclosure to a BNDE firm network consisting of two firms higher or lower than the dyadic data disclosure to a single firm?*

## 2 Theoretical Background on Risks

Privacy risk comprises "the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm" [3]. In traditional risk perception theory a rational evaluation is expected as the perceived risk of an outcome is defined as the probability of a certain unfavorable outcome multiplied by the severity of the respective outcome [14–16]. If a risk is constituted by different risk components they are often assumed to be additive [17]. The assumption of rational evaluation as well as the additivity of risks was challenged by the Prospect Theory [18, 19]. According to the Prospect Theory individuals transform benefits and risks into a simpler mental representation and use a function to assign a subjective value (perceived benefits and perceived risk) to them. For this value function, monotony as well as a diminishing marginal value is assumed [18, 19]. Since the main emphasis of our paper is on risks, this means particularly that each added potential loss should increase the perceived risk (monotony), but this effect diminishes the more potential losses already exist (diminishing marginal value). In this short paper we focus on the simplest possible BNDE network consisting of just two firms (see Table 1). According to traditional risk theory as well as Prospect Theory, we expect the risk of a data disclosure to a BNDE network with two firms should be perceived higher than the risk of each of the dyadic data disclosures due to the monotony assumption. The risk increase should be caused by the additional (second) firm which obtains the individuals' data. This leads to our proposition 1a.

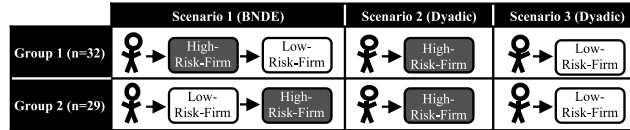
On the other hand, mutual control in cooperations plays a major role for firms [20, 21], thus it is possible that individuals' perceived or assumed control distribution among the firms in the network could alter individuals' risk perception as well. Furthermore, cooperations among firms offer several benefits for consumers and firms. For instance, firms can complement each other [22, 23], e.g., with technical security know-how. Additionally, firms can improve their own internal processes due to knowledge transfer in a cooperation [22, 24–26], which could reduce individuals' perceived risk for BNDE data disclosures, e.g., through better standards of conduct. Both was also described by some participants in pre-test interviews. This leads to our proposition 1b.

**Proposition 1a / 1b:** *The perceived risk for the BNDE data disclosure is perceived higher (Proposition 1a) / lower (Proposition 1b) than the maximum perceived risk of the two respective dyadic data disclosures.*

## 3 Exploratory Survey

The survey data (61 subjects, 33 male) was collected from end of November 2017 until mid of December 2017 in cooperation with a panel provider. The subjects were over 18 years, live in Germany, and the age distribution of them reflects the age distribution of German Internet users. The within-subject designed survey contained two groups with three scenarios each and a fixed scenario order (see Table 1).

Table 1. Empirical Setup



The first scenario was a BNDE data disclosure scenario with two existent firms: The subjects saw a screenshot of the respective firm's website and were asked to disclose some personal data (name, address, net-household income, expenses per week, supermarkets they regularly visit, number of persons in the household, phone number). In group 1 (n=32) the subjects disclosed their data to the High-Risk-Firm, which shares the exact same data subsequently not anonymized with the Low-Risk-Firm<sup>1</sup>. This data sharing procedure between the two firms was described in the scenario. In group 2 (n=29) the data was disclosed to the Low-Risk-Firm and then shared with the High-Risk-Firm. In both groups, both firms obtain the same data. The benefit in all three scenarios was identical (20 Euro coupon which could be redeemed in both firms). Two groups were used to control for firm order effects.

After reading the respective scenarios the subjects had to assess their perceived privacy risk (PR) on a seven-point Likert Scale with one being "strongly disagree" and 7 being "strongly agree" based on a scale of Dinev et al. [27] (PR1: It is very risky in this situation to disclose personal information. PR2: There would be high potential for privacy loss associated with data disclosure in this situation. PR3: Personal information could be inappropriately used in this situation. PR4: Providing personal information in this situation would involve many unexpected problems; The average of the items was used as perceived risk). For the High-Risk-Firm a well-known search engine firm and for the Low-Risk-Firm a well-known grocery store were selected. Existing firms were used to make the whole scenario easier to imagine and comprehend. After assessing the risk for the BNDE disclosure (scenario 1) the subjects had to imagine and assess their privacy risk for the two respective dyadic data disclosures without any data sharing to further firms (i.e., scenario 2: disclosure only to the High-Risk-Firm and scenario 3: disclosure only to the Low-Risk-Firm). These two dyadic scenarios were the same in both groups.

#### 4 Results, Discussion, and Outlook

As expected, the risk for the dyadic scenario 2 ( $PR_{High-Risk-Firm}$ ) is perceived in both groups significantly higher than the risk for the dyadic scenario 3 ( $PR_{Low-Risk-Firm}$ ), thus  $PR_{High-Risk-Firm}$  is the maximum perceived risk of the two dyadic data disclosures. We used "R" with "EnvStats" for a one-sided paired randomization test for location [28–32] with 100k iterations to test each group separately as well as both groups together (see Table 2,  $\Delta$  means test statistic).  $PR_{BNDE-DD}$ , the perceived risk for scenario 1, was significantly smaller ( $\Delta = 40$ ,  $p = 0.001$ ) than the maximum perceived risk out of the dyadic data disclosures ( $PR_{High-Risk-Firm}$ ), thus we reject proposition 1a and accept 1b.

<sup>1</sup> We conducted interviews as a pre-test (14 subjects, 11 male, age between 21 and 71) to ensure that the risk level is perceived as different between the two dyadic data disclosures.

**Table 2. Preliminary Results**

Group	Scenario	Mean Perceived Risk (Standard Deviation)			One-Sided Paired Randomization Test for	
		PR <sub>BNDE</sub> Scenario 1	PR <sub>High-Risk-Firm</sub> Scenario 2	PR <sub>Low-Risk-Firm</sub> Scenario 3	PR <sub>Low-Risk-Firm</sub> < PR <sub>High-Risk-Firm</sub>	PR <sub>BNDE</sub> < PR <sub>High-Risk-Firm</sub>
Group 1 (n=32)		4.25 (1.52)	5.11 (1.33)	3.52 (1.44)	$\Delta = 50.75, p = 0.000$	$\Delta = 27.50, p = 0.003$
Group 2 (n=29)		4.90 (1.52)	5.33 (1.33)	4.35 (1.44)	$\Delta = 28.25, p = 0.003$	$\Delta = 12.50, p = 0.074$
Both groups (n=61)		4.56 (1.61)	5.21 (1.52)	3.92 (1.63)	$\Delta = 79.00, p = 0.000$	$\Delta = 40.00, p = 0.001$

Contrary to the monotony assumption of the Prospect Theory, the perceived risk for data disclosures in a BNDE context with two firms is perceived as less risky than the maximum of the two respective dyadic data disclosures. These preliminary results indicate that we observe non-monotony behavior that could be explained by positive cooperation effects which reduce individuals' perceived risk due to individuals' assumption of positive changes in firms' data handling process. Future research could review the monotony assumption of the Prospect Theory in the BNDE context and extend the Privacy Calculus by considering positive cooperation effects. Future research should also investigate whether the changes in individuals' risk perception are an instance of irrational behavior in the context of the Privacy Calculus as suggested by Dinev et al. [9].

Additionally, our preliminary results have important practical implications: When the risk for a BNDE data disclosure is perceived as less risky than one of the separate dyadic disclosures, joint data collections are more effective in total and specifically for firms associated with high risk. Since the perceived risk for BNDE data disclosures is nevertheless expected to be the same or higher than the minimum of the separate dyadic data disclosures, it might be beneficial to investigate redistribution mechanisms among firms to balance their cooperation benefits.

The presented preliminary results should be viewed in the light of their limitations: The sample size is small and the within-design without scenario order randomization could distort the results. Also, our results could hold only for BNDE networks consisting of just two firms. To rule out these possible error sources a new survey with bigger sample size, hypothetical firms, varying network size, and a between-subject design is in work.

In sum, we showed that data disclosures in a BNDE context are an interesting and unexplored field that requires further research. Thus, we aim for a deeper understanding in which BNDE constellations (e.g., firm combinations, network characteristics, etc.) individuals assume positive changes in the data handling process of the network firms and perceive less risk for the BNDE data disclosure. For this, our exploratory study with the focus on risk perception shall serve as a starting point.

## References

1. Li, H., Sarathy, R., Xu, H.: The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decis. Support Syst.* 51, 434–445 (2011).
2. Madsbjerg, S.: It's Time to Tax Companies for Using Our Personal Data, <https://www.nytimes.com/2017/11/14/business/dealbook/taxing-companies-for-using-our-personal-data.html> (Accessed: 24.04.2018).
3. Smith, H.J., Dinev, T., Xu, H.: Information privacy research: an interdisciplinary review. *MIS Q.* 35, 989–1016 (2011).

4. M. Bidler, J. H. Schumann, T. Widjaja: Challenging the Cognitive Privacy Calculus: Affective Reactions in Consumers' Privacy Related Decision Making. Presented at the EMAC Conference. Glasgow, United Kingdom (05. - 01.06.2018).
5. Spotify: Spotify Privacy Policy, <https://www.spotify.com/us/legal/privacy-policy/> (Accessed: 23.04.2018).
6. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. *Science*. 347, 509–514 (2015).
7. Amos Tversky, Daniel Kahneman: Rational Choice and the Framing of Decisions. *J. Bus.* 59, 251–278 (1986).
8. Finucane, M.L., Alhakami, A., Slovic, P., Johnson, S.M.: The Affect Heuristic in Judgments of Risks and Benefits. *J. Behav. Decis. Mak.* 13, 17 (2000).
9. Dinev, T., McConnell, A.R., Smith, H.J.: Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. *Inf. Syst. Res.* 26, 639–655 (2015).
10. Laufer, R.S., Wolfe, M.: Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *J. Soc. Issues*. 33, 22–42 (1977).
11. Li, Y.: Theories in online information privacy research: A critical review and an integrated framework. *Decis. Support Syst.* 54, 471–481 (2012).
12. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* 15, 336–355 (2004).
13. Xu, H., Teo, H.-H., Tan, B.C.Y.: Predicting the adoption of location-based services: The role of trust and perceived privacy risk. In: *ICIS 2005 proceedings*. pp. 897–910 (2005).
14. Bauer, R.A.: Consumer Behavior as Risk Taking. In: *Risk Taking and Information Handling in Consumer Behavior*. pp. 389–398. , Boston: Harvard University (1967).
15. Cunningham, S.: The Major Dimensions of Perceived Risk. In: *Risk Taking and Information Handling in Consumer Behavior*. pp. 82–108. , Boston: Harvard University (1967).
16. Sieber, J.E., Lanzetta, J.T.: Conflict and conceptual structure as determinants of decision-making behavior. *J. Pers.* 32, 622–641 (2006).
17. Peter, J.P., Tarpey, L.X.: A Comparative Analysis of Three Consumer Decision Strategies. *J. Consum. Res.* 2, 29–37 (1975).
18. Tversky, A., Kahneman, D.: Advances in prospect theory: Cumulative representation of uncertainty. *J. Risk Uncertain.* 5, 297–323 (1992).
19. Kahneman, D., Tversky, A.: Prospect Theory: An Analysis of Decision under Risk. *Econometrica*. 47, 263–291 (1979).
20. Killing, J.P.: How to Make a Global Joint Venture Work, <https://hbr.org/1982/05/how-to-make-a-global-joint-venture-work> (Accessed: 24.04.2018).
21. Ahern, R.: The Role of Strategic Alliances in the International Organization of Industry. *Environ. Plan. A*. 25, 1229–1246 (1993).
22. Lei, D., Slocum Jr., J.W.: Global Strategy, Competence-Building and Strategic Alliances. *Calif. Manage. Rev.* 35, 81–97 (1992).
23. Mason, J.C.: Strategic alliances: Partnering for Success. *Manage. Rev.* 82, 10 (1993).
24. Hamel, G., Doz, Y.L., Prahalad, C.K.: Collaborate with Your Competitors and Win. 8 (1989).
25. Doz, Y.L.: Technology Partnerships between Larger and Smaller Firms: Some Critical Issues. *Int. Stud. Manag. Organ.* 17, 31–57 (1987).
26. Prahalad, C.K., Doz, Y.L.: The Multinational Mission: Balancing Local Demands and Global Vision. Simon and Schuster (1999).

27. Dinev, T., Xu, H., Smith, J.H., Hart, P.: Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *Eur. J. Inf. Syst.* 22, 295–316 (2013).
28. Fisher, R.A.: *The Design of Experiments*. Des. Exp. (1935).
29. Smucker, M.D., Allan, J., Carterette, B.: A comparison of statistical significance tests for information retrieval evaluation. In: *Proceedings of the sixteenth ACM Conference on Information and Knowledge Management*. p. 623. ACM Press, Lisbon, Portugal (2007).
30. Efron, B., Tibshirani, R.J.: *An Introduction to the Bootstrap*. CRC Press (1994).
31. Cohen, P.: *Empirical Methods for Artificial Intelligence*. 128 (2006).
32. Millard, S.P.: *EnvStats: An R package for environmental statistics*. Springer, New York (2013).



# **The Effect of Data Sharing Between Firms on Low-Cognitive-Effort Processing – An Integrative Approach**

**Author:** Tobias Steudner, University of Passau, Germany

**Presented at:** Information Systems Brown-Bag Seminar, 2019, Passau Germany  
Doctoral Colloquium of the School of Business, Economics and Information Systems, 2019, Passau, Germany

## **Abstract**

In privacy research mostly dyadic disclosure settings are examined, i.e., individuals disclose their personal data to a single firm that does not share personal data with further firms. However, individuals often disclose their personal data to a network of firms, i.e., to a firm which shares their personal data with other firms. We refer to such a procedure as business network data exchange (BNDE). In previous privacy research mostly a cognitive effortful data decision-making process was assumed for individuals. Nevertheless, individuals can base their decision also on another processing system that is based on different factors, e.g., affect/emotions, and requires less cognitive resources. In this study, we explore how a personal data disclosure to a network of firms (i.e., BNDE setting) compared to a dyadic disclosure impacts individuals decision-making. Therefore, we compare individuals' reliance on the cognitively less effortful processing system between dyadic and BNDE disclosure settings. Based on reinforcement learning knowledge, we predict that individuals in a BNDE disclosure setting rely more strongly on low-cognitive-effort processing for their decision-making process. Due to that, we also assume that these individuals perceive the decision-making process in retrospect as easier and perceive less decision-uncertainty. We draw on two hypothetical data disclosure scenarios and perform structural equation modeling to compare the effect sizes of affect. We find a stronger reliance on low-cognitive-effort processing for BNDE disclosure settings. This study contributes to a refined understanding of individuals' disclosure decision-making process. The results also demonstrate that it could be beneficial for firms and regulators to adapt firm communication to individuals' low-cognitive-effort processing system, especially for BNDE disclosure settings.

# The Effect of Data Sharing Between Firms on Low-Cognitive-Effort Processing – An Integrative Approach

Completed Research Paper

**Tobias Steudner**

University of Passau,  
Chair of Business Information Systems,  
Passau, Germany,  
tobias.steudner@uni-passau.de

## Abstract

*In privacy research mostly dyadic disclosure settings are examined, i.e., individuals disclose their personal data to a single firm that does not share personal data with further firms. However, individuals often disclose their personal data to a network of firms, i.e., to a firm which shares their personal data with other firms. We refer to such a procedure as business network data exchange (BNDE). In previous privacy research mostly a cognitive effortful data decision-making process was assumed for individuals. Nevertheless, individuals can base their decision also on another processing system that is based on different factors, e.g., affect/emotions, and requires less cognitive resources. In this study, we explore how a personal data disclosure to a network of firms (i.e., BNDE setting) compared to a dyadic disclosure impacts individuals decision-making. Therefore, we compare individuals' reliance on the cognitively less effortful processing system between dyadic and BNDE disclosure settings. Based on reinforcement learning knowledge, we predict that individuals in a BNDE disclosure setting rely more strongly on low-cognitive-effort processing for their decision-making process. Due to that, we also assume that these individuals perceive the decision-making process in retrospect as easier and perceive less decision-uncertainty. We draw on two hypothetical data disclosure scenarios and perform structural equation modeling to compare the effect sizes of affect. We find a stronger reliance on low-cognitive-effort processing for BNDE disclosure settings. This study contributes to a refined understanding of individuals' disclosure decision-making process. The results also demonstrate that it could be beneficial for firms and regulators to adapt firm communication to individuals' low-cognitive-effort processing system, especially for BNDE disclosure settings.*

*Keywords: Privacy Concerns, Privacy Risk, Privacy Paradox, Abstraction Levels*

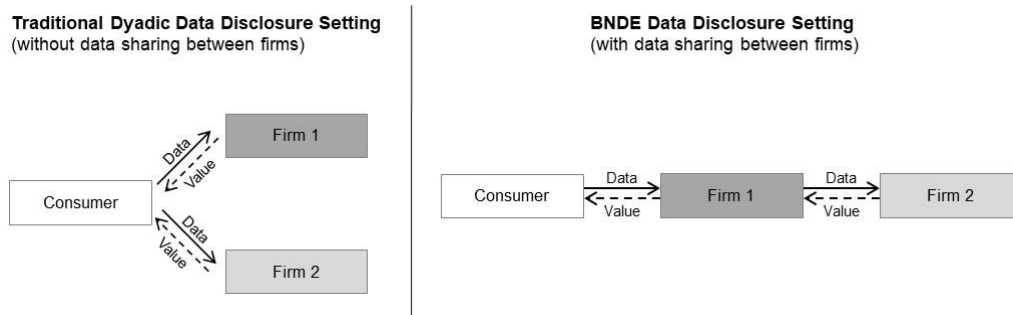
## Introduction

The lion's share of privacy literature examine situations in which individuals disclose their personal data to a single firm (e.g., Li et al. 2011). However, firms started to change this dyadic consumer-firm relationship as they began to share consumers' personal data within a network of firms (Madsbjerg 2017; Smith et al. 2011). We refer to such procedures as business network data exchange (BNDE, cf. Bidler et al. 2018). The music streaming service Spotify is an excellent example of a BNDE: Spotify shares its consumers' data with a network of artists, record labels, and further third parties (Spotify 2018). Despite there are several differences between dyadic and BNDE data disclosure settings, most studies examine only dyadic data disclosures (e.g., Bansal et al. 2010; Li et al. 2011). Even when a possible BNDE setting is examined, unique characteristics like data sharing between firms or the network structure in such BNDE data disclosure settings are mostly ignored or are not the focus of the respective studies (e.g., Angst and Agarwal 2009; Wirtz and Lwin 2009).<sup>1</sup> Especially with new

---

<sup>1</sup> These insights are the result of a structured literature review conducted for a proposal. More information on the structured literature review is available upon request.

regulations that foster more transparency regarding firms' data handling procedures, such as the "General Data Protection Regulation" (GDPR, 2016), BNDE characteristics become more visible to consumers. For example, all data sharing with third-parties must be stated. Such a peculiarity in BNDE data disclosure settings could be that there is a certain touchpoint firm for the consumers (i.e., the first and only firm that is in direct contact with consumers), or there could be a dominant firm in the network that contributes the most to the offered services, or that a firm in the network has a certain well-known reputation, et cetera. The simplest form of a data exchange network consists of only two firms, which have a data sharing cooperation. In this simplest form of a BNDE disclosure setting the consumers disclose their data to the touchpoint firm 1, which subsequently shares the personal consumer data with firm 2 (see Figure 1, right). In an exchange network with several firms, there are even more peculiarities. For instance, it is possible that any firm in the exchange network shares consumer data with further firms or that there is a certain sharing order. Also, the network structure, number of firms and several other aspects can vary in such bigger data exchange networks. Besides, data sharing between firms (i.e., a BNDE setting) can be necessary (or unnecessary) to offer certain services to consumers. A reason for data sharing between firms when this is not done in order to offer services to consumers, is for example, to increase the companies' return by monetizing consumer data (Hanafizadeh and Harati Nik 2020; Wixom 2014). Furthermore, it is possible that firms in the data exchange network complement their information about their consumers and thus, they mutually enrich their consumer data. However, as one of the first studies on characteristics of such a BNDE network, this study focuses on the sole impact of a "data sharing between firms" aspect in its simplest form in a BNDE disclosure setting compared to the identical disclosure setting in form of a dyadic data disclosures (cf. figure 1, left side).



**Figure 1.** Settings for a data disclosure to two firms. Dyadic data disclosure setting, i.e., no data sharing between firms (left) and BNDE data disclosure setting, i.e., data sharing between firms (right).

An important aspect to understand how individuals decide whether to disclose or not disclose their personal data is their applied processing approach for decision-making. Most privacy research focused solely on effortful decision-making neglecting effects of less effortful decision-making approaches. Such low-cognitive-effort processing approaches are rather based on factors like intuition, affective reactions, or feelings (Dinev et al. 2015; Goes 2013). Therefore, we follow the call of Dinev et al. (2015) to consider low-cognitive-effort processing in individuals' personal data disclosure decision-making.

In this study, both topics, i.e., a BNDE peculiarity as well as individuals' low-cognitive-effort decision-making are examined with the following research question:

*Is individuals' reliance on low-effort processing for their decision-making stronger in a BNDE disclosure setting, in which two firms share consumer data, or in an identical dyadic disclosure setting (without data sharing between the two firms)?*

To this end a short overview of the privacy calculus and some low-cognitive-effort heuristics is provided, with a focus on affective reactions. Afterwards, we draw on reinforcement knowledge to develop the hypotheses. To assess in which disclosure setting individuals rely more strongly on their affective reaction as instance of low-cognitive-effort (abbr. low-effort) processing, the effect sizes of affect between a BNDE and dyadic disclosure settings are compared.

We confirm that the effect of affect on disclosure willingness as well as on benefit perception for the BNDE disclosure setting are stronger compared to the dyadic setting. We also find that participants in

the BNDE setting perceive the disclosure decision-making process as easier in retrospect and that they also perceive a lower decision-uncertainty compared to participants in the dyadic setting.

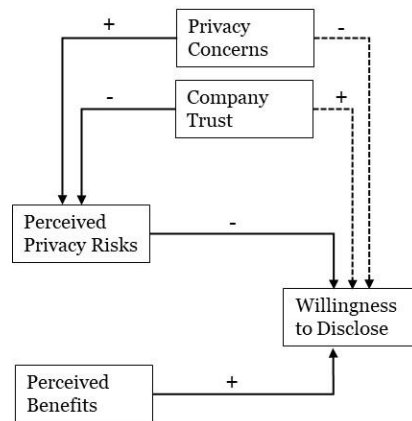
This study contributes to privacy research primarily in two ways. First, we transfer knowledge of reinforcement learning into the privacy field which offers a new perspective on individuals' data disclosure decision-making process. This could help to explore new phenomena and allows to derive adequate hypotheses based on this perspective, which could be especially helpful to understand peculiarities in BNDE disclosure settings. Second, by differentiating BNDE disclosure settings from dyadic settings, we shed light on the impact of "data sharing between firms" on individuals' reliance on low-cognitive-effort decision-making. This deepens the understanding of individuals' disclosure decision-making and offers implications for practitioners as well: especially when firms collect data in a BNDE setting, their communication with consumers regarding data handling practices needs to be adapted to the stronger reliance on low-effort processing.

## **Theoretical Background and Hypotheses Development**

### ***Privacy Calculus and the Base Model***

The privacy calculus is one of the dominant theories to explain individuals' willingness to disclose personal data (Dinev et al. 2015; Smith et al. 2011). This theory is closely linked to the "maximum utility theory" which assumes that individuals always choose the option with the highest utility that is calculated by benefits minus costs (Awad and Krishnan 2006; Li 2012). Equally, the privacy calculus assumes that an individual deliberatively processes and weighs their perceived benefits (e.g., monetary, or social incentives) of a data disclosure against its' costs in form of perceived privacy risks (e.g., spam mails or loss of privacy). The individuals form their willingness to disclose in a certain situation based on the result of this trade-off (Awad and Krishnan 2006; Dinev et al. 2015; Laufer and Wolfe 1977). Whereby the sum of the probability times the severity of each respective risk results in the total risk and likewise for the benefits (Peter and Tarpey 1975). Thus, to assess benefits and privacy risks, sub-evaluations, e.g., regarding the probability and severity must be performed. The privacy calculus is mostly seen as a purely deliberative thinking process, which requires high cognitive effort. Only few studies in this context underline the importance of another processing approach for decision-making (Dinev et al. 2015; Goes 2013). To be able to consider low-effort processing, the privacy calculus and the model of Smith et al. (2011) is used as basis for our structural equation base model.

Another important antecedent that decreases individuals' willingness to disclose in the model of Smith et al. (2011) is individuals' general privacy concern (cf. Dinev et al. 2015; Li 2012). Therefore, privacy concerns are included in the base model as well. However, there are contradictory findings whether privacy concerns exert a direct effect on disclosure willingness (e.g., H. Li et al., 2017) or whether this effect is mediated by perceived privacy risks (e.g., Keith et al., 2012; Kehr et al., 2015). We argue that general privacy concerns are a rather situation independent construct and thus, we expect its effect on disclosure willingness to be mediated by perceived privacy risks. Nevertheless, for additional verification purposes we also test the direct effect of privacy concerns on disclosure willingness in the structural equation model. Besides perceived benefits also individuals' trust in the data collecting company increases disclosure willingness in the model of Smith et al. (2011). Various studies additionally showed that trust decreases perceived privacy risks (Malhotra et al. 2004; Xu et al. 2005). Therefore, we consider trust and its effects on disclosure willingness and on perceived risks in the base model. However, we similarly assume that the effect of trust on disclosure willingness is mediated by risk perception. This leads to our base model displayed in Figure 2.



**Figure 2.** Structural equation base model including the expected effect directions. Dashed arrows are only included for control reasons.

### Low and High Cognitive Effort Processing

To address the issue that in privacy research mostly a pure high cognitive effort decision-making perspective is applied (Dinev et al. 2015), we consider low cognitive effort decision-making as well. There is a wide consensus that each individual has at least two systems for decision-making, which can interact with each other (Epstein 1994; Evans and Stanovich 2013; Finucane et al. 2000; Kahneman 2012; Petty et al. 1998; Rangel et al. 2008; Sloman 1996):

*System 1* is an intuitive, habitual, and emotional system that can even work unconsciously and requires only little cognitive effort, making processing with system 1 very fast. Decisions made with this type of processing are based strongly on factors like feelings, vividness or mental accessibility (Epstein 1994; Evans and Stanovich 2013; Kahneman 2003; Loewenstein et al. 2001; Slovic et al. 2004; Tversky and Kahneman 1974; Tversky and Koehler 1994). We refer to this type of processing as low-effort processing (cf. Dinev et al. 2015).

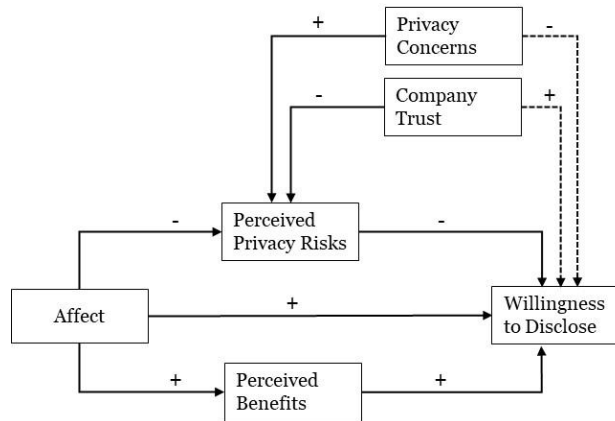
In contrast, *system 2* is connected to a reasoning, deliberate, serial thinking process and requires high cognitive effort to make a decision and thus, processing is slow (Daw 2012; Epstein 1994; Evans and Stanovich 2013; Finucane et al. 2000; Kahneman 2003). Also, this type of processing is rather rule-governed and more flexible to changes (Daw et al. 2005; Kahneman 2003). For example, the privacy calculus is assumed to be mainly processed by system 2 (Dinev et al. 2015). Especially the amount of benefits, the probability and the severity of a negative outcome are some of the most important factors influencing the decision when decision-making is based on system 2 (Dinev et al. 2015; Kahneman 2012; Loewenstein et al. 2001; Peter and Tarpey 1975; Smith et al. 2011). We refer to this type of processing as high-effort processing (cf. Dinev et al. 2015).

### Affective Reaction

In this study, the focus lies on a certain instance of low-effort heuristics, in particular on the affect heuristic (Slovic et al. 2007). “Affect means the specific quality of *goodness* or *badness* (i) experienced as a feeling state (with or without consciousness) and (ii) demarcating a positive or negative quality of a stimulus.” (Slovic et al. 2002, p. 329). Affective reactions occur “rapidly” and “automatically” (Slovic et al. 2002). An affective reaction is the very first processing result to a situation or stimulus, that cannot be influenced by slow high-effort processing (Kahneman 2003; Loewenstein et al. 2001; Pezzulo et al. 2013; Slovic et al. 2007; Zajonc 1980).<sup>2</sup> Thus, an affective reaction should be a pure result of low-effort processing (Slovic et al. 2002; Zajonc 1980). A more positive affective reaction towards a data disclosure decision increases the disclosure intention (Bidler et al. 2018; Wakefield 2013), decreases individuals’ perceived risks (Bidler et al. 2018; Chaudhuri 2002; Li et al. 2011; Loewenstein et al. 2001), and increases individuals’ perceived benefits (Bidler et al. 2018; Kehr et al. 2015; Li et al. 2011; Shampianier

<sup>2</sup> However, we agree on possible correlations or bidirectional effects of other low-effort heuristics and high-effort processing in general (cf. Kahneman 2003; Loewenstein et al. 2001; Pezzulo et al. 2013).

et al. 2007). Therefore, affect is used as a proxy construct in our structural equation model (SEM) to examine the impact of low-effort processing in this study.



**Figure 3.** Structural equation model including affect and the expected effect directions. Dashed arrows are only included for control reasons.

### Privacy Calculus from a Reinforcement Learning Perspective

The primary aim of this study is to examine how BNDE settings alter the impact of low-effort processing in form of affect regarding the disclosure decision-making process. To predict individuals' disclosure behavior for this new and unexplored BNDE disclosure setting, we integrate interdisciplinary dual-processing and signaling research in this study. Especially, studies on reinforcement learning as well as on cognitive effort in decision-making is used as a basis for this study. With this we try to extrapolate new hypotheses regarding low-effort processing effect sizes in our structural equation model. We adopt a new perspective in which we break down individuals' disclosure decision-making process in simple sequential "steps" for a high-effort processing approach (cf. Daw 2012) based on the privacy calculus, i.e., weighing of benefits against privacy risks (Smith et al. 2011).

One goal of reinforcement learning research is to understand the decision-making process of subjects. Subjects usually try to optimize their benefit or respectively their reward when confronted with decision-making. To examine this process in such studies, subjects are confronted with a task that mostly consists of several "steps". In these steps the subjects must perform an action, i.e., to choose from two or more possible alternatives to get closer to solving their task. Each decision leads them to a new "state", which either can be another step that analogously requires an action, i.e., a further decision between alternatives, or is an end-state. Such an end-state can be associated with rewards, no-rewards or even punishment and requires no further decision. Therefore, each decision can be somehow associated with a certain outcome "value", e.g., positive for decisions leading to rewards, negative for decisions leading to punishments (Daw et al. 2005; Gläscher et al. 2010; Redish et al. 2008). We draw on this procedure to similarly display the privacy calculus as a very simplified decision-making process.

In reinforcement learning literature, high-effort processing is generally modeled as a tree-search, which makes it necessary for subjects to build the respective tree at first and then calculate every single possible step to make a decision. In contrast, low-effort processing does not need a tree as it draws on the associated "stored values" to make decisions without the need to calculate every step from scratch (Daw 2012; Daw et al. 2005; Gläscher et al. 2010; Pezzulo et al. 2013). These outcome values are based on prior experiences (Daw et al. 2005; Forgas 1995; Gläscher et al. 2010; Pezzulo et al. 2013).

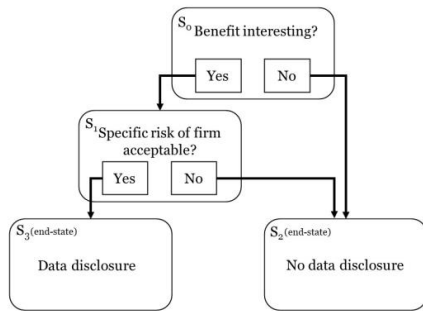
The decision-making process can be performed by high- as well as by low-effort processing. But for high-effort processing, individuals need to build the correct tree first and calculate every single step, which requires much more cognitive resources (Daw et al. 2005; Gläscher et al. 2010).

We visualize the privacy calculus in Figure 4 as a very simple disclosure decision-making process with only two decision options in each step. This resembles the decision-making modeling in reinforcement learning studies. In our simplified disclosure decision-making process, the individuals first must assess their perceived benefits, i.e., they perform an action which means that they are either interested in the

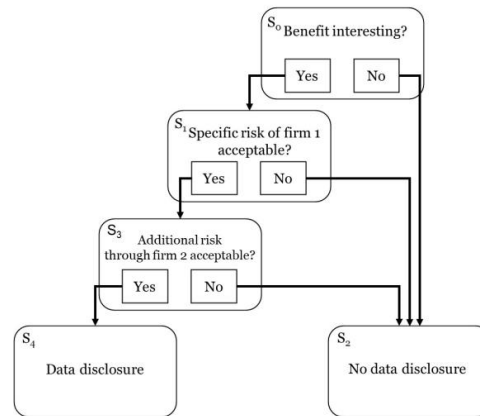
benefits (“yes”) or are not interested in the benefits (“no”). When individuals are not interested in the offered benefits, they have made their final decision to not disclose their data and end in a “no-disclosure end-state” (cf. Figure 4,  $S_2$ ). When individuals are interested in the benefits, they move on to the next step (cf. Figure 4, a:  $S_1$ ). Similarly, they have to assess their perceived privacy risks and equally perform an action: either, they decide the risk is acceptable (“yes”), or that the risk is not acceptable (“no”). When they decide it is not acceptable, they have made their final decision to not disclose their data and end in the no-disclosure end-state (cf. Figure 4, a:  $S_2$ ). When individuals perceive their risk to be acceptable, they have made their final decision to disclose their personal data and end in the data disclosure end-state (cf. Figure 4, a:  $S_3$ ). Each decision and the associated end-states are connected to a certain outcome value, which is based on previous experiences (Daw et al. 2005; Forgas 1995; Gläscher et al. 2010; Pezzulo et al. 2013).

In a BNDE setting individuals disclose personal data to a firm which subsequently shares their personal data with other firms. In such a setting individuals cannot always assign the offered benefits to the different firms. However, each firm adds additional privacy risks, e.g., as each firm has the potential for misuse of the data or is an additional hacking target, et cetera. Therefore, each firm adds an additional step in which the added risk must be assessed likewise and is either perceived as acceptable (“yes”) or not acceptable (“no”) (cf. Figure 4, b:  $S_3$ ). In a BNDE setting a firm oftentimes does not share consumer data with only one further firm but with several firms (e.g., Paypal 2018). Thus, such a BNDE setting requires individuals mostly to build a very long tree for high-effort processing as several steps are necessary.

a) Tree search (high-effort processing) for a data disclosure decision-making process in a dyadic setting, i.e., without data sharing between firms



b) Tree search (high-effort processing) for a data disclosure decision-making process in a BNDE setting, i.e., with data sharing between two firms



**Figure 4.** Privacy calculus modeled as a simplified decision-making process for a tree search (high-effort processing approach) regarding: a) individuals’ data disclosure decision-making process in a dyadic setting, i.e., without data sharing between firms; b) individuals’ data disclosure decision-making process in a BNDE setting, i.e., with data sharing between two firms. The tree belonging to the BNDE setting with data sharing between firms is longer as it has more steps. The exemplarily illustrated BNDE network is the simplest possible, consisting only of two firms.

It is possible at each step (and its inherent necessary action) in the decision-making process to switch between relying on low- or high- effort processing (Daw et al. 2005; Pezzulo et al. 2013). This means subjects can use both processing systems in one decision process, varying between the different steps. For example, in the first step high-effort processing is performed while in the second step low-effort processing is performed. Thus, we argue that also the total disclosure decision-making is not based either on low- or high-effort processing, but instead is based on both processing systems. However, one processing system can be more dominant depending on situational and individual characteristics. This is important as this study explores whether a BNDE disclosure setting leads to a more dominant low-effort decision-making compared to a dyadic setting.

Whether a decision is primarily based on low- or high-effort processing can cause different perceived uncertainty in one's decision (Maglio and Reich 2019; Tormala et al. 2011). Based on reinforcement learning knowledge, a subject prefers to base its decision on the processing system that has the lowest uncertainty regarding the predicted outcome for one's decision (Daw et al. 2005) in relation to the required cognitive resources (Pezzulo et al. 2013).

In reinforcement learning, highly trained subjects<sup>3</sup> with only two possible actions at each step rely for distal actions, i.e., actions that are further away from the outcome (end-state), more strongly on low-effort processing. This is because low-effort processing offers a sufficiently low uncertainty for outcome predictions for such distal actions. Whereas for proximal actions, i.e., actions closer to the outcome, high-effort processing offers a lower uncertainty in the prediction and thus, is rather relied on (Daw et al. 2005). However, if a decision-making process involves more distal actions (i.e., if the tree is longer as there are more steps) than another very similar decision process, subjects generally rely more strongly on low-effort processing *in total* for the longer decision-making process.

Individuals draw on their prior experiences to predict future outcomes and to apply an adequate behavioral reaction (Baumeister et al. 2007; Forgas 2008; Osberg and Shrauger 1986; Tversky and Kahneman 1974). In combination with perspectives of the signaling theory (for details on signaling cf. Books and Goffman 1969; Gambetta 2009; Varian 2016; Zahavi 2008), we assume the sole existence of a (privacy policy) statement regarding data sharing between firms can serve as a signal for individuals in a data disclosure setting (cf. Baumeister et al. 2007; Forgas 2008; Garbarino and Edell 1997; Klaczynski 2001; Pezzulo et al. 2013). This statement signalizes that there is a need to build a complex tree with many steps (cf. Figure 3, right half) as more firms obtain the disclosed data than in a single dyadic data disclosure. This always leads to a tree with more steps, i.e., a more complicated tree that needs to be build (cf. Figure 3). More steps in a certain decision-making process that need to be solved in a tree-search, i.e., under high-effort processing, lead to an even higher demand of cognitive resources (Daw et al. 2005; Kahneman 2003; Klaczynski 2001; Pezzulo et al. 2013; Redish et al. 2008). High requirements of cognitive resources for a decision-making process is generally unpleasant to consumers (Garbarino and Edell 1997). Such a "data sharing between firms" statement respectively such a BNDE signal could warn individuals that performing mostly high-effort processing would need too much cognitive resources and maybe does not lead to a satisfying (perceived) decision certainty (cf. Daw et al. 2005; Kahneman 2003; Maglio and Reich 2019; Pezzulo et al. 2013). The reason for this complexity could lie in the data policies of BNDE settings and their network characteristics (e.g., high number of firms in the exchange network), as the policies can be especially long, opaque, and thus, hard to understand (Ermakova et al. 2014; Furnell and Phippen 2012).<sup>4</sup> However, individuals thrive to use their cognitive resources sparingly (Fischer 2011; Garbarino and Edell 1997; Kahneman 2003; Pezzulo et al. 2013) and are more satisfied when they perceive lower uncertainty in their decisions (Camerer and Weber 1991; Daw et al. 2005; Ellsberg 1961; Maglio and Reich 2019).

In line with this, we argue that such a BNDE signal with associated expectation of high cognitive demand and a relatively high perceived decision uncertainty when performing high-effort processing leads automatically to a stronger reliance on low-effort processing for individuals' data disclosure decision-making (cf. Daw et al. 2005; Maglio and Reich 2019; Pezzulo et al. 2013). This stronger reliance on low-effort processing for their disclosure decision should be reflected by a stronger impact of affect on disclosure willingness. This is because affect is the very first impression/association experienced as a feeling state (Slovic et al. 2002), which resembles the low-effort processing approach in reinforcement learning studies where "stored values" are used for decision-making (cf. Daw et al. 2005).

In contrast, dyadic data disclosures have no statement regarding data sharing between firms, which means the BNDE signal for the need to build a complex tree in high-effort processing is missing. Thus,

---

<sup>3</sup> It is common in everyday life to be confronted with such disclosure decisions nowadays, which makes individuals highly trained regarding personal data disclosures and sharing of their data. This can be exemplarily illustrated by number of active daily users of Facebook (1,6 billion in 2019, cf. Facebook 2021), and how Facebook handles their users' data (cf. Ho 2018; Solon 2018; Vaidhyanathan 2018; Valentino-DeVries et al. 2018). Thus, we assume that everyone who participated in our survey like most individuals in general have gone through such personal data disclosure decision-making processes already very often for settings without as well as settings with data sharing between firms.

<sup>4</sup> We assume the newly enacted General Data Protection Regulation (GDPR) does help to solve this problem in the European Union at least partially ("General Data Protection Regulation" 2016). However, it remains to be seen to what degree this regulation helps to offer consumers transparent and easy understandable privacy policies. From our point of view, solely the fact that some firms share data with a high number of firms, which are often unknown to the consumers, makes it hard to process the risks in a high-effort processing manner. For example, this is the case for the privacy policy of Paypal (Paypal 2018).



individuals have no signal which makes them anticipate that high-effort processing would lead to an unsatisfying decision uncertainty or that high-effort processing would require a rather long tree-search which could demand too much cognitive resources. Therefore, we argue that in a dyadic setting the individuals do not expect to exceed a certain cognitive threshold or to exceed a specific decision uncertainty level when performing high-effort processing. This should make individuals more strongly rely on low-effort processing, e.g., in form of affect, in a BNDE data disclosure setting, i.e., where firms share consumer data with further firms, compared to the same data disclosure decision-making in an identical dyadic data sharing setting, i.e., where the firms do not share any consumer data with other firms. Thus, we hypothesize:

H1: *Individuals rely more strongly on affect for their disclosure willingness in a BNDE data disclosure setting with data sharing between firms than in an equal dyadic data disclosure setting without data sharing between firms.*

Evaluations of benefits and privacy risks can be similarly displayed as decision processes themselves in which several steps are necessary to make a final benefit/privacy risk decision. For example, steps in the risk evaluation could be simplified to: step 1) risk of spam existent? Step 2) risk of identity theft existent? For the sake of clarity, these evaluations of benefits and privacy risks were simplified and aggregated in figure 2 into a single step, respectively. This means the evaluations of benefits and privacy risks are sub-processes in the data disclosure decision-making process.

Previous studies found that higher (positive) affect decreases individuals' perceived risks while it increases individuals' perceived benefits as well as their disclosure willingness (Alhakami and Slovic 1994; Chaudhuri 2002; Kehr et al. 2015; Li et al. 2011; Shampanier et al. 2007; Slovic et al. 2007; Wakefield 2013). As argued for H1, individuals' disclosure willingness should be more strongly influenced by affect as instance of low-effort processing. Equally, individuals should rely more strongly on affect for sub-processes like their benefit or their privacy risk evaluation. Therefore, we hypothesize:

H2: *Individuals rely more strongly on affect for their benefit perception in a BNDE data disclosure setting with data sharing between firms than in an equal dyadic data disclosure setting without data sharing between firms.*

H3: *Individuals rely more strongly on affect for their privacy risk perception in a BNDE data disclosure setting with data sharing between firms than in an equal dyadic data disclosure setting without data sharing between firms.*

As mentioned above, we assume that building the tree and performing all necessary steps in high-effort processing for BNDE data disclosure settings with data sharing between firms is cognitively more demanding compared to dyadic data disclosure settings without data sharing. On first sight, this could mean individuals perceive higher complexity for disclosure decision-making in a data sharing setting before conducting the decision-making process. However, we are interested how individuals perceive this in *retrospect*, i.e., after individuals have completed their decision-making process. We expect individuals in the BNDE setting should perceive in *retrospect* less decision-making complexity than in a dyadic setting. The reason for this expectation lies in H1-H3. We expect individuals in the BNDE setting to rely more strongly on low-effort processing due to the BNDE warning cue, which signals them that this decision-making process could require too much cognitive resources in respect to the possible outcomes under high-effort processing (cf. Baumeister et al. 2007; Klaczynski 2001; Pezzulo et al. 2013). If individuals in the BNDE setting do rely more strongly on low-effort processing as hypothesized, we expect individuals in the BNDE setting also to perceive the decision-making process *after performing* it to be less complex as they performed less high-effort processing than individuals in a dyadic setting.

Therefore, we hypothesize:

H4: *Individuals perceive less decision-making complexity in a BNDE data disclosure setting with data sharing between firms than in an equal dyadic data disclosure setting without data sharing between firms.*

One reason for individuals to rely more strongly on low-effort processing besides the lower necessary cognitive resources (Pezzulo et al. 2013) is the potential for a lower decision uncertainty (Daw et al. 2005; Zajonc 1980). Individuals' uncertainty in a decision can decrease when new confirmatory information is available (Fischer 2011) or when another processing type is used (Daw et al. 2005; Garbarino and Edell 1997; Maglio and Reich 2019; Pezzulo et al. 2013; Tormala et al. 2011; Zajonc 1980). If individuals' perceived decision uncertainty can be decreased for certain situations by relying more strongly on low-effort processing, they probably do this to decrease decision-making complexity

and to be more accurate in their outcome prediction (cf. Daw et al. 2005; Garbarino and Edell 1997; Pezzulo et al. 2013; Tormala et al. 2011). From a psychology perspective, they may prefer the low-effort processing to “feel” better when they realize this opportunity, e.g., when they have a signal that stands to reason a high decision uncertainty for high-effort processing (Maglio and Reich 2019; Tormala et al. 2011). This should be the case, even when it is only a perceived lower decision uncertainty (without the need to be objectively more precise in the prediction). This perceived lower decision uncertainty under low-effort processing can be explained by different factors that are relied on compared to high-effort processing, e.g., vividness, (Kahneman 2003; Loewenstein et al. 2001; Zajonc 1980). Similarly, under low-effort processing individuals may neglect certain contradictory information or factors that are rather processed by high-effort processing, e.g., probabilities. To perceive less decision uncertainty can be considered desirable for individuals, even when it is just a *perceived* lower uncertainty (cf. Maglio and Reich 2019; Tormala et al. 2011). As we assume data sharing as a signal to rely more strongly on low-effort processing, we hypothesize:

H5: *Individuals perceive less decision uncertainty in a BNDE data disclosure setting with data sharing between firms than in an equal dyadic data disclosure setting without data sharing between firms.*

## Sample and Setup

In this study, we use a hypothetical-scenario based survey, as this is a common approach in privacy research (e.g., Kehr et al. 2015; Malhotra et al. 2004). A first pre-test was conducted in form of 5 interviews regarding the survey to ensure understandability of the scenarios and to ensure an appropriate level of perceived benefits and privacy risks. First data was collected in October 2018. To increase the sample size, further data was obtained in April 2019. It was verified that the obtained observations during the two collection phases were not significantly different. The data was collected in cooperation with a panel provider. All participants lived in Germany and were 18 years or older.

The participants were randomly split into two groups. The participants were introduced to the same two hypothetical firms in both groups. The first firm was a software company that is not privacy certified, has low know-how regarding IT security, and high know-how regarding consumer data analysis. Whereby, the second firm was a retail firm that was privacy certified, had high know-how regarding IT security, and low know-how regarding consumer data analysis. The firm introductions were followed by a data disclosure scenario, in which the individuals were asked to disclose personal data in exchange for a 20 Euro cinema voucher.

The only difference between the two groups was regarding the disclosure setting type. To be more particular, whether the two firms share consumer data: in the first group, referred to as group 1 or “BNDE setting”, the individuals were asked to disclose their data only to firm 1 which shares the exact same data subsequently with firm 2. The participants were promised a 20 Euro cinema voucher for this data disclosure. Whereas, in group 2, the individuals were asked to disclose their data to the two respective firms separately, i.e., two dyadic data disclosures with the exact same data and no data sharing between the firms (we refer to this as the “dyadic setting”). With an “autofill” possibility in the scenario of group 2, it was ensured that no additional effort for filling out the second data disclosure form was anticipated by the participants. The participants in group 2 were offered a cinema voucher share of 10 Euro for a data disclosure to each of the two firms (in total 20 Euro cinema voucher). However, it was clearly stated that the consumers need to disclose their personal data to both firms in order to obtain a cinema voucher due to a minimum voucher payout amount of 20 Euro. Therefore, they had to choose either to disclose to both firms, or choose to not disclose at all. With this, participants’ benefits (in form of a cinema voucher of 20 Euro in total) and their privacy risks (in form of the same two firms obtaining the data) are identical for both scenarios as in both scenarios the identical two firms collect the same personal data. We ensured the participants have read and understood their scenario (i.e., that the two described firms obtain the exact same data when the participants decide to disclose their data) and the following questions adequately, otherwise they were removed from the sample.

After the scenario, the participants had directly to state their affect (AFF). After this they had to assess their willingness to disclose (WTD), perceived uncertainty in their disclosure decision (DU), perceived complexity of their decision-making process (DC), perceived benefits (BENE), perceived privacy risks (RISK), trust in the firms (TRUST), and their privacy concerns (PC and GIPC).<sup>5</sup> Additionally, we asked

---

<sup>5</sup> An alternative privacy concerns measurement instrument designed for the online context (PC) was added at the end of the survey in the second data collection phase.

and controlled for participants' age (AGE), perceived transparency of firms' data handling procedures (TRANS), sensitivity of the disclosed data (SENS), participants' perceived control over their disclosed data (CONT), and their perceived realism for the scenario (REAL). For all constructs existing measurement instruments were used, that were adapted to this studies' context when necessary (cf. Appendix Table 5 for details). With our study design, we ensured not only that identical firms collect the personal data but also that the participants in both groups obtain the same relevant descriptions for assessing their benefits, privacy risks, et cetera to hold these constructs objectively constant between the groups. We also designed the study in such a way, that the individuals do not anticipate the data sharing aspect to improve the offered service respectively their benefit. This allows us to specifically study the influence of disclosure settings *with* versus *without* data sharing between firms regarding the reliance on affective heuristics.

We removed observations from participants that seem to have paused the survey. This was necessary as the study examines the influence of affective reactions towards two different disclosure settings which can hardly be observed when the disclosure stimulus is "overwritten" by other tasks while participants paused the survey. Thus, we decided to remove survey duration time outliers in a conservative manner to not sort out those participants who just took their time to assess benefits and risks thoughtfully. Therefore, we only removed observations which were extreme outliers regarding the time needed to complete the survey. By doing so 27 participants which took more time to complete the survey than double the median duration (participants' median duration to complete the survey was 902s) were removed. This led to a final sample of 337 total participants (BNDE setting: n= 165; dyadic setting: n=172; for a more detailed distribution cf. Appendix Table 6).

## **Results**

Before starting to analyze the data, we verify that the scenarios are perceived as sufficiently realistic in both groups without differences between the groups. We analyze the data with a second generation structural equation modeling technique: the variance-based partial least squares (PLS) method (Hair et al. 2011; Wold 1966). PLS is especially suited for predictive and exploratory research as done in this study and because there are no distributional requirements for this method, it is suited well to analyze our collected data (cf. Hair et al. 2011). This method can be used to test the measurement model as well as the hypothesized structural model (Bagozzi and Yi 1989; Gefen et al. 2000; Hair et al. 2016). Furthermore, the path coefficients and the effect sizes between two groups can be compared with PLS multi group analysis (MGA) and PLS permutation test (Hair et al. 2017), which is the primary goal of this study.

### **Measurement Model Assessment**

The psychometric properties for the measurement models of the two groups are assessed separately. We test for internal consistency reliability, convergent validity, and discriminant validity (Hair et al. 2017).

Internal consistency reliability is established, as Cronbach's  $\alpha$  as well as composite reliability are above the lower threshold of 0.7 for all constructs in both groups (Bagozzi and Yi 2012).

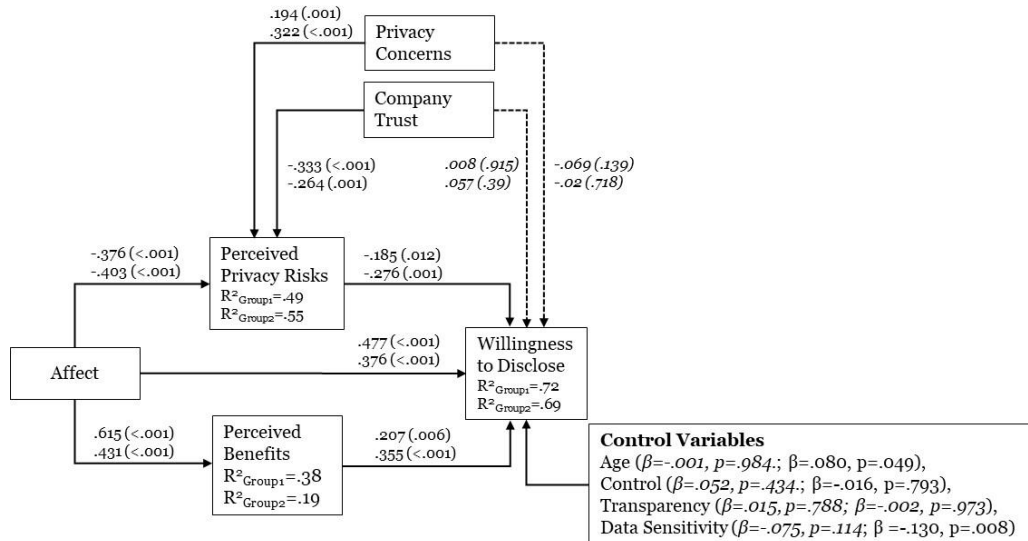
To verify convergent validity, we assess the item loadings as well as the average variance extracted (AVE). The outer loadings of the items on their respective constructs should exceed 0.7 (Bagozzi et al. 1991; Hair et al. 2011), which applies to all items in the structural equation model for both groups. The AVEs for the constructs should exceed the threshold of 0.5 to confirm convergent validity (Hair et al. 2011) which applies to all constructs in the structural equation model for both groups.

We confirm discriminant validity, as the following three criteria are fulfilled in both groups: all item loadings are greater than the respective cross-loadings on other constructs (Bagozzi and Yi 2012), the Fornell-Larcker criterion is met (Fornell and Larcker 1981), and the constructs' heterotrait-monotrait ratios (HTMT) are below the conservative threshold of 0.85 (Henseler et al. 2015). Detailed measurement model assessment results can be found in the Appendix Table 7-14.

### **Structural Model Assessment**

Next, we assess the structural model and the hypothesized relationships separately for both groups. To ensure no collinearity issues are present between the exogenous latent variables, the variance inflation factors (VIFs) have to be below the threshold of 5 for each construct (Thatcher and Perrewé 2002). This

is the case for group 1 with a maximum VIF value of 3.0 and for group 2 with a maximum VIF value of 2.6 (for detailed results cf. Appendix Table 15).



**Figure 5.** Structural equation modeling results for both groups (results of group 1 are displayed in the figure above/before results of group 2), including path coefficients followed by the respective p-values in brackets. Results for control variables are separated between the two groups with a semicolon. All effects with a significance level  $p > .1$  are in italics.

We perform a bootstrap procedure with 5,000 bootstrapping samples to evaluate the significance of the path coefficients.<sup>6</sup> In the estimated structural model displayed in Figure 5, besides the control variables all path coefficients have the expected directions and are significant ( $p < .05$ ) with two exceptions: as expected, the effect of privacy concerns and trust on individuals' disclosure willingness are non-significant. Our interpretation of these constructs as rather "general" constructs which exert their effects on disclosure willingness via more situational constructs, like privacy risks, seems to be appropriate (cf. Kehr et al. 2015). All assumed significant effects have an effect size above the lower threshold of  $f^2 = .02$  (Cohen 1988; Hair et al. 2016).

### Group Comparison

After ensuring the measurement as well as the structural model is valid for both groups, we proceed to the initial aim of this study to compare the effect sizes between the two groups. We perform the PLS multi group analysis (PLS-MGA, cf. Hair et al. 2017; Henseler et al. 2009) as well as the permutation test (cf. Chin and Dibbern 2010; Hair et al. 2017). For the group comparison, we firstly ensure partial measurement invariance by assessing the first two steps of the measurement invariance assessment (MICOM, cf. Hair et al. 2017; Henseler et al. 2016). The first step is verifying configural invariance, which is given as the participants in both groups were confronted with identical measurement items and data handling was also identical. The second step is ensuring compositional invariance, which we can confirm since the composite scores are not significantly different from 1 (all p-values  $> .1$ , cf. Appendix Table 16).

<sup>6</sup> For the two constructs privacy concerns and perceived decision uncertainty only 211 observations (group 1: 98, group 2: 113) were obtained. To ensure that all available observations for the other constructs can be used, we used a mean value replacement for missing data in accordance with the recommendation of Hair et al. (2016). Likewise, pairwise deletion led to identical results. For privacy concerns an alternative measurement instrument, the global information privacy concerns scale, with all 337 observations was used – leading to almost identical results.

The Effect of Data Sharing Between Firms

Table 1 displays the group comparison results regarding the path coefficients ( $\beta$ ). In table 2, the group comparison results regarding the effect sizes ( $f^2$ ) are displayed. We provide both, one-tailed p-values for hypotheses testing as these are directed and thus a one-tailed test is more appropriate (cf. Hair et al. 2017) as well as two-tailed p-values to allow better comparability of differences between the groups regarding other effects.

**Table 1.** Path coefficient ( $\beta$ ) group comparison test results (two-tailed).

Effect	$\beta_{\text{Group1}}$	$\beta_{\text{Group2}}$	$\beta_{\text{Group1}} - \beta_{\text{Group2}}$	PLS-MGA p-value two-tailed / one-tailed*	$\Delta(\beta_{\text{PermutationGroup1}} - \beta_{\text{PermutationGroup2}})$ [95% CI two-tailed]	Permutation p-value two-tailed / one-tailed*
AFF -> WTD (H1)	.477	.306	.171	.054 / .027	-.002 [ -.175;.17]	.053 / .027
AFF -> BENE (H2)	.615	.431	.185	.030 / .015	.000 [ -.171;.168]	.033 / .017
AFF -> RISK (H3)	-.376	-.403	.027	.772 / .386	.000 [ -.183;.179]	.775 / .386
AGE -> WTD	-.001	.080	-.081	.192 / .904	-.001 [ -.13;.126]	.215 / .900
BENE -> WTD	.207	.355	-.148	.127 / .937	.000 [ -.19;.192]	.134 / .937
CONT -> WTD	.052	-.016	.068	.447 / .224	.001 [ -.177;.177]	.459 / .238
SENS -> WTD	-.075	-.130	.056	.414 / .207	.000 [ -.137;.136]	.436 / .201
RISK -> WTD	-.185	-.276	.091	.409 / .204	-.001 [ -.214;.217]	.410 / .210
PC -> WTD	-.069	-.020	-.049	.488 / .756	.000 [ -.135;.134]	.485 / .753
PC -> RISK	.194	.322	-.128	.142 / .929	-.002 [ -.179;.174]	.163 / .917
TRANS -> WTD	.015	-.002	.017	.842 / .421	.001 [ -.157;.16]	.848 / .574
TRUST -> WTD	.008	.057	-.049	.640 / .680	-.001 [ -.176;.184]	.590 / .697
TRUST -> RISK	-.333	-.264	-.069	.544 / .728	.000 [ -.235;.237]	.551 / .725

\*One-tailed tests are always performed in the direction group 1 > group 2.

**Table 2.** Effect size ( $f^2$ ) group comparison test results (two-tailed).

Effect	$f^2_{\text{Group1}}$	$f^2_{\text{Group2}}$	$f^2_{\text{Group1}} - f^2_{\text{Group2}}$	PLS-MGA p-value two-tailed / one-tailed*	$\Delta(f^2_{\text{PermutationGroup1}} - f^2_{\text{PermutationGroup2}})$ [95% CI two-tailed]	Permutation p-value two-tailed / one-tailed*
AFF -> WTD (H1)	.383	.166	.217	.091 / .046	-.003 [ -.26;.247]	.098 / .047
AFF -> BENE (H2)	.610	.228	.382	.043 / .021	.000 [ -.35;.357]	.033 / .019
AFF -> RISK (H3)	.194	.275	-.081	.516 / .742	.000 [ -.253;.262]	.532 / .731
AGE -> WTD	.000	.020	-.020	.317 / .841	.000 [ -.03;.031]	.180 / .921
BENE -> WTD	.062	.270	-.208	.038 / .981	-.001 [ -.208;.21]	.051 / .975
CONT -> WTD	.004	.000	.004	.963 / .482	.000 [ -.008;.01]	.242 / .136
SENS -> WTD	.015	.041	-.027	.503 / .749	.000 [ -.068;.072]	.452 / .795
RISK -> WTD	.055	.095	-.040	.591 / .704	.001 [ -.138;.137]	.558 / .715
PC -> WTD	.013	.001	.012	.561 / .280	.000 [ -.034;.035]	.467 / .240
PC -> RISK	.067	.208	-.141	.145 / .928	-.002 [ -.188;.186]	.143 / .928
TRANS -> WTD	.001	.000	.000	.871 / .436	.000 [ -.009;.011]	.852 / .438
TRUST -> WTD	.000	.005	-.005	.696 / .652	.000 [ -.015;.018]	.496 / .749
TRUST -> RISK	.141	.118	.022	.844 / .422	.000 [ -.216;.218]	.839 / .414

\*One-tailed tests are always performed in the direction group 1 > group 2.

According to the PLS-MGA and permutation test, the path coefficient (cf. Table 1) and effect size (cf. Table 2) regarding the effect of affect on disclosure willingness are significantly larger in group 1 than in group 2 ( $\Delta\beta = .171$ ,  $p_{\text{MGA}} = .027$ ,  $p_{\text{Perm}} = .027$ ;  $\Delta f^2 = .217$ ,  $p_{\text{MGA}} = .046$ ,  $p_{\text{Perm}} = .047$ ). Therefore, we accept H1.

The path coefficient and effect size for the effect of affect on perceived benefits are significantly larger in group 1 than in group 2 ( $\Delta\beta = .185$ ,  $p_{\text{MGA}} = .015$ ,  $p_{\text{Perm}} = .017$ ;  $\Delta f^2 = .382$ ,  $p_{\text{MGA}} = .021$ ,  $p_{\text{Perm}} = .019$ ). Thus, we accept H2.

The Effect of Data Sharing Between Firms

We reject H3 as the path coefficient for the effect affect on perceived privacy risks is not smaller (i.e., more negative) for group 1 than for group 2. Also, the respective effect size is not larger in group 1 than in group 2 ( $\Delta\beta = .027$ ,  $p_{MGA} = .614$ ,  $p_{Perm} = .614$ ;  $\Delta f^2 = -.081$ ,  $p_{MGA} = .742$ ,  $p_{Perm} = .731$ ).<sup>7</sup>

Also noteworthy are the following group comparison results: the effect of age on disclosure willingness is somewhat stronger in group 2 ( $\Delta\beta = -.081$ ,  $p_{MGA} = .096$ ,  $p_{Perm} = .1$ ;  $\Delta f^2 = -.02$ ,  $p_{MGA} = .159$ ,  $p_{Perm} = .079$ ). Also, the effect of perceived benefits on disclosure willingness is stronger for group 2 than for group 1 on a significance level of  $p < .1$  ( $\Delta\beta = -.148$ ,  $p_{MGA} = .063$ ,  $p_{Perm} = .063$ ;  $\Delta f^2 = -.208$ ,  $p_{MGA} = .019$ ,  $p_{Perm} = .025$ ). Furthermore, the effect of privacy concerns on perceived privacy risks in group 2 is stronger on a  $p < .1$  significance level ( $\Delta\beta = -.128$ ,  $p_{MGA} = .071$ ,  $p_{Perm} = .083$ ;  $\Delta f^2 = -.141$ ,  $p_{MGA} = .072$ ,  $p_{Perm} = .072$ ). All other group comparison results regarding path coefficients and effect sizes for the other effects have  $p > .1$  for two-tailed as well as one-tailed tests.

The “R” package “EnvStats” is used for a two-tailed unpaired randomization test for location (Cohen 1995; Fisher 1935; Richards and Byrd 1996; Smucker et al. 2007) with 50,000 permutations to control for the equality of affect, perceived benefits, perceived privacy risks, privacy concerns, trust in the firms, perceived control, data sensitivity and perceived data handling transparency between the groups (cf. Table 3). This is done to ensure that no processing type is preferred over the other one due to an unintended manipulation respectively due to a difference of these constructs between the groups. We additionally perform one-tailed unpaired randomization tests to be able to reject alternative explanations. We obtain solely insignificant differences between the two groups ( $p > .1$ ) and therefore, we can reject alternative explanations based on a distinct expression regarding these tested variables.

**Table 3.** Results for unpaired randomization tests for location.

	Mean Group 1 (number of observations)	Mean Group 2 (number of observations)	Difference	p-Value (two- tailed / one- tailed)
Affect	2.909 (n=165)	2.971 (n=172)	-.062	.577 / .297
Benefits	3.762 (n=165)	3.600 (n=172)	.162	.336 / .834
Privacy Risks	4.651 (n=165)	4.700 (n=172)	-.049	.784 / .392
Privacy Concerns	4.390 (n=98)	4.429 (n=113)	-.039	.847 / .423
Trust in Companies	3.891 (n=165)	4.091 (n=172)	-.201	.238 / .118
Data Sensitivity	4.782 (n=165)	4.767 (n=172)	.014	.948 / .547
Data Handling Transparency	4.198 (n=165)	4.083 (n=172)	.115	.520 / .738
Control over Data	2.774 (n=165)	2.842 (n=172)	-.068	.680 / .340

<sup>7</sup>One-tailed tests were always performed in the direction group 1 < group 2.

Equally, a one-tailed unpaired randomization test for location (Cohen 1995; Fisher 1935; Smucker et al. 2007) with 50,000 permutation samples is used to verify H4 and H5, i.e., lower perceived decision complexity (H4) and lower perceived decision uncertainty (H5) after the decision-making process in group 1 than in group 2 (Table 4). Participants in group 1 assess the decision-making process complexity in retrospect significantly lower than those in group 2 ( $\Delta = -.296$ ,  $p = .036$ ). Therefore, we accept H4. Similarly, we observe a lower perceived decision uncertainty ( $\Delta = -.341$ ,  $p = .077$ ) in group 1 than in group 2 on a significance level  $p < .1$ . Thus, we accept H5 on a 10% significance level.

**Table 4.** Results for one-sided unpaired randomization tests for location.

	Mean Group 1 (number of observations)	Mean Group 2 (number of observations)	Difference	p-Value one-tailed test (group 1 < group 2)
Decision Complexity (H4)	3.158 (n=165)	3.453 (n=172)	-.296	.036
Decision Uncertainty (H5)	3.355 (n=98)	3.696 (n=113)	-.341	.077

<sup>7</sup> Due to the negative sign for the effect of affect on perceived privacy risk, the correct p-values for the one-tailed tests regarding the path coefficients in H3 are obtained by subtracting the one-tailed p-values (displayed in table 1) from 1. The same procedure must be applied when the test direction is inverted.

## **Discussion, Implications and Limitations**

In this chapter, we briefly summarize and discuss the results. In the implications section, we explain in which way this study contributes to theory and helps researchers as well as practitioners. In the end, limitations of this study are discussed and opportunities for future research are identified.

### **Discussion**

We extend the privacy calculus model of Smith et al. (2011) by implementing affect as instance of low-effort processing (cf. Slovic et al. 2002) into the research model. Based on the results, our model with affect is acceptable as the assumed effects are significant in both groups: a more positive affective reaction towards a data disclosure setting does increase individuals' disclosure willingness, as well as their perceived benefits, while it decreases individuals' perceived privacy risks. Privacy concerns and trust have, as expected, only an indirect effect on disclosure willingness, which is mediated by perceived privacy risks.

In line with our hypotheses H1, participants in the BNDE setting rely more strongly on their affect than those in the dyadic setting. Similarly, in the BNDE setting affect impacts perceived benefits more strongly than in a dyadic setting (H2). However, H3 is rejected as participants in the BNDE setting do not rely more strongly on affect for their privacy risk perception than those in the dyadic setting.

Both, the path coefficients and effect sizes are not significantly different between the groups regarding this effect. In the following a first explanation is provided, why affect seems to have a stronger impact on benefit perception but not on privacy risk perception in the BNDE compared to the dyadic setting. The reason could lie in individuals' perspectives towards a data exchange cooperation like BNDE and its impact on their privacy risk perception: i) a data exchange cooperation of firms could generally either be perceived by the consumers to reduce privacy risks through know-how exchange or mutual control between the firms (Gartner 2013; Lei and Slocum Jr. 1992; Mason 1993); ii) it could also lead to an increase in privacy risk perception, e.g., due to an unsafe additional data transfer (cf. O'Neill 2021; Satariano 2020); iii) or the data sharing cooperation aspect between the firms could be seen as neutral or is simply ignored in their privacy risk assessment.

This aspect only exists in the BNDE setting but not in the dyadic setting. Therefore, such a data sharing cooperation between firms adds another facet that needs to be considered to understand individuals' risk perception, i.e., how such a data sharing cooperation is perceived by individuals. In contrast, this factor does not impact individuals' perceived benefits in the dyadic scenario, as the only benefit the participants can obtain is a cinema voucher of the same value as in the BNDE setting. Thus, the data sharing cooperation of the firms does not alter their expected benefits. However, this could change when the service, i.e., benefits could be improved through a data sharing cooperation in form of better personalized offers, faster search results, or a greater choice of products as there are more stores to choose from, et cetera (cf. Ball et al. 2006; Komiak and Benbasat 2006; Mittal and Lassar 1996). We assume that this perceived data sharing characteristic could also serve as an additional factor of influence respectively as another applicable heuristic for the privacy risk assessment in the BNDE setting. This could explain why affect does not explain more variance of consumers' perceived privacy risk in the BNDE compared to the dyadic setting. This could be due to a new factor only existent in the BNDE setting, that could exert an disturbing effect.

Nonetheless, in total, this study shows that the transfer of reinforcement knowledge to privacy behavior can be helpful and offers first explanations for individuals' behavior in BNDE disclosure settings. We confirmed that individuals in a BNDE disclosure setting generally perform less high-effort processing but instead draw more strongly on low-effort processing for decision-making. We argue the reason for this behavior is the BNDE statement, which signals to them that much cognitive resources are necessary and that a stronger reliance on low-effort processing could be beneficial. This reduces the chance of individuals to surpass a threshold of cognitive resources or prevents them from finding and effortfully processing contradictory information, which results in a lower decision process complexity and reduces individuals perceived decision uncertainty. In line, we observe that individuals perceive a lower decision complexity and a lower decision uncertainty after performing the decision-making process in a BNDE setting, in which low-effort processing is more dominant, compared to the dyadic setting.

### **Implications**

This study shows that individuals are more strongly influenced by affect in BNDE data disclosure settings, compared to the respective dyadic data disclosures. With this study, we contribute to theory in two ways:

*First*, we integrate reinforcement learning knowledge and low-effort processing knowledge in the privacy calculus by viewing the privacy calculus as a simplified decision-making process, which can include several steps and sub-processes. We bring a new perspective to the privacy calculus as each step in a decision-making (sub-)process, e.g., the privacy risk assessment, can be processed by high- and low-effort processing, whereby the dominant system depends on the situation (cf. Daw et al. 2005; Loewenstein et al. 2001; Pezzulo et al. 2013). This new perspective on the privacy calculus should allow researchers to develop hypotheses and explain results regarding the influence of affect in several circumstances that were hard to explain until now. For instance, when individuals must disclose more data types this could lead to a stronger reliance on affect as there are more processing steps compared to data disclosures in which less data types must be disclosed – even when the total sensitivity of the disclosed data would be held constant.

*Second*, while other studies do not recognize that BNDE has several peculiarities (e.g., network size, firm order, et cetera) and examined it like a dyadic data disclosure (e.g., Angst and Agarwal 2009), we focus on the most apparent peculiarity: the data sharing between firms aspect itself. We show that individuals are more strongly influenced by affect (as exemplary instance of low-effort processing) when data sharing between firms is present than when it is not. Therefore, data sharing between firms itself is an important characteristic of BNDE settings, that impacts individuals' decision-making. The knowledge regarding increased decision-making based on affect in complex BNDE settings could eventually help to better understand the success of certain businesses despite their extensive data collection and further sharing of personal consumer data with several third-parties (e.g., Facebook 2021; Vaidhyathan 2018).

Besides theoretical contribution, this study offers important insights especially for regulators and personal-data-driven businesses. We agree on the necessity that firms state their data handling practices completely transparent and truthful in form of a data policy. However, we show that affect is in both disclosure settings, i.e., for BNDE as well as dyadic settings, an important influence factor that determines individuals' willingness to disclose personal data to a firm. This result highlights the importance to include cues and information for consumers which are suited to be used as input for individuals' low-effort processing. This is especially important for BNDE settings as individuals base their decision more strongly on low-effort processing than in dyadic disclosure settings. For example, a EU-certified privacy ample that does not include all detailed data handling information but rather displays an overall privacy intrusiveness for the respective data disclosure could possibly serve as such a low-effort processable information (cf. Bal 2014; Great Britain Food Standards Agency 2008). As red could be associated intuitively with "stop" or "danger" while green probably could be stronger connected to a "go" or an "everything okay" feeling and thus is a more adequate information input for low-effort processing. Firms could also use this knowledge to adapt their communication strategy by using an information presentation that fits better to the strength of influence of affect respectively of low-effort processing. This could help consumers to include more information in their low-effort processing and in turn, could lead to a higher number of consumers that are willing to disclose their personal data.

### **Limitations and Future Research**

Like every research, this study must be viewed in light of its' limitations and by doing so, we want to open up further roads for research.

We observe some unexpected effect size differences between the groups. For example, data sensitivity has a stronger negative effect on disclosure willingness in the dyadic setting. This seems reasonable, as data sensitivity is connected to the damage severity that is mainly used as a factor in high-effort processing (Loewenstein et al. 2001; Peter and Tarpey 1975). However, further research is required to verify and understand the mechanisms in more detail. Especially regarding the effects of perceived benefits, privacy concerns, and data sensitivity.

Furthermore, it would be interesting to understand exactly why affect has a stronger effect on perceived benefits but not on perceived privacy risks in the BNDE setting compared to the dyadic setting. Particularly, the varying influence of individuals' privacy concerns on perceived privacy risks depending



on the data sharing characteristic could open up a promising road for future research to deepen the understanding of individuals' risk evaluation process.

Another limitation relates to the scenario design in our study. Nevertheless, we are convinced that our hypothetical scenarios are suited for our research aim as the scenarios are as identical as possible under the condition that the exact same data must be disclosed to the same two firms in both groups. We additionally ensured that common predictors were not distinct between the two groups (except for the hypothesized differences). However, we still compare one single data disclosure to a data exchange network consisting of two firms in group 1 with two dyadic data disclosures to the respective firms in group 2. A complementary study could apply the same methodology but compare the effects of individuals that can disclose once in a BNDE setting with individuals that can disclose once to one firm in a dyadic disclosure situation, i.e., hold the number of data disclosures equal between the groups.

This limitation is also related to the next one. With our study design we are not able to verify that the lower perceived decision complexity and lower perceived decision uncertainty in the BNDE setting is purely based on the stronger reliance on low-effort processing. An alternative explanation could be the fact that participants in the dyadic setting are confronted with two dyadic data disclosures whereas it is only one disclosure in the BNDE setting. Thus, the participants' respective decision complexities/uncertainties of the two data disclosures in group 2 could be added or somehow altered differently in the evaluation process of the total decision complexity/uncertainty than in group 1. Again, future studies could help to verify our results when drawing on the same methodology but comparing the same number of disclosures.

We also do not examine how the respective privacy risk or benefit perception is influenced or obtained by high-effort processing but instead we focus on affect as proxy for low-effort processing. It could be beneficial to use other low-effort proxies as well as to focus equally on the differences regarding the effect sizes of high-effort constructs to understand the mechanism in detail. Similarly, it could be helpful to understand how several firms in a BNDE setting are contributing to individuals' benefit and privacy risk perceptions – are the risks summed up (cf. Peter and Tarpey 1975), or is there a decreasing marginal risk (utility) function (cf. Tversky and Kahneman 1992)?

With the methodology applied in this study, it is also not possible to verify whether the decision-making process we assumed is really what individuals perform in their minds. We rather observe the final outcome of the decision-making process and the influence of the affective reaction on the disclosure decision. To verify the mechanism in detail, other approaches are necessary, e.g., functional magnetic resonance imaging could be helpful (cf. Gläscher et al. 2010). However, such disclosure situations are highly complex, cues can be very subtle, and negative outcomes, i.e., privacy invasions, happen often only after a longer period of time. Ergo, we think it is hard to examine the single steps in individuals' minds regarding such a decision process even with adequate procedures.

Another limitation is that we only examine a very small exchange network with only one certain firm order. There could be differences between BNDE settings that may be caused by the firm order in the exchange network: for instance, the affective reaction could mainly depend on the touchpoint firm (i.e., the firm to which the individual directly discloses) in the BNDE disclosure setting. This could mean that individuals' affective reaction would be altered as soon as the touchpoint firm changes despite the individuals still disclose the identical data to the exact same firms. This could either be as the first firm is so positively/negatively associated in the minds of individuals that the other firms in the network are negligible. Another possible mechanism could be based on anchor points, i.e., the first or the most prominent firm acts as anchor point and if the other firm in the BNDE network is better in terms of privacy (e.g., less risks) there is a privacy "gain" for the individuals while for the other case there is a privacy "loss" (cf. Tversky and Kahneman 1974). Thus, future studies should not only examine the firm order effect but additionally verify our results in a BNDE setting where the network consists of more than two firms.







Also, an unexamined possibility is that the firms in a data sharing network are not consciously noticed as distinct firms. This shall be briefly explained in more detail: we are fully aware that sometimes firms in a big data exchange network or even in its simplest instance, a data sharing cooperation between two firms, are not perceived as separate firms. This means individuals could perceive the whole data exchange network as "one firm" instead of as distinctive firms. This view could arise through firm characteristics, i.e., one firm is much bigger and more dominant compared to the other firms so that it outshines all other firms in the data exchange network. Another explanation could lie in the data disclosure setting itself, for example, the data exchange network could emphasize the network itself but not the included firms (e.g., a cooperation like Star Alliance does mention the firms that are part of the network but emphasizes primarily the network itself, cf. Star Alliance 2020). Thus, we easily can

imagine that there are certain factors like the network presentation or exceeding a certain threshold regarding the size of the firm, popularity of the firm, experience with the firm, or the perception of the firm that could lead individuals to an identical processing behavior like in a dyadic data disclosure setting. Future research could examine which factors increase individuals' perception of a data exchange network as "one firm".

In sum, there are many open issues for future research: verifying and improving the decision process model for individuals' disclosure decision-making developed in this study could increase knowledge on the role of low-effort processing in disclosure decisions. Also, unique peculiarities of BNDE settings are almost completely unexplored, which offers a practical and future-oriented research field as already many firms share their data with partners to be able to offer their services or to monetize the data (Hanafizadeh and Harati Nik 2020; Wixom 2014). This study examines differences in processing behavior when a BNDE disclosure setting is compared to an identical dyadic setting as a starting point for future research. However, there are many more, maybe even opposing, BNDE-related effects that could simultaneously occur and are unexplored, e.g., a firm-order respectively an anchoring effect.

## Appendix

**Table 5.** Construct measurement instruments.

<b>Affect (AFF)</b>	
AFF	Please indicate how you feel about the potential participation in this/these data collection/s.
Adapted from Shampanier et al. (2007); 5-Point Likert scale with anchors:	
 1 =  , 2 =  , 3 =  , 4 =  , 5 = 	
<b>Willingness to Disclose (WTD)</b>	
Adapted from Anderson and Agarwal (2011); 7-Point semantic differential with following anchors:	
To what extent would you be willing to disclose the required data in this/these data collection/s and thus participate in this/these data collection/s?	
WTD1	unlikely - likely
WTD2	not probable - probably
WTD3	unwilling - willing
<b>Perceived Privacy Risks (RISK)</b>	
Adapted from Dinev et al. (2013), Dinev and Hart (2006), Featherman and Pavlou (2003); 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
RISK1	It is very risky in this/these data collection/s to reveal personal information.
RISK2	The disclosure of personal information in this/these data collection/s is associated with a high potential risk of losing privacy.
RISK3	My disclosed personal information may be used improperly in this/these data collection/s.
RISK4	The disclosure of personal information in this/these data collection/s could cause many unexpected problems.
<b>Perceived Benefits (BENE)</b>	
Adapted from Voss et al. (2003); 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
The benefits I get from participating in this/these data collection/s, I will probably describe as ...	
BENE1	functional
BENE2	practical
BENE3	necessary
BENE4	helpful
<b>Trust (TRUST)</b>	
Adapted from Wirtz and Lwin (2009), Morgan and Hunt (1994); 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
TRUST1	I can rely on the fact that the data from this data collection is handled properly.
TRUST2	I believe that the companies involved have a high level of integrity.
TRUST3	I trust that the companies involved will act in my interest.
<b>Data Use Transparency (TRANS)</b>	
Adapted from Martin et al. (2016), Awad and Krishnan (2006); 7-Point semantic differential with following anchors:	
The handling of my data by the companies involved is	
TRANS1	unclear to me - clear to me
TRANS2	confusing - straightforward
TRANS3	difficult to understand - easy to understand
TRANS4	vague - transparent

The Effect of Data Sharing Between Firms

<b>Perceived Decision Complexity (DCOMP)</b>	
Adapted from Gupta et al. (2013), Maynard and Hakel (1997); 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
DC1	I found the decision-making process complex.
DC2	This decision-making was mentally demanding.
DC3	This decision-making process required a lot of thought.
DC4	I found the decision-making process difficult.
<b>Consumer Control (CONT)</b>	
Adapted from Martin et al. (2016), Mothersbaugh et al. (2012); Cronbach's $\alpha$ : .9; Composite-Reliability: .89; 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
CONT1	I believe that I have control over what happens to my data from this/these data collection/s.
CONT2	It is up to me how much the companies involved use my data from this data collection/s.
CONT3	I have a say in how my data from this/these data collection/s is used by the companies involved.
<b>Perceived Decision Uncertainty (DU)</b>	
Adapted from Pavlou et al. (2007), Torkzadeh and Dhillon (2002); 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
DU1	My decision to participate in this/these data disclosure/s involves a high degree of uncertainty.
DU2	The uncertainty in my decision to participate in this/these data disclosure/s is high.
DU3	I am exposed to many insecurities in my decision to participate in this/these data disclosure/s.
DU4	There is a high degree of uncertainty in my decision to participate in this/these data disclosure/s.
<b>Perceived Realism of the Scenario (REAL)</b>	
Adapted from Vogel and Paul (2015), 5-Point semantic scale with following anchors: How realistic do you think the situation described is?	
REAL	not realistic/realistic
<b>Global Information Privacy Concerns (GIPC)</b>	
Adapted from Malhotra et al. (2004), Smith et al. (1996); 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
GIPC1	Compared to others, I am more sensitive about the way online companies handle my personal information.
GIPC2	To me, it is the most important thing to keep my privacy intact from online companies.
GIPC3	I am concerned about threats to my personal privacy today.
<b>Privacy Concerns (PC)</b>	
Adapted from Dinev and Hart (2006), Culnan and Armstrong (1999), Smith et al. (1996); 7-Point Likert scale with anchors 1 = "not at all concerned" and 7 = "very concerned"	
PC1	I am concerned that the information I submit on the Internet could be misused.
PC2	I am concerned that a person can find private information about me on the Internet.
PC3	I am concerned about submitting information on the Internet, because of what others might do with it.
PC4	I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.
<b>Data Sensitivity (SENS)</b>	
Adapted from Xie et al. (2006), 7-Point semantic differential with following anchors: Please indicate how sensitive you think the data to be collected in this/these data collection/s?	
SENS	not sensitive at all – very sensitive

**Table 6.** Age, sex, and group distribution in the sample.

	18-29	30-39	40-49	50-59	60+	Sum (%male)
Group 1 (BNDE setting)	44	37	33	31	20	165 (55%)
Group 2 (Dyadic setting)	43	34	31	34	30	172 (48%)

The Effect of Data Sharing Between Firms

**Table 7.** Cronbach's  $\alpha$ , composite-reliability and average variance extracted (AVE).

Construct	Group 1			Group 2		
	Cronbach's $\alpha$	Composite-Reliability	Average Variance Extracted	Cronbach's $\alpha$	Composite-Reliability	Average Variance Extracted
AFF	1.000	1.000	1.000	1.000	1.000	1.000
AGE	1.000	1.000	1.000	1.000	1.000	1.000
BENE	.925	.947	.817	.881	.918	.738
CONT	.899	.937	.832	.840	.903	.757
SENS	1.000	1.000	1.000	1.000	1.000	1.000
WTD	.987	.992	.975	.982	.988	.965
RISK	.956	.968	.883	.933	.952	.833
PC	.925	.946	.814	.922	.944	.810
TRANS	.936	.954	.838	.923	.945	.812
TRUST	.924	.952	.868	.923	.951	.866
UNCERTAINTY	.942	.943	.804	.932	.933	.776
DCOMP	.883	.884	.657	.921	.922	.748
GIPC	.720	.842	.642	.805	.880	.711

**Table 8.** Loadings and cross loadings of the items in group 1.

	AFF	AGE	BENE	CONT	SENS	WTD	RISK	PC	TRANS	TRUST
AFF	1.000	-.287	.615	-.433	-.339	.782	-.591	-.160	.321	-.553
AGE	-.287	1.000	-.139	-.021	.032	-.166	.039	-.178	.004	-.117
WTD1	.776	-.185	.655	-.493	-.397	.989	-.655	-.279	.370	-.583
WTD2	.767	-.166	.666	-.509	-.404	.990	-.649	-.275	.375	-.598
WTD3	.774	-.140	.674	-.499	-.403	.984	-.675	-.268	.376	-.615
CONT1	.417	-.101	.596	.914	-.117	.494	-.436	-.184	.443	.672
CONT2	.402	.052	.547	.885	-.107	.399	-.363	-.277	.389	.539
CONT3	.368	.006	.590	.936	-.071	.483	-.358	-.272	.429	.599
BENE1	.602	-.173	.929	.525	-.310	.641	-.534	-.101	.362	.609
BENE2	.582	-.144	.931	.530	-.271	.642	-.486	-.156	.371	.612
BENE3	.511	-.052	.834	.678	-.160	.549	-.419	-.189	.380	.601
BENE4	.524	-.123	.917	.580	-.247	.597	-.469	-.078	.414	.583
RISK1	-.575	.023	-.527	-.381	.437	-.667	.951	.333	-.313	-.544
RISK2	-.595	.038	-.538	-.422	.489	-.677	.951	.329	-.333	-.581
RISK3	-.508	.065	-.461	-.389	.390	-.566	.921	.358	-.344	-.583
RISK4	-.539	.021	-.458	-.400	.435	-.594	.935	.339	-.325	-.560
SENS	-.339	.032	-.277	-.107	1.000	-.407	.467	.228	-.203	-.277
PC1	-.162	-.135	-.152	-.236	.237	-.284	.314	.900	-.257	-.317
PC2	-.125	-.218	-.061	-.122	.093	-.175	.189	.845	-.114	-.170
PC3	-.136	-.194	-.074	-.222	.235	-.220	.326	.924	-.158	-.216
PC4	-.149	-.132	-.191	-.320	.220	-.290	.411	.938	-.227	-.386
TRANS1	.259	-.011	.363	.363	-.175	.306	-.259	-.077	.907	.452
TRANS2	.276	.008	.346	.414	-.157	.319	-.317	-.252	.927	.520
TRANS3	.319	-.004	.398	.405	-.177	.363	-.308	-.261	.906	.518
TRANS4	.313	.020	.424	.496	-.228	.386	-.382	-.199	.921	.590
TRUST1	.531	-.130	.578	.673	-.260	.574	-.600	-.268	.492	.935
TRUST2	.476	-.110	.628	.559	-.209	.514	-.535	-.266	.528	.929
TRUST3	.533	-.087	.654	.621	-.299	.603	-.548	-.356	.581	.931

The Effect of Data Sharing Between Firms

**Table 9.** Loadings and cross loadings of the items in group 2.

	AFF	AGE	BENE	CONT	SENS	WTD	RISK	PC	TRANS	TRUST
AFF	1.000	-.107	.431	.387	-.316	.685	-.613	-.273	.364	.464
AGE	-.107	1.000	-.207	-.023	-.049	-.021	.007	-.006	-.028	-.006
WTD1	.684	-.027	.594	.372	-.388	.986	-.679	-.353	.427	.490
WTD2	.677	-.030	.618	.392	-.404	.987	-.678	-.338	.421	.495
WTD3	.659	-.005	.569	.393	-.368	.975	-.684	-.333	.425	.504
CONT1	.380	-.037	.434	.875	.043	.368	-.309	-.107	.366	.553
CONT2	.340	.007	.369	.882	-.097	.355	-.316	-.155	.341	.472
CONT3	.281	-.033	.402	.852	-.013	.293	-.215	-.061	.337	.450
BENE1	.446	-.219	.905	.441	-.108	.617	-.364	-.083	.274	.421
BENE2	.375	-.295	.897	.328	-.030	.546	-.354	-.172	.319	.359
BENE3	.293	.044	.756	.443	-.058	.405	-.274	-.072	.275	.305
BENE4	.343	-.187	.870	.391	-.051	.475	-.327	-.174	.255	.315
RISK1	-.535	.015	-.307	-.274	.410	-.620	.922	.458	-.496	-.442
RISK2	-.554	-.006	-.363	-.333	.468	-.680	.920	.442	-.474	-.477
RISK3	-.602	-.004	-.398	-.350	.331	-.610	.885	.423	-.506	-.545
RISK4	-.545	.020	-.344	-.233	.426	-.618	.924	.513	-.478	-.494
SENS	-.316	-.049	-.074	-.025	1.000	-.394	.448	.316	-.201	-.132
PC1	-.338	.020	-.187	-.163	.306	-.377	.492	.882	-.362	-.266
PC2	-.124	-.032	-.058	-.070	.175	-.238	.334	.844	-.233	-.153
PC3	-.215	-.031	-.120	-.072	.285	-.310	.439	.945	-.329	-.233
PC4	-.262	.008	-.132	-.134	.340	-.301	.510	.924	-.345	-.283
TRANS1	.327	-.034	.290	.398	-.134	.398	-.474	-.299	.908	.572
TRANS2	.314	-.015	.272	.289	-.206	.408	-.510	-.302	.914	.543
TRANS3	.251	.013	.239	.296	-.119	.307	-.400	-.244	.889	.469
TRANS4	.398	-.053	.357	.443	-.245	.422	-.525	-.428	.892	.618
TRUST1	.435	-.041	.390	.502	-.067	.457	-.499	-.231	.590	.923
TRUST2	.440	.005	.368	.538	-.126	.463	-.495	-.238	.527	.951
TRUST3	.420	.018	.394	.546	-.172	.488	-.504	-.275	.605	.918

**Table 10.** Supplementary item loadings for constructs not included in the SEM.

	Loading Group 1	Loading Group 2
DUNC1	.908	.790
DUNC2	.919	.878
DUNC3	.832	.914
DUNC4	.925	.935
DCOMP1	.752	.782
DCOMP2	.860	.920
DCOMP3	.861	.902
DCOMP4	.763	.848
GIPC1	.812	.753
GIPC2	.879	.898
GIPC3	.704	.871

**Table 11.** Correlations between constructs and square root of the AVEs on the diagonal (group 1).

	AFF	AGE	BENE	CONT	SENS	WTD	RISK	PC	TRANS	TRUST
AFF	1.000									
AGE	-.287	1.000								
BENE	.615	-.139	.904							
CONT	.433	-.021	.635	.912						
SENS	-.339	.032	-.277	-.107	1.000					
WTD	.782	-.166	.673	.507	-.407	.988				
RISK	-.591	.039	-.529	-.424	.467	-.668	.939			
PC	-.160	-.178	-.143	-.265	.228	-.277	.361	.902		
TRANS	.321	.004	.421	.462	-.203	.378	-.350	-.219	.916	
TRUST	.553	-.117	.665	.665	-.277	.606	-.603	-.319	.572	.932

The Effect of Data Sharing Between Firms

**Table 12.** Correlations between constructs and square root of the AVEs on the diagonal (group 2).

	AFF	AGE	BENE	CONT	SENS	WTD	RISK	PC	TRANS	TRUST
AFF	1.000									
AGE	-.107	1.000								
BENE	.431	-.207	.859							
CONT	.387	-.023	.462	.870						
SENS	-.316	-.049	-.074	-.025	1.000					
WTD	.685	-.021	.605	.392	-.394	.982				
RISK	-.613	.007	-.387	-.326	.448	-.692	.913			
PC	-.273	-.006	-.145	-.127	.316	-.347	.503	.900		
TRANS	.364	-.028	.325	.401	-.201	.432	-.535	-.360	.901	
TRUST	.464	-.006	.412	.569	-.132	.505	-.537	-.267	.617	.931

**Table 13.** Heterotrait-Monotrait Ratio (HTMT) of the constructs in group 1.

	AFF	AGE	BENE	CONT	SENS	WTD	RISK	PC	TRANS
AGE	.287								
BENE	.639	.141							
CONT	.457	.061	.701						
SENS	.339	.032	.285	.114					
WTD	.787	.167	.704	.534	.409				
RISK	.604	.040	.560	.456	.477	.686			
PC	.164	.195	.144	.277	.226	.280	.366		
TRANS	.329	.012	.451	.498	.208	.390	.366	.223	
TRUST	.573	.122	.721	.723	.286	.633	.641	.325	.611

**Table 14.** Heterotrait-Monotrait Ratio (HTMT) of the constructs in group 2.

	AFF	AGE	BENE	CONT	SENS	WTD	RISK	PC	TRANS
AGE	.107								
BENE	.452	.231							
CONT	.418	.032	.541						
SENS	.316	.049	.077	.064					
WTD	.691	.021	.640	.428	.397				
RISK	.634	.013	.423	.363	.464	.723			
PC	.272	.026	.157	.135	.320	.358	.531		
TRANS	.372	.033	.358	.448	.203	.448	.570	.375	
TRUST	.483	.024	.452	.641	.136	.530	.578	.281	.661

**Table 15.** Inner VIF values of the constructs for both groups.

	Group 1			Group 2		
	BENE	WTD	RISK	BENE	WTD	RISK
AFF	1	2.133	1.440	1	1.839	1.314
AGE		1.187			1.072	
BENE		2.489			1.521	
CONT		2.185			1.679	
SENS		1.349			1.334	
WTD						
RISK		2.228			2.606	
PC		1.288	1.114		1.394	1.110
TRANS		1.535			1.842	
TRUST		2.981	1.562		2.246	1.309

**Table 16.** MICOM step 2: test for compositional invariance between the groups.

	AFF	AGE	BENE	CONT	SENS	WTD	RISK	PC	TRANS	TRUST
p-value	.532	.392	.278	.270	.114	.138	.171	.601	.287	.559

**Table 17.** R<sup>2</sup> results and group comparison results.

	R <sup>2</sup> <sub>Group1</sub> (SD)	R <sup>2</sup> <sub>Group2</sub> (SD)	R <sup>2</sup> <sub>Group1</sub> - R <sup>2</sup> <sub>Group2</sub>	PLS-MGA p-value two-tailed / one-tailed	Permutation p-value two-tailed / one-tailed
BENE	0.379 (.072)	0.185 (.051)	0.193	.030 / .015	.033 / .019
WTD	0.722 (.030)	0.693 (.040)	0.029	.570 / .285	.568 / .291
RISK	0.494 (.066)	0.551 (.046)	-0.057	.485 / .757	.503 / .246

**Table 18.** Bootstrapped path coefficient ( $\beta$ ) results.

Effect	Group 1				Group 2			
	$\beta$	Bootstrap $\hat{O}(\beta)$	Bootstrap SD	p- value	$\beta$	Bootstrap $\hat{O}(\beta)$	Bootstrap SD	p- value
AFF -> BENE	.615	.616	.059	.000	.431	.435	.059	.000
AFF -> WTD	.477	.475	.067	.000	.306	.300	.060	.000
AFF -> RISK	-.376	-.376	.071	.000	-.403	-.401	.058	.000
AGE -> WTD	-.001	-.003	.047	.984	.080	.078	.041	.049
BENE -> WTD	.207	.207	.075	.006	.355	.352	.061	.000
CONT -> WTD	.052	.056	.067	.434	-.016	-.013	.059	.793
SENS -> WTD	-.075	-.073	.047	.114	-.130	-.135	.049	.008
RISK -> WTD	-.185	-.188	.073	.012	-.276	-.277	.083	.001
PC -> WTD	-.069	-.069	.046	.139	-.020	-.018	.054	.718
PC -> RISK	.194	.198	.057	.001	.322	.325	.065	.000
TRANS -> WTD	.015	.021	.055	.788	-.002	-.002	.069	.973
TRUST -> WTD	.008	-.002	.079	.915	.057	.057	.067	.390
TRUST -> RISK	-.333	-.331	.085	.000	-.264	-.264	.078	.001

**Table 19.** Bootstrapped effect size ( $f^2$ ) results.

Effect	Group 1			Group 2		
	$f^2$	Bootstrap $\hat{O}(f^2)$	Bootstrap SD	$f^2$	Bootstrap $\hat{O}(f^2)$	Bootstrap SD
AFF -> BENE	.610	.643	.197	.228	.244	.081
AFF -> WTD	.383	.390	.116	.166	.169	.071
AFF -> RISK	.194	.207	.087	.275	.286	.096
AGE -> WTD	.000	.007	.010	.020	.025	.023
BENE -> WTD	.062	.069	.045	.270	.275	.103
CONT -> WTD	.004	.012	.016	.000	.007	.010
SENS -> WTD	.015	.020	.021	.041	.052	.036
RISK -> WTD	.055	.065	.046	.095	.106	.063
PC -> WTD	.013	.020	.021	.001	.007	.010
PC -> RISK	.067	.077	.044	.208	.225	.096
TRANS -> WTD	.001	.008	.011	.000	.009	.012
TRUST -> WTD	.000	.007	.010	.005	.011	.014
TRUST -> RISK	.141	.154	.085	.118	.131	.075

## References

- Alhakami, A. S., and Slovic, P. 1994. "A Psychological Study of the Inverse Relationship Between Perceived Risk and Perceived Benefit," *Risk Analysis* (14:6), pp. 1085–1096.
- Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339–370.
- Awad, N. F., and 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), pp. 13–28.
- Bagozzi, R. P., and Yi, Y. 1989. "On the Use of Structural Equation Models in Experimental Designs," *Journal of Marketing Research* (26:3), pp. 273–284.
- Bagozzi, R. P., and Yi, Y. 2012. "Specification, Evaluation, and Interpretation of Structural Equation Models," *Journal of the Academy of Marketing Science* (40:1), pp. 8–34.

- Bagozzi, R. P., Yi, Y., and Phillips, L. W. 1991. "Assessing Construct Validity in Organizational Research," *Administrative Science Quarterly* (36:3), p. 421.
- Bal, G. 2014. "Designing Privacy Indicators for Smartphone App Markets: A New Perspective on the Nature of Privacy Risks of Apps," *AMCIS 2014 Proceedings*.
- Ball, D., Coelho, P. S., and Vilares, M. J. 2006. "Service Personalization and Loyalty," *Journal of Services Marketing* (20:6), Emerald Group Publishing Limited, pp. 391–403.
- Bansal, G., Zahedi, F. "Mariam," and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), pp. 138–150.
- Baumeister, R. F., Vohs, K. D., Nathan DeWall, C., and Zhang, L. 2007. "How Emotion Shapes Behavior: Feedback, Anticipation, and Reflection, Rather Than Direct Causation," *Personality and Social Psychology Review* (11:2), SAGE Publications Inc, pp. 167–203.
- Bidler, M., Schumann, J. H., and Widjaja, T. 2018. "Challenging the Cognitive Privacy Calculus: Affective Reactions in Consumers' Privacy Related Decision Making.," in *SERVSIG Proceedings*, Paris, 06. -- 16.06, pp. 839–844.
- Books, A., and Goffman, E. 1969. *The Presentation of Self in Everyday Life*, London: Allen Lane.
- Camerer, C., and Weber, M. 1991. "Recent Developments in Modelling Preferences: Uncertainty and Ambiguity," *Manuskripte Aus Den Instituten für Betriebswirtschaftslehre Der Universität Kiel* (275).
- Chaudhuri, A. 2002. "A Study of Emotion and Reason in Products and Services," *Journal of Consumer Behaviour* (1:3), pp. 267–279.
- Chin, W. W., and Dibbern, J. 2010. "A Permutation Based Procedure for Multi-Group Pls Analysis: Results of Test of Differences on Simulated Data and a Cross Cultural Analysis of the Sourcing of Information System Services between Germany and the USA," in *Handbook of Partial Least Squares*, Springer, pp. 501–517.
- Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, (2<sup>nd</sup> ed.), Hillsdale, N.J: L. Erlbaum Associates.
- Cohen, P. 2006. *Empirical Methods for Artificial Intelligence*, p. 128.
- Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104–115.
- Daw, N. D. 2012. "Model-Based Reinforcement Learning as Cognitive Search: Neurocomputational Theories," *Cognitive Search: Evolution, Algorithms and the Brain*, pp. 195–208.
- Daw, N. D., Niv, Y., and Dayan, P. 2005. "Uncertainty-Based Competition between Prefrontal and Dorsolateral Striatal Systems for Behavioral Control," *Nature Neuroscience* (8:12), pp. 1704–1711.
- Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61–80.
- Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box," *Information Systems Research* (26:4), pp. 639–655.
- Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts," *European Journal of Information Systems* (22:3), pp. 295–316.
- Ellsberg, D. 1961. "Risk, Ambiguity, and the Savage Axioms," *The Quarterly Journal of Economics* (75:4), p. 643.
- Epstein, S. 1994. "Integration of the Cognitive and the Psychodynamic Unconscious," *American Psychologist* (49:8), pp. 709–724.
- Ermakova, T., Baumann, A., Fabian, B., and Krasnova, H. 2014. "Privacy Policies and Users' Trust: Does Readability Matter?," *AMCIS 2014 Proceedings*.
- Evans, J. S. B., and Stanovich, K. E. 2013. "Dual-Process Theories of Higher Cognition: Advancing the Debate," *Perspectives on Psychological Science* (8:3), SAGE Publications Inc, pp. 223–241.
- Facebook. 2021. *Facebooks Earnings Presentation Q4 2020*. URL: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (accessed: 18.02.2021).
- Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451–474.
- Finucane, M. L., Alhakami, A., Slovic, P., and Johnson, S. M. 2000. "The Affect Heuristic in Judgments of Risks and Benefits," *Journal of Behavioral Decision Making* (13:1), p. 17.
- Fischer, P. 2011. "Selective Exposure, Decision Uncertainty, and Cognitive Economy: A New Theoretical Perspective on Confirmatory Information Search: Selective Exposure and Cognitive Economy," *Social and Personality Psychology Compass* (5:10), pp. 751–762.
- Fisher, R. A. 1935. "The Design of Experiments."



- Forgas, J. P. 1995. "Mood and Judgment: The Affect Infusion Model (AIM).," *Psychological Bulletin* (117:1), pp. 39–66.
- Forgas, J. P. 2008. "Affect and Cognition," *Perspectives on Psychological Science* (3:2), SAGE Publications Inc, pp. 94–101.
- Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39–50.
- Furnell, S., and Phippen, A. 2012. "Online Privacy: A Matter of Policy?," *Computer Fraud & Security* (2012:8), pp. 12–18.
- Gambetta, D. 2009. "Signaling," in *The Oxford Handbook of Analytical Sociology*, pp. 168–194.
- Garbarino, E. C., and Edell, J. A. 1997. "Cognitive Effort, Affect, and Choice," *Journal of Consumer Research* (24:2), pp. 147–158.
- Gartner. 2013. "Information Sharing as an Industry Imperative to Improve Security," *Gartner*. URL: <https://www.gartner.com/en/documents/2518715/information-sharing-as-an-industry-imperative-to-improve> (accessed: 13.08.2019).
- Gefen, D., Straub, D., and Boudreau, M.-C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4, Article 7).
- "General Data Protection Regulation (GDPR)." 2016. *Official Journal of the European Union*. URL: <https://gdpr-info.eu/> (accessed: 22.11.2019).
- Gläscher, J., Daw, N., Dayan, P., and O'Doherty, J. P. 2010. "States versus Rewards: Dissociable Neural Prediction Error Signals Underlying Model-Based and Model-Free Reinforcement Learning," *Neuron* (66:4), pp. 585–595.
- Goes, P. B. 2013. "EDITOR'S COMMENTS. Information Systems Research and Behavioral Economics," *MIS Quarterly* (37:3), pp. iii–vii.
- Great Britain Food Standards Agency. 2008. *Food Standards Agency Annual Report 2007/08*, London: Stationery Office.
- Gupta, A., Li, H., and Sharda, R. 2013. "Should I Send This Message? Understanding the Impact of Interruptions, Social Hierarchy and Perceived Task Complexity on User Performance and Perceived Workload," *Decision Support Systems* (55:1), pp. 135–145.
- Hair, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2016. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, SAGE Publications.
- Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed a Silver Bullet," *Journal of Marketing Theory and Practice* (19:2), pp. 139–152.
- Hair, J. F., Sarstedt, M., Ringle, C. M., and Gudergan, S. P. 2017. *Advanced Issues in Partial Least Squares Structural Equation Modeling*, SAGE Publications.
- Hanafizadeh, P., and Harati Nik, M. R. 2020. "Configuration of Data Monetization: A Review of Literature with Thematic Analysis," *Global Journal of Flexible Systems Management* (21:1), pp. 17–34.
- Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 115–135.
- Henseler, J., Ringle, C. M., and Sarstedt, M. 2016. "Testing Measurement Invariance of Composites Using Partial Least Squares," *International Marketing Review* (33:3), (R. R. Sinkovics, Ruy-Jer "Bryan" Jean, ed.), pp. 405–431.
- Henseler, J., Ringle, C. M., and Sinkovics, R. R. (eds.). 2009. *Advances in International Marketing*, (Vol. 20), Advances in International Marketing, Bingley: Emerald Group Publishing.
- Ho, V. 2018. "Facebook's Privacy Problems: A Roundup," *The Guardian*. URL: <https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup> (accessed: 31.07.2019).
- Hong, W., and Thong, J. Y. L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275–298.
- Kahneman, D. 2003. "Maps of Bounded Rationality: Psychology for Behavioral Economics," *American Economic Review* (93:5), pp. 1449–1475.
- Kahneman, D. 2012. *Thinking, Fast and Slow*, London: Penguin Books.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607–635.
- Keith, Thompson, and Greer. 2012. *Examining the Rationality of Information Disclosure through Mobile Devices*, presented at the Thirty Third International Conference on Information Systems, Orlando, Florida.

- Klaczynski, P. A. 2001. "Framing Effects on Adolescent Task Representations, Analytic and Heuristic Processing, and Decision Making Implications for the Normative/Descriptive Gap," *Applied Developmental Psychology*, p. 21.
- Komiak, S. Y. X., and Benbasat, I. 2006. "The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents," *MIS Quarterly* (30:4), Management Information Systems Research Center, University of Minnesota, pp. 941–960.
- Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22–42.
- Lei, D., and Slocum Jr., J. W. 1992. "Global Strategy, Competence-Building and Strategic Alliances," *California Management Review* (35:1), pp. 81–97.
- Li, H., Luo, X. (Robert), Zhang, J., and Xu, H. 2017. "Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors," *Information & Management* (54:8), pp. 1012–1022.
- Li, H., Sarathy, R., and Xu, H. 2011. "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51:3), pp. 434–445.
- Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), pp. 471–481.
- Loewenstein, G. F., Weber, E. U., Hsee, C. K., and Welch, N. 2001. "Risk as Feelings.," *Psychological Bulletin* (127:2), pp. 267–286.
- Madsbjerg, S. 2017. "It's Time to Tax Companies for Using Our Personal Data," *The New York Times*. URL: <https://www.nytimes.com/2017/11/14/business/dealbook/taxing-companies-for-using-our-personal-data.html> (accessed: 13.08.2019).
- Maglio, S. J., and Reich, T. 2019. "Feeling Certain: Gut Choice, the True Self, and Attitude Certainty.," *Emotion* (19:5), pp. 876–888.
- Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355.
- Martin, K. D., Borah, A., and Palmatier, R. W. 2016. "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing* (81:1), pp. 36–58.
- Mason, J. C. 1993. "Strategic Alliances: Partnering for Success," *Management Review* (82:5).
- Maynard, D. C., and Hakel, M. D. 1997. "Effects of Objective and Subjective Task Complexity on Performance," *Human Performance* (10:4), pp. 303–330.
- Mittal, B., and Lassar, W. M. 1996. "The Role of Personalization in Service Encounters," *Journal of Retailing* (72:1), pp. 95–109.
- Morgan, R. M., and Hunt, S. D. 1994. "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing* (58:3), pp. 20–38.
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research* (15:1), pp. 76–98.
- O'Neill, P. H. 2021. "Google Says It's Too Easy for Hackers to Find New Security Flaws," *MIT Technology Review*. URL: <https://www.technologyreview.com/2021/02/03/1017242/google-project-zero-day-flaw-security> (accessed: 05.03.2021).
- Osberg, T. M., and Shrauger, J. S. 1986. "Self-Prediction: Exploring the Parameters of Accuracy.," *Journal of Personality and Social Psychology* (51:5), pp. 1044–1057.
- Pavlou, Liang, and Xue. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), p. 105.
- Paypal. 2018. "Paypal's Third-Party List." URL: <https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list> (accessed: 09.07.2018).
- Peter, J. P., and Tarpey, L. X. 1975. "A Comparative Analysis of Three Consumer Decision Strategies," *Journal of Consumer Research* (2:1), pp. 29–37.
- Petty, R. E., Wegener, D. T., and White, P. H. 1998. "Flexible Correction Processes in Social Judgment: Implications for Persuasion," *Social Cognition* (16:1), pp. 93–113.
- Pezzulo, G., Rigoli, F., and Chersi, F. 2013. "The Mixed Instrumental Controller: Using Value of Information to Combine Habitual Choice and Mental Simulation," *Frontiers in Psychology* (4).
- Rangel, A., Camerer, C., and Montague, P. R. 2008. "A Framework for Studying the Neurobiology of Value-Based Decision Making.," *Nature Reviews. Neuroscience* (9:7), pp. 545–556.
- Redish, A. D., Jensen, S., and Johnson, A. 2008. "A Unified Framework for Addiction: Vulnerabilities in the Decision Process," *Behavioral and Brain Sciences* (31:04).
- Richards, L. E., and Byrd, J. 1996. "Algorithm AS 304: Fisher's Randomization Test for Two Small Independent Samples," *Applied Statistics* (45:3), p. 394.

- Satariano, A. 2020. "E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact," *The New York Times*. URL: <https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html> (accessed: 05.03.2021).
- Schaub, F., Balebako, R., Durity, A. L., and Cranor, L. F. 2015. "A Design Space for Effective Privacy Notices\*," in *The Cambridge Handbook of Consumer Privacy* (1st ed.), E. Selinger, J. Polonetsky, and O. Tene (eds.), Cambridge University Press, pp. 365–393.
- Shampanier, K., Mazar, N., and Ariely, D. 2007. "Zero as a Special Price: The True Value of Free Products," *Marketing Science* (26:6), pp. 742–757.
- Slooman, S. A. 1996. *The Empirical Case for Two Systems of Reasoning*, (119:1), pp. 3–22.
- Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. 2004. "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality," *Risk Analysis* (24:2), pp. 311–322.
- Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. 2007. "The Affect Heuristic," *European Journal of Operational Research* (177:3), pp. 1333–1352.
- Slovic, P., Finucane, M., Peters, E., and MacGregor, D. G. 2002. "Rational Actors or Rational Fools: Implications of the Affect Heuristic for Behavioral Economics," *The Journal of Socio-Economics* (31:4), pp. 329–342.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1016.
- Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167–196.
- Smith, M. D. 2011. "The Ecological Role of Climate Extremes: Current Understanding and Future Prospects," *Journal of Ecology* (99:3), pp. 651–655.
- Smucker, M. D., Allan, J., and Carterette, B. 2007. "A Comparison of Statistical Significance Tests for Information Retrieval Evaluation," in *Proceedings of the Sixteenth ACM Conference on Information and Knowledge Management*, Lisbon, Portugal: ACM Press, pp. 623–632.
- Solon, O. 2018. "Facebook Says Cambridge Analytica May Have Gained 37m More Users' Data," *The Guardian*, URL: <http://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought> (accessed: 23.04.2018).
- Spotify. 2018. "Spotify Privacy Policy," URL: <https://www.spotify.com/us/legal/privacy-policy/>, (accessed: 23.04.2018).
- Star Alliance. 2020. "Homepage." URL: <https://www.staralliance.com/en> (accessed: 09.03.2020).
- Stuedner, T., Widjaja, T., and Schumann, J. H. 2019. "An Exploratory Study of Risk Perception for Data Disclosure to a Network of Firms," in *Human Practice. Digital Ecologies. Our Future*, Siegen: Academic Press, pp. 1352–1357.
- Thatcher, J. B., and Perrewe, P. L. 2002. "An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy," *MIS Quarterly* (26:4), p. 381.
- Torkzadeh, G., and Dhillon, G. 2002. "Measuring Factors That Influence the Success of Internet Commerce," *Information Systems Research* (13:2), p. 19.
- Tormala, Z. L., Clarkson, J. J., and Henderson, M. D. 2011. "Does Fast or Slow Evaluation Foster Greater Certainty?," *Personality and Social Psychology Bulletin* (37:3), pp. 422–434.
- Tversky, A., and Kahneman, D. 1974. "Judgment under Uncertainty: Heuristics and Biases," *Science* (185:4157), pp. 1124–1131.
- Tversky, A., and Kahneman, D. 1992. "Advances in Prospect Theory: Cumulative Representation of Uncertainty," *Journal of Risk and Uncertainty* (5:4), pp. 297–323.
- Tversky, A., and Koehler, D. J. 1994. "Support Theory: A Nonextensional Representation of Subjective Probability," *American Psychological Association* (101:4), pp. 547–567.
- Vaidhyanathan, S. 2018. "Violating Our Privacy Is in Facebook's DNA | Siva Vaidhyanathan," *The Guardian*. URL: <https://www.theguardian.com/commentisfree/2018/dec/20/facebook-violating-privacy-mark-zuckerberg> (accessed: 31.07.2019).
- Valentino-DeVries, J., Singer, N., Keller, M. H., and Krolik, A. 2018. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times*. URL: <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> (accessed: 05.03.2019).
- Varian, H. R. 2016. *Grundzüge der Mikroökonomik*, (9th updated and expanded edition.), Berlin/Boston: De Gruyter Oldenbourg.
- Vogel, J., and Paul, M. 2015. "One Firm, One Product, Two Prices\_ Channel-Based Price Differentiation and Customer Retention," *Journal of Retailing and Consumer Services* (27), pp. 126–139.
- Voss, K. E., Spangenberg, E. R., and Grohmann, B. 2003. "Measuring the Hedonic and Utilitarian Dimensions of Consumer Attitude," *Journal of Marketing Research* (40:3), pp. 310–320.

*The Effect of Data Sharing Between Firms*

- Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157–174.
- Wirtz, J., and Lwin, M. O. 2009. "Regulatory Focus Theory, Trust, and Privacy Concern," *Journal of Service Research* (12:2), pp. 190–207.
- Wixom, B. H. 2014. "Cashing In on Your Data," *MIT CISR* (14:8). URL: [https://cistr.mit.edu/publication/2014\\_0801\\_DataMonetization\\_Wixom](https://cistr.mit.edu/publication/2014_0801_DataMonetization_Wixom) (accessed: 13.08.2019).
- Wold, H. 1966. "Estimation of Principal Components and Related Models by Iterative Least Squares," *Multivariate Analysis*, pp. 391–420.
- Xie, E., Teo, H.-H., and Wan, W. 2006. "Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behavior," *Marketing Letters* (17:1), pp. 61–74.
- Xu, H., Teo, H.-H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk," in *ICIS 2005 Proceedings*, pp. 897–910.
- Zahavi, A. 2008. "The Handicap Principle and Signalling in Collaborative Systems," *Sociobiology of Communication*, pp. 1–10.
- Zajonc, R. B. 1980. "Feeling and Thinking: Preferences Need No Inferences," *American Psychologist* (35:2), pp. 151–175.

## **Consumer Groups and Their Risk Perception in a Data Sharing Cooperation Between Two Firms**

**Author:** Tobias Steudner, University of Passau, Germany

**Presented at:** Conference of the International Telecommunications Society, 2020, online conference due to COVID-19

**Published in:** Proceedings of the Conference of the International Telecommunications Society, 2020

### **Abstract**

Privacy research has paid little attention to consequences and peculiarities when firms share consumer data with a third party. Thus, we explore consumers' distinct standpoints regarding an impact on their perceived privacy risks due to a data sharing cooperation between two firms. We identify three consumer groups, whereby two of them see their privacy risks affected (either increased or decreased) and the third consumer group sees their privacy risks not affected due to a data sharing cooperation between two firms. We show that this special third group does not intensively deal with privacy related issues in this situation, which results in lower perceived privacy risks and a higher willingness to disclose personal data compared to the two other consumer groups. We show that this group effect on willingness to disclose even holds when controlling for effects of consumers' privacy concerns and their perceived benefits. Furthermore, this effect is fully mediated by consumers' perceived privacy risks. Our study provides first insights into different consumer groups and its characteristics in a data disclosure setting in which firms have a data sharing cooperation. Therefore, this work allows future research to apply a refined view on consumers, especially in such complex data disclosure settings.

## **CONSUMER GROUPS AND THEIR RISK PERCEPTION IN A DATA SHARING COOPERATION BETWEEN TWO FIRMS**

Tobias Steudner

University of Passau, Chair of Business Information Systems, Passau, Germany, tobias.steudner@uni-passau.de

*Abstract: Privacy research has paid little attention to consequences and peculiarities when firms share consumer data with a third party. Thus, we explore consumers' distinct standpoints regarding an impact on their perceived privacy risks due to a data sharing cooperation between two firms. We identify three consumer groups, whereby two of them see their privacy risks affected (either increased or decreased) and the third consumer group sees their privacy risks not affected due to a data sharing cooperation between two firms. We show that this special third group does not intensively deal with privacy related issues in this situation, which results in lower perceived privacy risks and a higher willingness to disclose personal data compared to the two other consumer groups. We show that this group effect on willingness to disclose even holds when controlling for effects of consumers' privacy concerns and their perceived benefits. Furthermore, this effect is fully mediated by consumers' perceived privacy risks. Our study provides first insights into different consumer groups and its characteristics in a data disclosure setting in which firms have a data sharing cooperation. Therefore, this work allows future research to apply a refined view on consumers, especially in such complex data disclosure settings.*

*Keywords: Privacy Risk Perception, Data Sharing Cooperation, Privacy Concerns, Privacy Calculus.*

## 1 Introduction

Nowadays, privacy becomes more and more important (Gartner, 2019): many news about privacy intrusions due to legal but still privacy intrusive data policies of firms (e.g., by sharing personal consumer data to other firms), or due to illegal data breaches or misuses appear in the newscasts (e.g., Techcrunch.com, 2018; Solon, 2018; Ho, 2018). Thus, consumers' privacy concerns and their privacy risk perception continue to be key topics, not only for privacy research but also for firms' data handling strategies, for example, regarding consumer data sharing with a third party (Ho, 2018; Vaidhyanathan, 2018; Gartner, 2019). Nevertheless, most studies in the privacy context just examine data disclosure settings in which consumers disclose their personal data only to a single firm which does not share this data with a third party (e.g., Bansal, Zahedi and Gefen, 2010; H. Li, Sarathy and Xu, 2011). However, more and more firms started to deviate from this dyadic consumer-firm relationship and began a data sharing cooperation with other firms (Smith, Dinev and Xu, 2011; Madsbjerg, 2017; Gartner, 2018). An example for a data sharing cooperation between two firms is illustrated by the recently held beach volleyball world cup: to watch the matches at home via stream consumers could either pay 4.99 Euro to the streaming provider or allow the streaming provider to share their personal data (name and e-mail address) to a firm in the banking sector (Augsburger Allgemeine, 2019; Beach Majors GmbH, 2019). Even when a disclosure setting with a data sharing cooperation between firms is examined in the literature, almost no study considers the peculiarities of such a disclosure setting (e.g., Angst and Agarwal, 2009). The importance of examining peculiarities in data sharing cooperation increased when the General Data Protection Regulation (GDPR) came into force in May, 2018. The GDPR requires a high data handling transparency and firms are forced to inform consumers intelligibly about data handling procedures as well as their data sharing cooperation (*General Data Protection Regulation*, 2016). This means, consumers are highly informed about firms' data sharing cooperations nowadays, which makes it necessary to examine peculiarities of such data sharing settings in more detail in future studies.

To adequately understand the peculiarities of a more complex disclosure setting with a data sharing cooperation, first, it is necessary to identify consumer groups and their characteristics, especially with respect to their privacy risk perception towards a data sharing cooperation between firms. As it is intuitive to answer how consumers' positive respectively negative views on a data sharing cooperation regarding their privacy risks will influence their risk perception and their willingness to disclose data, we focus on the third consumer group: on those consumers who see their privacy risks not affected through a data sharing cooperation between firms, as it is not intuitive to answer what this means for their risk perception and their willingness to disclose data. This leads to the following two research questions:

1) *Are there consumer groups with distinct perceptions of a data sharing cooperation between two firms?* 2) *What are the differences between consumers who see their privacy risks not affected due to a data sharing cooperation and consumers who see their privacy risks affected?*

To this end, we compare these consumer groups, i.e., consumers who think their privacy risks increase ("risks increase"-group), decrease ("risks decrease"-group) with consumers who see their privacy risks unaffected ("unreflected"-group) due to a data sharing cooperation between two firms, regarding their perceived privacy risks and their willingness to disclose data and its influencing factors in such a data disclosure setting. For this comparison we use Fisher's permutation test and additionally regression analyses to verify the effect based on consumers' distinct standpoints (displayed by consumers' group) in more detail.

We obtain interesting results, as consumers who do not see their privacy risks affected have experienced the least privacy invasions, used the least mental effort to assess their privacy risks and dealt least intensively with privacy issues in this situation. Consumers in this group also have a significant lower perception of privacy risks and a higher willingness to disclose than other consumers, even compared to consumers who see their privacy risks decreased due to a data sharing cooperation. We show that the effect based on different standpoints regarding a data sharing

cooperation (we refer to it from now on simply as group effect) on consumers' risk perception and on their willingness to disclose is stable when controlling for privacy concerns and perceived benefits. Furthermore, we find that this group effect on consumers' willingness to disclose is fully mediated by perceived privacy risks.

With these findings, we contribute to a theory for analyzing (type I, cf. Gregor, 2006) as we explore the differences between these unexplored consumer groups. This enables future research to apply a more refined view on consumers in such complex disclosure settings. Moreover, we also provide elements of a theory for explaining (type II, cf. Gregor, 2006), as we provide first explanations regarding the reason for different standpoints and its' consequences.

Besides, we offer practical implications, as we examine the consequences of this special "unreflected"-group regarding consumers' perceived privacy risks and their willingness to disclose personal data, which allows firms and legislators to adapt communication strategies more specific to the needs of consumers.

## **2 Theoretical Background**

### **2.1 Privacy Concerns**

For privacy studies in the digital context, information privacy is of special interest (Malhotra, Kim and Agarwal, 2004; Smith et al., 2011). Information privacy is tightly linked to consumers' ability to "determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7; Malhotra et al., 2004; Pavlou, 2011). Information privacy concerns in the context of data disclosures relate to what happens with the disclosed data (Dinev and Hart, 2006).

Such privacy concerns are consumers' general (non-situational) concerns regarding their privacy (Malhotra et al., 2004). Higher general privacy concerns can influence situational factors, e.g., privacy concerns can increase consumers' perceived privacy risks, which are briefly described in chapter 2.2. Higher privacy concerns generally lead to a reduced willingness to disclose data but the effect of privacy concerns can be overruled by situational factors (Malhotra et al., 2004; Dinev, McConnell and Smith, 2015), which are not only dependent on general concerns: for example, by perceived benefits, or perceived privacy risks associated with a specific data disclosure (cf. chapter 2.2).

### **2.2 Privacy Calculus and Perceived Privacy Risks**

To understand how consumers decide whether they disclose personal data in disclosure situations, the dominant theory in privacy research is the *Privacy Calculus*. The Privacy Calculus draws on the *Theory of Reasoned Action*, which assumes that consumers' behavior is determined by their intention respectively their attitude towards the behavior and the associated outcome (Ajzen and Fishbein, 1980; Li, 2012).

The Privacy Calculus also draws on the *Maximum Utility Theory*, which means that consumers opt for the option with the highest utility calculated on the basis of their perceived benefits minus their perceived costs (Awad and Krishnan, 2006; Bansal et al., 2010; Li, 2012).

In case of a data disclosure, monetary rewards, social advantages or better personalization can be perceived by consumers as benefits resulting from disclosing their data and, in turn, these benefits increase consumers' willingness to disclose data (Caudill and Murphy, 2000; Hann, Hui, Lee and Png, 2007; Smith et al., 2011).

In contrast, the costs of data disclosures are consumers' perceived privacy risks associated with the respective disclosure (Awad and Krishnan, 2006; Smith et al., 2011; Li, 2012), such as unauthorized access to or use of the data with negative consequences for consumers (Rindfleisch, 1997; Smith et al., 2011). *Privacy risks* describe "the degree to which an individual believes that a high potential for loss [of privacy, annotation of the author] is associated with the release of personal information to a firm" (Smith et al., 2011, p. 1001). When consumers are confronted with privacy risks, consumers' risk



perception can be described cognitively by the probability of a certain unfavorable outcome multiplied by the severity of the respective outcome (Bauer, 1967; Cunningham, 1967; Sieber and Lanzetta, 1964). The more risks or sub-risks exist, the higher the total risk (Peter and Tarpey, 1975; Kahneman and Tversky, 1979; Tversky and Kahneman, 1992).

Apart from the exact assessment, consumers weigh up their perceived benefits against their perceived privacy risks that are dependent on the respective situation. Based on this assessment, they decide whether to disclose their data or not (Smith et al., 2011). Of course, one limitation in the Privacy Calculus is that a “rational” choice for consumers’ behavior is assumed, which is not necessarily always given (Dinev et al., 2015). Instead of evaluating the choices solely with high cognitive effort, Dinev et al. (2015) assumed mental shortcuts, i.e., simple heuristics, also to be used in a data disclosure setting, which is assumed to be connected to less mental effort. Therefore, we also examine mental effort in this study and a possible connection to consumers’ perceived privacy risks and their willingness to disclose data. How consumers perceive a data sharing cooperation between two firms, in which consumers’ personal data is shared, and its consequences for consumers’ risk perception and their willingness to disclose data is not only interesting for researchers but also for firms: for instance, to extend and adapt privacy study designs to a “data sharing cooperation between firms”-context, and also for firms’ to refine their privacy or data handling strategies (Gartner, 2019).

### 3 Hypotheses Development

Regarding a firms’ data sharing cooperation and its’ consequences on consumers privacy risks, there can be three standpoints:

- 1) *“risks increasing”-group*: consumers could see their privacy risks increasing, e.g., because more data transfers could be applied and more firms obtain the data (Peter and Tarpey, 1975; Tversky and Kahneman, 1992; Gartner, 2018);
- 2) *“risks decreasing”-group*: consumers could see their privacy risks decreasing, e.g., due to mutual monitoring of the firms regarding data handling (cf. Killing, 1982; Ahern, 1993; Gartner, 2013), complementing each other (Lei and Slocum Jr., 1992; Mason, 1993) through the exchange of IT-security know-how, or application of the most privacy protective policy (Gartner, 2013; Steudner, Widjaja and Schumann, 2019); and
- 3) *“unreflected”-group*: consumers could see no effects on their privacy risks when a firm has a data sharing cooperation with another firm, maybe because they do not think intensively about the impact on their privacy risks (cf. Kool, McGuire, Rosen and Botvinick, 2010).

As it is intuitively to answer how consumers’ perceived privacy risks and their willingness to disclose is affected when they see their privacy risks increasing respectively decreasing, we want to focus on the third group, that sees no impact on their privacy risks due to a data sharing cooperation. We examine their characteristics and reveal what makes this consumer group so special and what this means for their perceived privacy risks and their willingness to disclose compared to the other two consumer groups. Therefore, we hypothesize what makes this “unreflected”-group special first, and then below, we explain which consequences emerge from those characteristics.

“Unreflected”-consumers report that such a data sharing cooperation will not affect their privacy risks. To obtain this perspective intensive thinking about the situation and its privacy relevant circumstances in detail is not necessary, as it is easier to avoid thinking about the consequences and just assume no consequences (cf. Kool et al., 2010). This is in contrast to the other two perspectives, which require usually to think more intensively about possible consequences. Therefore, we hypothesize:

**H1:** *Consumers in the “unreflected”-group have used less mental effort in assessing their privacy risks than consumers in the “risks increase”-group as well as consumers in the “risks decrease”-group.*

Consumers typically use their prior experiences to form inferences, e.g., about correct behavior and future outcomes (Osberg and Shrauger, 1986). These findings are in line with the availability and the

representativeness heuristic, which assumes that consequences are becoming more dominant and more likely in the mind of consumers the more often these consequences were experienced (Tversky and Kahneman, 1974). When consumers' privacy intrusion experience is less pronounced, they may not see the necessity to deal intensively with the issue of how their privacy risks are affected when a firm shares their personal data to another firm. Hence, consumers that experienced less privacy intrusions do usually not assess the consequences of a data sharing cooperation as effortful as other consumers, who have experienced more privacy intrusions. In accordance with H1, consumers with low privacy intrusion experience simply see no need to use high mental effort to assess possible consequences, e.g., in form of privacy intrusions, as these consequences are not dominant in their mind. Vice versa, consumers with low privacy intrusion experience simply think, that such a data sharing cooperation will not affect their privacy risks. Thus, consumers that spent less mental effort, as assumed for the "unreflected" consumers in H1, should probably also have experienced less privacy intrusions. Therefore, we hypothesize:

**H2:** *Consumers in the "unreflected"-group have experienced less privacy intrusions than consumers in the "risks increase"-group as well as consumers in the "risks decrease"-group.*

Consumers who experienced less privacy intrusions are less concerned regarding their privacy in general (Perloff, 1987; Smith et al., 1996; Cranor, Reagle, Joseph and Ackerman, 1999; Awad and Krishnan, 2006). Based on the previous hypothesized characteristic of the "unreflected"-group in H2, this means that consumers in the "unreflected"-group should have lower general privacy concerns as they should have lower privacy intrusion experience. Therefore, we hypothesize:

**H3:** *Consumers in the "unreflected"-group have lower privacy concerns than consumers in the "risks increase"-group as well as consumers in the "risks decrease"-group.*

According to the hypotheses above, the third "unreflected"-group should be special, as these consumers do not form an elaborated opinion and do not reflect on consequences of a data sharing cooperation intensively. The reason for this is their lower privacy intrusion experience which is also connected to lower privacy concerns as previously explained.

When consumers have experienced less privacy intrusions and have lower privacy concerns, it follows that they also should perceive lower privacy risks and have a higher willingness to disclose (Cranor et al., 1999; Awad and Krishnan, 2006; Smith et al., 2011; Dinev et al., 2015). Therefore, we expect the, at first glance surprising result that consumers in the "unreflected"-group perceive less privacy risks and have a higher willingness to disclose than even those consumers in the "risks decrease"-group, i.e., those consumers who see their privacy risks decreasing through the data sharing cooperation.

**H4:** *Consumers in the "unreflected"-group perceive lower privacy risks than consumers in the "risks increase"-group as well as consumers in the "risks decrease"-group.*

**H5:** *Consumers in the "unreflected"-group have a higher willingness to disclose than consumers in the "risks increase"-group as well as consumers in the "risks decrease"-group.*

In addition, we expect that the effect resulting from the different perspectives between the consumer groups (i.e., the group effect) on consumers' willingness to disclose is mediated by perceived risks. We expect this group effect to be stable even when controlling for other effects. We expect the group effect of the "unreflected"-group (compared to the other two groups) on perceived risks and on their willingness to disclose data which should be distinct from general privacy concerns as not thinking about consequences of a certain disclosure situation and its associated risks regarding one's privacy is different from general low privacy concerns (cf. Hoofnagle and Urban, 2014). Thus, we use control variables for hypotheses H4 and H5 to ensure this group effect is not solely based on different levels of privacy concerns.

As we build the groups based on how the consumers think their privacy risks are affected by a firm cooperation, we expect that this group effect on consumers' willingness to disclose (H5) is fully mediated by perceived privacy risks. Therefore, we hypothesize:

**H6:** *The group effect of consumers in the "unreflected"-group compared to the "risks increase"-group and "risks decrease"-group that leads to an increased willingness to disclose is fully mediated by consumers' perceived risks.*

## 4 Sample and Setup

We used a hypothetical scenario-based survey which is a common approach for information privacy research (e.g., Malhotra et al., 2004; Hann et al., 2007; Xu, Luo, Carroll and Rosson, 2011) to prevent influences from external variables (Kirk, 2013; Coolican, 2014), like it could occur with brand or loyalty effects (e.g., Pan and Zinkhan, 2006).

The survey data was collected in cooperation with a panel provider in two phases: First data was gathered in October 2018 and in the second phase further data was obtained in April 2019 to increase sample size.<sup>1</sup> The subjects were over 18 years and lived in Germany.

The survey was structured as follows: first, each participant had to state age and sex. Then, the same two hypothetical firms were introduced to all participants: the first firm (firm 1) is a software company that is not privacy certified, has low know-how regarding IT security, and was already victim of a cyber-attack. In contrast, the other firm (firm 2) is a retail clothing firm that is privacy certified, has high know-how regarding IT security, and has defended all previous cyber-attacks.

The introduction of the firms was followed by a scenario (same scenario for all participants) in which the participants were asked to hypothetically disclose personal data (name, e-mail address, address, net household income, expenditure on clothing per quarter, and number of persons in the household) in exchange for a cinema voucher with a value of 20 Euro to firm 1, which shares the exact same data obtained from the participant with firm 2 (i.e., with a data sharing cooperation between these two firms). By implementing control questions, it was ensured that the participants have read the questions adequately and understood that there is a cooperation in form of data sharing between these two firms, i.e., that both firms obtain the exact same data. With these criteria, we obtained a number of 182 participants in total with a mean age of 43 and with 56% male. In more detail, 25% of the participants were between 18-29, 20% were between 30-39, 20% were between 40-49, 19% were between 50-59 and 16% were older than 60.

After the scenario, the participants had to indicate, in the following order, their willingness to disclose data (WTD), their perceived privacy risks (RISK) as well as their used mental effort for assessing their privacy risks (ME), their perceived benefits (BENE), their privacy concerns<sup>2</sup>, their frequency of being a privacy intrusion victim (VICT), and their general need for cognition (NfC, i.e., participants' general need to think decisions or problems through, cf. Cacioppo, Petty and Chuan Feng Kao, 1984). For all these constructs existing measurement instruments were used, that were adapted to this study's context when necessary (cf. Appendix 1). A confirmatory factor analysis was performed with principal axes

---

<sup>1</sup> It was verified that the obtained observations during the two collections are not significantly different.

<sup>2</sup> To measure general privacy concerns we used the *Global Information Privacy Concerns* (GIPC). For supplementary verification purposes and as an alternative measurement instrument for general privacy concerns the *Internet Privacy Concerns* (IPC), which measures general privacy concerns related to the internet context (IPC from Dinev and Hart, 2006), was added in the data collection phase 2. For validation purposes, the correlation of the two scales were analyzed. The correlation of the GIPC scale with the IPC scale is highly significant (IPC regressed on GIPC:  $R^2 = .216$ ,  $p < .001$ ;  $\beta = .59$ ,  $p < .001$ ) and behaves analogically in all group comparisons. Due to the higher number of observations for GIPC, we focus on GIPC for the regression analyses. In phase two, the following measurement instruments were also added: mental effort (ME) and dealing intensity (DEAL) as well as the control construct need for cognition (NfC). Thus, for the constructs "IPC", "ME", "NfC", and "DEAL" only 40 observations in group 1, 34 in group 2, and 36 in group 3 were obtained.

factoring and oblimin transformation to obtain the item loadings for the respective constructs (cf. Bandalos and Boehm-Kaufman, 2009), see Appendix 1 for loadings. The participants were asked whether and how the data sharing cooperation of the two firms impacts their privacy risks (see Appendix 1). This was done to divide the participants into the three consumer groups for the analysis<sup>3</sup>, i.e., if the participants think that their privacy risks increase (“risks increase”-group, n = 71), decrease (“risks decrease”-group, n = 54), or see no change regarding their privacy risks (“unreflected”-group, n = 57) since firm 1 shares their disclosed data with firm 2. In addition, the participants had to answer statements on privacy relevant aspects of the data disclosure (see Appendix 1). The sum of correct answers was used to verify how intensively they have dealt (DEAL) with privacy relevant issues in this situation as supplementary verification of participants self-reported mental effort.

## 5 Method and Results

The data was gathered in two phases (cf. chapter 4). Thus, we firstly controlled and verified that no differences exist between the observations obtained at the two different time spans. Next, internal consistency reliability was verified: all examined constructs have Cronbach’s  $\alpha$  above the lower threshold of .7, see Appendix 1 (Bagozzi and Yi, 2012).

The mean values and standard deviations for the variables are displayed in Table 1, which is subdivided into the three different consumer groups.

To ensure that possible effects are not caused by general differences in the three groups regarding age, sex, or consumers’ need for cognition we use analysis of variance (ANOVA) and the Kruskal-Wallis test if the requirements for an ANOVA are not fulfilled (McKight and Najab, 2010), to verify no differences between the groups.

Consumer Group	Construct Mean (Construct Standard Deviation)										
	WTD	BENE	RISK	IPC	GIPC	VICT	ME	DEAL	NfC	AGE	SEX
Group 1: „risks increase“ (n=71)	3.22 (2.15)	3.34 (1.52)	5.28 (1.47)	4.60 (1.49)	4.42 (1.28)	2.52 (1.60)	4.93 (2.34)	4.45 (1.50)	4.49 (1.21)	43.53 (15.50)	52% male
Group 2: „risks decrease“ (n=54)	3.49 (2.04)	3.82 (1.58)	4.77 (1.58)	4.77 (1.39)	4.39 (1.22)	2.54 (1.71)	4.82 (2.22)	4.56 (1.65)	4.57 (.99)	42.65 (14.59)	61% male
Group 3: „unreflected“ (n=57)	4.71 (2.11)	4.24 (1.64)	3.78 (1.78)	3.86 (1.42)	3.74 (1.14)	1.75 (1.09)	4.03 (1.87)	3.56 (1.54)	4.60 (1.07)	41.47 (13.36)	56% male

Table 1. Mean values for the respective consumer groups

No significant differences regarding the control variables “NfC” ( $\chi^2(2, 107) = .024, p = .988$ ), “Age” ( $F(2, 178) = .312, p = .732$ ), and “Sex” ( $F(2, 179) = .499, p = .608$ ) are existent between the three consumer groups.

The group comparisons to answer hypotheses H1-H6 are conducted via Fisher’s unpaired mean permutation test with respectively 50,000 permutations (Fisher, 1935; Smucker, Allan and Carterette, 2007; Millard, 2013), see Table 2.

<sup>3</sup> The option „other“ was selectable in this question and three participants of the initially 185 participants chose this option and could not be assigned into one of the three consumer groups. Thus, these three participants were sorted out of the sample, which lead to the described 182 participants.

Comparison of	Difference of Means (p-value) for						
	ME x > y	DEAL x > y	VICT x > y	GIPC x > y	IPC x > y	RISK x > y	WTD x < y
Group 1 “risks increase” (x) compared to Group 3 “unreflected” (y)	.90* (.040)	.89** (.008)	.77** (.001)	.68*** ( $<.001$ )	.74* (.015)	1.51*** ( $<.001$ )	-1.49*** ( $<.001$ )
Group 2 “risks decrease” (x) compared to Group 3 “unreflected” (y)	.80† (.060)	1.00** (.007)	.78** (.002)	.66** (.002)	.91** (.004)	1.00** (.001)	-1.22** (.001)

Table 2. Differences of means and significance levels for one-sided comparison tests. With † for  $p < .1$ ; \* for  $p < .05$ ; \*\* for  $p < .01$ ; \*\*\* for  $p < .001$ .

Consumers in the “unreflected”-group have used the least mental effort ( $\Delta_{Gr1-3} = .90$ ,  $p = .04$ ;  $\Delta_{Gr2-3} = .80$ ,  $p = .06$ ) and dealt least intensively with privacy related issues in this situation ( $\Delta_{Gr1-3} = .89$ ,  $p = .008$ ;  $\Delta_{Gr2-3} = 1.00$ ,  $p = .007$ ) among the three groups. Thus, we accept H1. Analogously, we accept H2 as consumers in the “unreflected”-group have experienced less privacy intrusions than consumers in the other two groups ( $\Delta_{Gr1-3} = .77$ ,  $p = .001$ ;  $\Delta_{Gr2-3} = .78$ ,  $p = .002$ ). Consumers in the “unreflected”-group have lower privacy concerns (GIPC:  $\Delta_{Gr1-3} = .68$ ,  $p < .001$ ;  $\Delta_{Gr2-3} = .66$ ,  $p = .002$ ; IPC:  $\Delta_{Gr1-3} = .74$ ,  $p = .015$ ;  $\Delta_{Gr2-3} = .91$ ,  $p = .004$ ). Thus, we accept H3.

To verify H4-H6 we perform three regression analyses in addition to the group comparison tests to be able to control for effects caused by consumers’ privacy concerns (GIPC) or their perceived benefits of the data disclosure (models and control variables based on the model of Smith et al. (2011) and Dinev et al. (2015). We use the dummy variable “Group Effect” as a variable to describe the effect which is caused by the group differences with the “unreflected”-group as reference point. Therefore, we have two regression coefficients for this variable: the first regression coefficient (Group Effect<sub>3-1</sub>) describes the effect for the “unreflective”-group compared to the “risks increase”-group, and the second regression coefficient (Group Effect<sub>3-2</sub>) displays the effect of the “unreflective”-group compared to the “risks decrease”-group. In short, we compare the group effect of the “unreflective” consumers with the more “reflective” consumers in the “risks increase”- and “risks decrease”-group while controlling for other factors.

The first regression analysis in Table 3 is necessary for H4: consumers’ perceived privacy risks (RISK) is regressed on “Group Effect” and as a measure of control additionally regressed on consumers’ privacy concerns (GIPC).

The second regression analysis is necessary to verify H5: consumers’ willingness to disclose (WTD) is regressed on “Group Effect” and as a measure of control additionally regressed on consumers’ perceived benefits (BENE) and their privacy concerns (GIPC).

The third regression analysis is necessary to establish a mediation for H6 (cf. Baron and Kenny, 1986; Shrout and Bolger, 2002; Tingley et al., 2014): consumers’ willingness to disclose (WTD) is regressed on “Group Effect” as well as on consumers’ perceived privacy risks (RISK).<sup>4</sup>

We accept hypothesis H4, as consumers in the “unreflected”-group perceive the lowest privacy risks (Table 2:  $\Delta_{Gr1-3} = 1.51$ ,  $p < .001$ ;  $\Delta_{Gr2-3} = 1.00$ ,  $p = .001$ ) and even when controlling for effects of consumers’ privacy concerns, the group effect is still significant (Table 3, Regression 1:  $\beta_{Gr3-1} = 1.202$ ,  $p < .001$ ;  $\beta_{Gr3-2} = .700$ ,  $p = .018$ ). As intuitively expected, the “unreflected”-group perceives less privacy risks than the “risks increase”-group. However, the biggest peculiarity of the “unreflected”-group is that consumers in the “unreflected”-group perceive even lower privacy risks than those in the

<sup>4</sup> No further control variable was used in the third regression on purpose to prevent an inflation of the group effect p-value. Nevertheless, we tested the model also with GIPC and BENE as control variables resulting in an even bigger p-value for the group effect.

“risks decrease”-group, which is not solely explainable due to direct effects resulting from privacy concerns.

Model: F-statistic, p-Value, R <sup>2</sup>		Regression 1		Regression 2		Regression 3	
		RISK regressed on GIPC and Group-Effect: F(3, 178) = 18.51, p<.001; R <sup>2</sup> = .238		WTD regressed on BENE, GIPC and Group-Effect: F(4, 177) = 50.5, p<.001; R <sup>2</sup> = .533		WTD regressed on RISK and Group-Effect: F(3, 178) = 51.93, p<.001; R <sup>2</sup> = .467	
Variable		$\beta$ (std. error)	t-Value (p-Value)	$\beta$ (std. error)	t-Value (p-Value)	$\beta$ (std. error)	t-Value (p-Value)
Group Effect3-1		1.202*** (.276)	4.348 (<.001)	-.468† (.283)	-1.657 (.099)	-.217 (.483)	-.702 (.483)
Group Effect3-2		.700* (.294)	2.383 (.018)	-.613* (.295)	-2.079 (.039)	-.379 (.316)	-1.200 (.232)
RISK						-.845*** (.075)	-11.248 (<.001)
Control variable	BENE			.841*** (.072)	11.627 (<.001)		
	GIPC	.451*** (.0927)	4.863 (<.001)	-.392*** (.094)	-4.184 (<.001)		

Table 3. Regression analyses for H4 – H6 with the “unreflected”-group (group 3) as reference point for the group effect in the respective models. Unstandardized regression coefficients ( $\beta$ ) are used as the groups have different standard deviations. With † for p<.1; \* for p<.05; \*\* for p<.01; \*\*\* for p<.001.

Analogously, we accept H5 as consumers in the “unreflected”-group have a higher willingness to disclose their data than consumers in the other groups (Table 2:  $\Delta_{Gr1-3} = -1.49, p < .001$ ;  $\Delta_{Gr2-3} = -1.22, p = .001$ ) and even when controlling for consumers’ perceived benefits and their privacy concerns, the group effect is still significant on a 10% respectively 5% significance level (Table 3, Regression 2:  $\beta_{Gr3-1} = -.468, p = .099$ ;  $\beta_{Gr3-2} = -.613, p = .039$ ).

To confirm a full mediation as hypothesized in H6, the group effect is not allowed to be significant in the third model. This non-significance of the group effect on consumers’ willingness to disclose while controlling for their perceived risks can be confirmed (Table 3, Regression 3:  $\beta_{Gr3-1} = -.217, p = .483$ ;  $\beta_{Gr3-2} = -.379, p = .232$ ).

To further confirm this mediation, we test the significance of this indirect effect via “mediation”, an R package that is based on a bootstrapping procedure (cf. Tingley et al., 2014). We use bias-corrected and accelerated bootstrapping with 5000 bootstrapped samples for each analysis. We perform two bootstrapping analyses as we want to confirm perceived privacy risks as full mediator in both comparisons, i.e., the group effect of “unreflected”-group compared to “risks increase”-group as well as “unreflected”-group compared to “risks decrease”-group. We perform regression analyses equal to regression 1 and regression 3 (cf. Table 3) containing only the respective two groups and then use these two models per comparison for the bootstrapping analyses (cf. Tingley et al., 2014). We obtain a significant indirect group effect for the bootstrapping analysis containing the “unreflected”-group and the “risks increase”-group with an estimate of -1.020 ( $p < .001$ ), while the direct group effect is non-significant with an estimate of -.140 ( $p = .637$ ). Similarly, we obtain a significant indirect group effect for the bootstrapping analysis containing the “unreflected”-group and the “risks decrease”-group with an estimate of -.557 ( $p = .024$ ), while the direct group effect is non-significant with an estimate of -.465 ( $p = .158$ ). Therefore, we confirm hypothesis H6, i.e., that the group effect on consumers’ willingness to disclose is fully mediated by their perceived privacy risks.

## **6 Discussion**

This study extends privacy research to the unexplored field of data disclosure settings where firms share consumer data with a third party. The focus in this study lies on the most outstanding peculiarity: the data sharing aspect and its consequences for consumers' decision-making regarding perceived privacy risks and their willingness to disclose data. This study shows that all three consumer groups, i.e., consumers who think that their privacy risks increase, decrease, or see no effect regarding their privacy risks due to a data sharing cooperation between two firms, are present in such a data disclosure setting, comprising a privacy protective and a privacy unprotective firm. In this specific setting all three consumer groups are of roughly the same size with a slight dominance of the consumers who think their privacy risks increase ("risks increase": 39%; "risks decrease": 30%; "unreflected": 31%).

The results confirm our expectation that the third group is clearly special: consumers in the "unreflected"-group have the greatest willingness to disclose, lowest perceived privacy risks, lowest privacy concerns, least privacy intrusion experience, and they have also spent the least mental effort on assessing their privacy risks.

We essentially compared consumers who reflected impacts of a data sharing cooperation between two firms (consumers in the "risks increase" and "risks decrease" group) with consumers who did not reflect equally intensive about privacy consequences ("unreflected"-group) due to the firm cooperation via Fisher's permutation test. Furthermore, we examined the group effect and its mediator via regression analyses and a bootstrapping procedure.

Based on this study, future research can generally use a more refined view on consumers in more complex data disclosure settings, i.e., where firms share consumer data to a third party. We find that being in the "unreflected"-group has an effect that leads indirectly to a higher willingness to disclose data with perceived privacy risks as a full mediator. This effect still exists when controlled for general privacy concerns.

### **6.1 Implications**

This study provides a first foundation for future research in more complex data sharing settings, since we contribute to a theory for analyzing (type I, cf. Gregor, 2006), as we explored, analyzed, and compared new consumer groups – enabling an appropriate understanding of consumers in such complex data disclosure settings. Additionally, we show a new possibility to identify a consumer group that deal mentally less intensive with situational, privacy relevant issues in such complex data sharing settings compared to other consumers without asking consumers directly for their spent mental effort. This could prevent possible priming or bias effects in future studies.

Furthermore, we contribute to elements of a theory for explaining (type II, cf. Gregor, 2006): our results indicate that heuristics that draw mainly on experience, like the availability or representativeness heuristic (Tversky and Kahneman, 1974; Osberg and Shrauger, 1986), offer plausible explanations for "unreflected"-consumers' perceived privacy risks and their willingness to disclose data. Moreover, our explanation approach is also in accordance with the critique regarding consumers' "rationality" (Dinev et al., 2015): the special "unreflected"-group has used the least mental effort in assessing their privacy risks, and those consumers have the lowest perceived privacy risks and the greatest willingness to disclose data as well. These results reveal that further investigations regarding the exact role of mental effort and low cognitive effort heuristics as claimed by Dinev et al. (2015) is indeed necessary. Future research can take this study as first indication to work out the causality of consumers' cognitive effort, privacy intrusion experience, and willingness to disclose in more detail (cf. Dinev et al., 2015).

Besides theoretical contributions, this study also offers practical implications: firms should not be too anxious about consequences of a data sharing cooperation in regard to consumers data sharing behavior. This is because around 30% of the consumers do not deal in such situations intensively with privacy issues of a data sharing cooperation and they see their privacy risks also not affected anyhow due to the cooperation. These 30% of the consumers are generally more inclined to disclose their data

even in data disclosure settings with a data sharing cooperation between firms. Therefore, firms should focus on the remaining consumers to achieve a sufficient disclosure willingness. It could be helpful to emphasize benefits provided through the data sharing cooperation, such as an increased personalization, or time savings for the consumers, which increase consumers' willingness to disclose (Smith et al., 2011; Dinev et al., 2015; Krafft, Arden and Verhoef, 2017). In particular, it could be helpful to decrease consumers' perceived privacy risks to explain advantages of the data sharing cooperation regarding consumers privacy. For example, in regard to data security know-how or stricter privacy policies as this could convince even "reflective" consumers of reduced privacy risks and thus, make them more inclined to disclose data (cf. Tsai et al., 2011). Furthermore, such logical arguments may be more convincing for "reflective" consumers, as they are willing to use their cognitive resources to assess the data disclosure circumstances more detailed.

On the other hand, legislators may need to protect these particular 30% of consumers who do not deal mentally intensive with possible consequences of a data sharing procedure or other privacy relevant characteristics ("unreflected"-consumers). All consumers should have the possibility to assess their privacy risks without too much mental effort, so that even the 30% of consumers who use their cognitive resources sparingly for this task, can see consequences easily and have their own, more elaborated, standpoint. This could possibly be achieved by implementing a privacy signal or score, which was already implemented for food in some countries in the European Union (Santé publique France, 2019; tagesschau, 2019). Such tools seem to be highly helpful in the privacy context as well (Tsai et al., 2011; Maass, Wichmann, Pridöhl and Herrmann, 2017), which makes further development and analysis of such tools necessary – especially with respect to "unreflected"-consumers.

## **6.2 Limitations**

Nevertheless, these results have to be viewed in light of their limitations: the distribution of consumers' standpoints and its effects might vary for other firm constellations. The obtained results could also vary when there are more than two firms involved in the data sharing cooperation, which makes further studies necessary. Equally, these results are not necessarily transferable to other cultures with different attitudes on privacy. A cross-cultural study could provide helpful in-depth insights in this regard.

There is also critique on the Privacy Calculus in general, as there is probably an intention-behavior gap (e.g., Norberg, Horne and Horne, 2007), which some explain with missing "rationality" and differences in used mental effort for consumers' decision-making (e.g., Dinev et al., 2015). Independent whether the "rational" choice is true or not, various studies have shown that perceived privacy risks are a major reducing determinant for consumers' willingness to disclose data (Malhotra et al., 2004; Smith et al., 2011; Xu et al., 2011). Despite the criticism on the privacy calculus, perceived risks have been proven to influence behavior in different contexts (e.g., Bachman, Johnson and O'Malley, 1998; Miyazaki and Fernandez, 2001; Norberg et al., 2007; Tsai, Egelman, Cranor and Acquisti, 2011). Similarly intention is a well-established predictor of behavior across various contexts (e.g., Granberg and Holmberg, 1990; Bachman et al., 1998; Sniehotta, Scholz and Schwarzer, 2005; Xu et al., 2011; Li, 2011), which makes the results of this study valuable even when there was no behavior measured. Nevertheless, the effects and results of this study should further be verified and examined in a real setting with consumers' actual behavior measured. To this end, it could be helpful to re-examine the intention-behavior gap, similar to Norberg et al. (2007), when grouping consumers as done in this study or alternatively when grouping them by used mental effort. We would expect a stronger intention-behavior correlation for the more "reflected"-consumers than for the "unreflected"-consumers based on the first insights offered by this study.



## 7 Appendix

Appendix 1. Measurement Instruments, Item Loadings and Cronbach's  $\alpha$ . Item loadings in parentheses; correctness of statements in square brackets; \* signalizes a reverse coded item.

<b>Global Information Privacy Concerns (GIPC)</b>	
Abbreviated from Malhotra et al. (2004), Smith et al. (1996); Cronbach's $\alpha$ : .74; 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree".	
GIPC1 (.72)	Compared to others, I am more sensitive about the way online companies handle my personal information.
GIPC2 (.85)	To me, it is the most important thing to keep my privacy intact from online companies.
GIPC3 (.53)	I am concerned about threats to my personal privacy today.
<b>Internet Privacy Concerns (IPC)</b>	
Adapted from Dinev & Hart (2006), Culnan & Armstrong (1999), Smith et al. (1996); Cronbach's $\alpha$ : .92; 7-Point Likert scale with anchors 1 = "not at all concerned" and 7 = "very concerned".	
IPC1 (.85)	I am concerned that the information I submit on the Internet could be misused.
IPC2 (.83)	I am concerned that a person can find private information about me on the Internet.
IPC3 (.92)	I am concerned about submitting information on the Internet, because of what others might do with it.
IPC4 (.88)	I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.
<b>Mental Effort (ME)</b>	
Adapted from Paas & Van Merriënboer (1994), Bratfisch et al. (1972), 9-Point Likert scale with anchors 1 = "very, very low mental effort" and 9 = "very, very high mental effort".	
ME1	How much mental effort did you put into your risk assessment?
<b>Need for Cognition (NfC)</b>	
Abbreviated from Cacioppo et al. (1984); Cronbach's $\alpha$ : .79; 7-Point Likert scale with anchors 1 = "extremely uncharacteristic" and 7 = "extremely characteristic".	
NfC1 (.66)	I find satisfaction in deliberating hard and for long hours.
NfC2 (.85)	Thinking is not my idea of fun.*
NfC3 (.69)	I would rather do something that requires little thought than something that is sure to challenge my thinking abilities.*
NfC4 (.69)	I really enjoy a task that involves coming up with new solutions to problems.
<b>Intensity of Dealing with Privacy Relevant and Situational Aspects (DEAL)</b>	
Questions and answers, which are multiple response options, developed based on the scenario of this study. Question: Please specify what statement is true.	
Option 1	"Firm 1" is a privacy certified company. [false]
Option 2	"Firm 2" is a privacy certified company. [true]
Option 3	"Firm 1" was a victim of a cyber-attack. [true]
Option 4	"Firm 2" was a victim of a cyber-attack. [false]
Option 5	"Firm 1" has a high level of know-how in IT security. [false]
Option 6	"Firm 2" has a high level of know-how in IT security. [true]
<b>Privacy Intrusion Victim (VICT)</b>	
Adopted from Malhotra et al. (2004), 7-Point Likert scale with anchors 1 = "not at all" and 7 = "very much".	
VIC1	How frequently have you personally been the victim of what you felt was an improper invasion of privacy?

<b>Question on Consumers' Data Sharing Cooperation Privacy Risk Consequences</b>	
Question and answers, which are single response options, based on a pre-study (Stuedner et al., 2019).	
Question: Do you think that the cooperation of the companies involved influences the privacy risks that arise? [Exclusive Options]	
Option 1	Yes, privacy risks are decreased, without the possibility to say which company is responsible for this reduction in privacy risks.
Option 2	Yes, "firm 1" reduces privacy risks arising from "firm 2".
Option 3	Yes, "firm 2" reduces privacy risks arising from "firm 1".
Option 4	Yes, privacy risks are increased, without the possibility to say which company is responsible for this increase in privacy risks.
Option 5	Yes, "firm 1" increases privacy risks arising from "firm 2".
Option 6	Yes, "firm 2" increases privacy risks arising from "firm 1".
Option 7	Yes, other reason.
Option 8	No, the cooperation does not influence the privacy risks.
<b>Perceived Benefits (BENE)</b>	
Adapted from Voss, Spangenberg, & Grohmann (2003), 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
The benefits I get from participating in this/these data collection/s, I will probably describe as ...	
BENE1 (.90)	functional
BENE2 (.92)	practical
BENE3 (.77)	necessary
BENE4 (.90)	helpful
<b>Perceived Privacy Risks (RISK)</b>	
Adapted from Dinev, Xu, Smith, & Hart (2013), Dinev & Hart (2006), Featherman & Pavlou (2003); Cronbach's $\alpha$ : .95; 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree".	
RISK1 (.93)	It is very risky in this data collection to reveal personal information.
RISK2 (.94)	The disclosure of personal information in this data collection is associated with a high potential risk of losing privacy.
RISK3 (.89)	My disclosed personal information may be used improperly in this data collection.
RISK4 (.91)	The disclosure of personal information in this data collection could cause many unexpected problems.
<b>Willingness to Disclose (WTD)</b>	
Adapted from Anderson & Agarwal (2011); Cronbach's $\alpha$ : .98; 7-Point semantic differential with different anchors, see items below.	
Question: To what extent would you be willing to disclose the requested data in this data collection and thus to participate in this data collection.	
WTD1 (.99)	unlikely - likely
WTD2 (.99)	not probable - probably
WTD3 (.97)	unwilling - willing

## References

- Ahern, R. (1993). "The Role of Strategic Alliances in the International Organization of Industry." *Environment and Planning A*, 25(9), 1229–1246.

- Ajzen, I. and M. Fishbein. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, N.J: Pearson.
- Anderson, C. L. and R. Agarwal. (2011). "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information." *Information Systems Research*, 22(3), 469–49.
- Angst, C. M. and R. Agarwal. (2009). "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion." *MIS Quarterly*, 33(2), 339–37.
- Augsburger Allgemeine. (2019). *Beachvolleyball-WM 2019: Finale, Teams, Duelle live im TV und Stream*. URL: <https://www.augsburger-allgemeine.de/sport/Beachvolleyball-WM-2019-Finale-Teams-Duelle-live-im-TV-und-Stream-id54711401.html> (visited on 11/29/2019).
- Awad, N. F. and M. S. Krishnan. (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.
- Bachman, J. G., L. D. Johnson and P. M. O'Malley. (1998). "Explaining recent increases in students' marijuana use: impacts of perceived risks and disapproval, 1976 through 1996." *American Journal of Public Health*, 88(6), 887–892.
- Bagozzi, R. P. and Y. Yi. (2012). "Specification, evaluation, and interpretation of structural equation models." *Journal of the Academy of Marketing Science*, 40(1), 8–34.
- Bandalos, D. L. and M. R. Boehm-Kaufman. (2009). "Common misconceptions in exploratory factor analysis." *Statistical and Methodological Myths and Urban Legends: Where Pray Tell Did They Get This Idea*, 63–88.
- Bansal, G., F. "Mariam" Zahedi and D. Gefen. (2010). "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online." *Decision Support Systems*, 49(2), 138–15.
- Baron, R. M. and D. A. Kenny. (1986). "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations." *51(6)*, 1173–1182.
- Bauer, R. A. (1967). "Consumer Behavior as Risk Taking." In: *Risk Taking and Information Handling in Consumer Behavior* (pp. 389–398). Boston: Harvard University.
- Beach Majors GmbH. (2019). *Beachstream*. URL: [https://de.beachmajorseries.com/en/users/beach\\_stream](https://de.beachmajorseries.com/en/users/beach_stream) (visited on 07/05/2019).
- Bratfisch, O., G. Borg and S. Dornic. (1972). "Perceived item-difficulty in three tests of intellectual performance capacity." Stockholm: Institute of Applied Psychology.
- Cacioppo, J. T., R. E. Petty and Chuan Feng Kao. (1984). "The Efficient Assessment of Need for Cognition." *Journal of Personality Assessment*, 48(3), 306–307.
- Caudill, E. M. and P. E. Murphy. (2000). "Consumer Online Privacy: Legal and Ethical Issues." *Journal of Public Policy & Marketing*, 19(1), 7–19.
- Coolican, H. (2014). *Research methods and statistics in psychology* (Sixth edition). London ; New York: Psychology Press, Taylor & Francis Group.
- Cranor, L. F., Reagle, Joseph and Ackerman, M. S. (1999). "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy." *AT&T Labs Research Technical Report TR 99.4.3*.
- Culnan, M. J. and P. K. Armstrong. (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science*, 10(1), 104–115.
- Cunningham, S. (1967). "The Major Dimensions of Perceived Risk." In: *Risk Taking and Information Handling in Consumer Behavior* (pp. 82–108). Boston: Harvard University.
- Dinev, T. and P. Hart. (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research*, 17(1), 61–8.
- Dinev, T., A. R. McConnell and H. J. Smith. (2015). "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box." *Information Systems Research*, 26(4), 639–655.
- Dinev, T., H. Xu, J. H. Smith and P. Hart. (2013). "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts." *European Journal of Information Systems*, 22(3), 295–316.

- Featherman, M. S. and P. A. Pavlou. (2003). "Predicting e-services adoption: a perceived risk facets perspective." *International Journal of Human-Computer Studies*, 59(4), 451–474.
- Fisher, R. A. (1935). *The Design of Experiments*.
- Gartner. (2013). *Information Sharing as an Industry Imperative to Improve Security*. URL: <https://www.gartner.com/en/documents/2518715/information-sharing-as-an-industry-imperative-to-improve> (visited on 11/29/2019).
- Gartner. (2018). *Gartner Says Data and Analytics Risks Are Audit Executives' Prime Concerns for 2019*. URL: <https://www.gartner.com/en/newsroom/press-releases/2018-10-25-gartner-says-data-and-analytics-risks-are-audit-executives-prime-concerns-for-2019> (visited on 11/29/2019).
- Gartner. (2019). *Gartner Predicts for the Future of Privacy 2019*. URL: [www.gartner.com/smarterwithgartner/gartner-predicts-2019-for-the-future-of-privacy/](http://www.gartner.com/smarterwithgartner/gartner-predicts-2019-for-the-future-of-privacy/) (visited on 11/29/2019).
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. *Official Journal of the European Union* (2016).
- Granberg, D. and S. Holmberg. (1990). "The Intention-Behavior Relationship Among U.S. and Swedish Voters." *Social Psychology Quarterly*, 53(1), 44–54.
- Gregor, S. (2006). "The Nature of Theory in Information Systems." *MIS Quarterly*, 30(3), 611.
- Hann, I.-H., K.-L. Hui, S.-Y. T. Lee and I. P. L. Png. (2007). "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems*, 24(2), 13–42.
- Ho, V. (2018, December 15). "Facebook's privacy problems: a roundup." *The Guardian*.
- Kahneman, D. and A. Tversky. (1979). "Prospect Theory: An Analysis of Decision under Risk." *Econometrica*, 47(2), 263–291.
- Killing, J. P. (1982). *How to Make a Global Joint Venture Work*. URL: <https://hbr.org/1982/05/how-to-make-a-global-joint-venture-work> (visited on 11/29/2019).
- Kirk, R. E. (2013). "Experimental design." In: *Weiner, I.B., Schinka, J.A., Velicer, W.F. (Eds.), Handbook of Psychology, Research Methods in Psychology* (Vol. 2, pp. 23–45). New York: John Wiley & Sons Inc.
- Kool, W., J. T. McGuire, Z. B. Rosen and M. M. Botvinick. (2010). "Decision Making and the Avoidance of Cognitive Demand" *Journal of Experimental Psychology*, 139(4), 665–682.
- Krafft, M., C. M. Arden and P. C. Verhoef. (2017). "Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions?" *Journal of Interactive Marketing*, 39, 39–54.
- Lei, D. and J. W. Slocum Jr. (1992). "Global Strategy, Competence-Building and Strategic Alliances." *California Management Review*, 35(1), 81–97.
- Li, H., R. Sarathy and H. Xu. (2011). "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors." *Decision Support Systems*, 51(3), 434–445.
- Li, Y. (2011). "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework." *Communications of the Association for Information Systems*.
- Li, Y. (2012). "Theories in online information privacy research: A critical review and an integrated framework." *Decision Support Systems*, 54(1), 471–481.
- Maass, M., P. Wichmann, H. Pridöhl and D. Herrmann. (2017). "PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites." In: E. Schweighofer, H. Leitold, A. Mitrakas, & K. Rannenberg (Eds.), *Privacy Technologies and Policy* (pp. 178–191). Cham: Springer International Publishing.
- Madsbjerg, S. (2017). *It's Time to Tax Companies for Using Our Personal Data*. URL: <https://www.nytimes.com/2017/11/14/business/dealbook/taxing-companies-for-using-our-personal-data.html> (visited on 11/29/2019).
- Malhotra, N. K., S. S. Kim and J. Agarwal. (2004). "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research*, 15(4), 336–355.
- Mason, J. C. (1993). "Strategic alliances: Partnering for Success." *Management Review*, 82(5).

- McKight, P. E. and J. Najab. (2010). "Kruskal-Wallis Test." In: *The Corsini Encyclopedia of Psychology* (pp. 1–1). American Cancer Society.
- Millard, S. P. (2013). "EnvStats: An R package for environmental statistics." *Wiley StatsRef: Statistics Reference Online*.
- Miyazaki, A. D. and A. Fernandez. (2001). "Consumer Perceptions of Privacy and Security Risks for Online Shopping." *Journal of Consumer Affairs*, 35(1), 27–44.
- Norberg, P. A., D. R. Horne and D. A. Horne. (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs*, 41(1), 100–126.
- Osberg, T. M. and J. S. Shrauger. (1986). "Self-prediction: Exploring the parameters of accuracy." *Journal of Personality and Social Psychology*, 51(5), 1044–1057.
- Paas, F. G. W. C. and J. J. G. Van Merriënboer. (1994). "Variability of worked examples and transfer of geometrical problem-solving skills: A cognitive-load approach." *Journal of Educational Psychology*, 86(1), 122–133.
- Pan, Y. and G. M. Zinkhan. (2006). "Exploring the impact of online privacy disclosures on consumer trust." *Journal of Retailing*, 82(4), 331–338.
- Pavlou, P. (2011). "State of the Information Privacy Literature: Where are We Now and Where Should We Go?"; 35(4), 977–988.
- Perloff, L. S. (1987). "Social Comparison and Illusions of Invulnerability to Negative Life Events." In: C. R. Snyder & C. E. Ford (Eds.), *Coping with Negative Life Events: Clinical and Social Psychological Perspectives* (pp. 217–242). Boston, MA: Springer US.
- Peter, J. P. and L. X. Tarpey. (1975). "A Comparative Analysis of Three Consumer Decision Strategies." *Journal of Consumer Research*, 2(1), 29–37.
- Rindfleisch, T. C. (1997). "Privacy, Information Technology, and Health Care." *Commun. ACM*, 40(8), 92–10.
- Santé publique France. (2019). *Nutri-Score*. URL: <https://www.santepubliquefrance.fr/determinants-de-sante/nutrition-et-activite-physique/articles/nutri-score> (visited on 11/29/2019).
- Shrout, P. E. and N. Bolger. (2002). "Mediation in experimental and nonexperimental studies: New procedures and recommendations." *Psychological Methods*, 7(4), 422–445.
- Sieber, J. E. and J. T. Lanzetta. (1964). "Conflict and conceptual structure as determinants of decision-making behavior." *Journal of Personality*, 32(4), 622–641.
- Smith, H. J., T. Dinev and H. Xu. (2011). "Information privacy research: an interdisciplinary review." *MIS Q.*, 35(4), 989–1016.
- Smith, H. J., S. J. Milberg and S. J. Burke. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly*, 20(2), 167–196.
- Smucker, M. D., J. Allan and B. Carterette. (2007). "A comparison of statistical significance tests for information retrieval evaluation." In: *Proceedings of the sixteenth ACM Conference on Information and Knowledge Management* (pp. 623–632). Lisbon, Portugal: ACM Press.
- Sniehotta, F. F., U. Scholz and R. Schwarzer. (2005). "Bridging the intention-behaviour gap: Planning, self-efficacy, and action control in the adoption and maintenance of physical exercise." *Psychology & Health*, 20(2), 143–16.
- Solon, O. (2018, April 4). *Facebook says Cambridge Analytica may have gained 37m more users' data*. URL: <https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought> (visited on 11/29/2019).
- Stuedner, T., T. Widjaja and J. H. Schumann. (2019). "An Exploratory Study of Risk Perception for Data Disclosure to a Network of Firms". In: *Human Practice. Digital Ecologies. Our Future* (pp. 1352–1357). Siegen: Academic Press.
- tagesschau (2019). "Lebensmittel-Label Nutri-Score: Eine Ampel für Verbraucher." Retrieved from <https://www.tagesschau.de/inland/nutriscore-101.html> (visited on 11/29/2019).
- Techcrunch.com. (2018). *Amazon admits it exposed customer email addresses, but refuses to give details*. URL: <https://social.techcrunch.com/2018/11/21/amazon-admits-it-exposed-customer-email-addresses-doubles-down-on-secrecy/> (visited on 11/29/2019).
- Tingley, D., T. Yamamoto, K. Hirose, L. Keele and K. Imai. (2014). "mediation: R Package for Causal Mediation Analysis." *Journal of Statistical Software*, 59(5).

- Tsai, J. Y., S. Egelman, L. Cranor and A. Acquisti. (2011). "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research*, 22(2), 254–268.
- Tversky, A. and D. Kahneman. (1974). "Judgment under Uncertainty: Heuristics and Biases." *Science*, 185(4157), 1124–1131.
- Tversky, A. and D. Kahneman. (1992). "Advances in prospect theory: Cumulative representation of uncertainty." *Journal of Risk and Uncertainty*, 5(4), 297–323.
- Hoofnagle, C. J. and J. Urban, (2014). "Alan Westin's Privacy Homo Economicus." *Wake Forest Law Review*, 49, 261–317.
- Vaidhyanathan, S. (2018). *Violating our privacy is in Facebook's DNA*. URL: <https://www.theguardian.com/commentisfree/2018/dec/20/facebook-violating-privacy-mark-zuckerberg> (visited on 11/29/2019).
- Voss, K. E., E. R. Spangenberg and B. Grohmann. (2003). "Measuring the Hedonic and Utilitarian Dimensions of Consumer Attitude." *Journal of Marketing Research*, 40(3), 310–32.
- Westin, A. (1967). *Privacy And Freedom*. New York: Atheneum.
- Xu, H., X. (Robert) Luo, J. M. Carroll and M. B. Rosson. (2011). "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing." *Decision Support Systems*, 51(1), 42–52.

# The Impact of Abstraction Levels on the Effect Sizes of Privacy Concerns and Privacy Risks – A Quantitative Meta-Analysis

**Author:** Tobias Steudner, University of Passau, Germany

**Submitted to:** 29<sup>th</sup> European Conference on Information Systems, 2021, Marrakesh, Morocco (*rejected*)

## Abstract

Most studies obtain significant effects between privacy concerns / privacy risks and personal data disclosure / protection behavior, while some find non-significant effects between these constructs. We consider the abstraction levels of these constructs to explain the statistical differences. In particular, the abstraction level describes whether a construct is measured on a general, contextual, or situational level. Based on a structured literature review we classify the applied abstraction levels and compare the resulting effect sizes via meta-analyses for different abstraction level combinations. We propose to employ privacy concerns as a general self-schema and privacy risks as a more situation-specific construct suited to reflect privacy costs in a particular disclosure situation. In line with this perspective, we show that privacy concerns exert the strongest effect on a general abstraction level, while privacy risks exert the strongest effect on a more specific level. This work contributes to a better understanding of paradoxical appearing results for such effects.

# THE IMPACT OF ABSTRACTION LEVELS ON THE EFFECT SIZES OF PRIVACY CONCERNS AND PRIVACY RISKS – A QUANTITATIVE META-ANALYSIS

Tobias Steudner

University of Passau,

Chair of Business Information Systems,

Passau, Germany,

tobias.steudner@uni-passau.de

## Abstract

*Most studies obtain significant effects between privacy concerns / privacy risks and personal data disclosure / protection behavior, while some find non-significant effects between these constructs. We consider the abstraction levels of these constructs to explain the statistical differences. In particular, the abstraction level describes whether a construct is measured on a general, contextual, or situational level. Based on a structured literature review we classify the applied abstraction levels and compare the resulting effect sizes via meta-analyses for different abstraction level combinations. We propose to employ privacy concerns as a general self-schema and privacy risks as a more situation-specific construct suited to reflect privacy costs in a particular disclosure situation. In line with this perspective, we show that privacy concerns exert the strongest effect on a general abstraction level, while privacy risks exert the strongest effect on a more specific level. This work contributes to a better understanding of paradoxical appearing results for such effects.*

*Keywords: Privacy Concerns, Privacy Risks, Privacy Paradox, Abstraction Levels*



## 1 Introduction

To be successful most digital businesses need to collect and use personal data of their users (Gartner, 2019a, 2019b). Therefore, it is necessary to understand what prevents users to disclose their personal data. Especially users' privacy concerns and their perceived privacy risks are of particular interest as these constructs are seen as the most important factors reducing users' personal data disclosure behavior (Smith, Dinev and Xu, 2011; Y. Li, 2012; Jozani, Ayaburi, Ko and Choo, 2020; Okazaki et al., 2020). Despite the mature field of privacy, there is a certain ambiguity regarding the effects of privacy risks and privacy concerns. Sometimes researcher do not sufficiently differentiate between privacy concerns and privacy risks and interpret them as very similar (e.g., Y. Li, 2012). Furthermore, there are studies that find a significant effect, e.g., of privacy concerns on disclosure or protection behavior (e.g., Aivazpour and Rao, 2020).<sup>1</sup> In contrast, there are studies that obtain no significance for such effects (e.g., Zafeiropoulou, Millard, Webber and O'Hara, 2013). Such a non-significant effect of privacy concerns or privacy risks on disclosure behavior, is the most extreme manifestation of the cases where users perceived concerns or privacy risks are not in line with their behavior. When users' privacy concerns are not in line with their behavior, the term "privacy paradox" is used to describe this phenomenon (Pavlou, 2011; Smith et al., 2011; H. Li, Luo, Zhang and Xu, 2017). The term privacy paradox comprises even more paradoxical findings (Norberg, Horne and Horne, 2007; Kokolakis, 2017; Chen, 2018; Risius, Baumann and Krasnova, 2020), but we solely focus on findings based on the effects of privacy concerns and privacy risks on disclosure or protection behavior. The inconsistency in the resulting effect sizes and their differences in significance makes unclear when and why there is a strong respectively weak effect of privacy concerns and privacy risks on privacy behavior. Thus, this study strives to shed light on differences between the two most common antecedents that reduce disclosure behavior, i.e., between privacy concerns and privacy risks as well as their resulting effect sizes.

To allow a better comparison and understanding of distinct privacy studies and their varying results, it is firstly necessary to understand privacy concerns and privacy risks in detail. Furthermore, it is necessary to consider the applied abstraction levels, i.e., general, contextual or situation specific measurement of the constructs. For example, Davazdahemami et al. (2018) showed that it can have a considerable impact on the results whether privacy concerns and disclosure behavior are measured on the same abstraction level or not (Davazdahemami et al., 2018). Focusing on the abstraction levels, we firstly provide a refined understanding of privacy concerns and privacy risks and distinguish these two constructs to provide an explanation for the varying effect sizes obtained in privacy studies. Based on this understanding, the role of the abstraction levels for the effects of privacy concerns and privacy risks on disclosure and protection behavior is examined. With this we want to offer an explanation for the differences in effect sizes, by understanding why and in which abstraction level combination privacy concerns and privacy risks exert the strongest effects. This leads to the following research aim:

*Distinguishing the constructs privacy concerns and privacy risks and understanding differences in the resulting effect sizes based on abstraction level combinations.*

---

<sup>1</sup> Despite we acknowledge that there is a gap between disclosure intention and actual disclosure behavior, which is the original definition of the privacy paradox according to Norberg et al. (2007), only very few studies measure actual disclosure behavior. Most studies measure disclosure respectively protection intention, willingness, or self-reported behavior. Due to the fact that we want to apply a meta-analysis of paradoxical findings and focus on the abstraction levels of the constructs, we do not differentiate between actual-/self-reported behavior, intention and willingness in this study. For the sake of simplicity, we use the term behavior whenever we do not want to differentiate between the measurement types. However, we acknowledge that these constructs are distinct to a certain degree (N. Gerber, Gerber and Volkamer, 2018), but this distinction is not in the scope of this study.

To analyze the impact of abstraction level combinations on the resulting effect sizes a quantitative meta-analysis is conducted. As this study strives to examine unbiased effect sizes, focus is solely on literature that intends to examine the privacy paradox. This is reasonable as results in such paradox studies are interesting and publishable independent whether they observed significant or non-significant effects. With this approach a publication bias towards significant effects in the identified literature should be prevented (cf. Gerber and Malhotra, 2008).

As theoretical background for this work, firstly the different abstraction levels are explained in more detail. We also introduce and distinguish privacy concerns as a general-self schema and perceived privacy risks as the situational manifestation of the general self-schema to develop privacy concerns. Based upon that knowledge, hypotheses regarding the effect sizes for different abstraction level combinations are developed. Afterwards, the structured literature review process as well as the procedures for the meta-analysis are described. The meta-analysis results verify our hypotheses regarding the varying effect sizes due to distinct abstraction level combinations: in line with our expectation, we find that the effect for privacy concerns on disclosure as well as protection behavior is the strongest when independent and dependent variables are measured on a general level. In line with our expectation, that a less general abstraction level leads to a larger effect size for privacy risks, we find that the effect for privacy risks on disclosure behavior is stronger, when both independent and dependent variables are measured on a situational compared to a general abstraction level. We also verify that privacy risks have a stronger effect on disclosure behavior compared to privacy concerns when the independent and dependent variables are measured on a situational abstraction level.

This work increases the understanding as well as simplifies comparability of previous and future privacy concerns and privacy risks studies. Furthermore, the results confirm the importance to consider the abstraction level combinations and discuss its influence for effects of privacy concerns and privacy risks. We suggest to conceptualize privacy concerns as a general-self schema that reflects the disposition to develop concerns in this regard, while privacy risks are the particular manifestation of this disposition. Based on this conceptualization and the meta-analysis, this study helps to understand and predict resulting effect sizes for these constructs in more detail and thus, helps to design and interpret future studies.

## **2 Theoretical Background and Hypotheses Development**

### **2.1 Abstraction Levels applied in Privacy Studies**

In this section our interpretation of the three abstraction levels a variable can be measured on is based on Davazdahemami et al. (2018) and shall be shortly explained: a measurement scale can be on i) a general level (gen), which is the case when the measurement does neither relate to situational nor to sufficient contextual information, ii) a contextual level (cont), which is the case when the measurement refers to contextual information, e.g., the industry branch (we do not define an app or website “context” as contextual but rather as general, since information privacy is mainly important in this field, cf. Smith et al., 2011), and iii) situational level (sit), which is the case when the measurement relates to information that allows a sufficient idea what is associated with that specific situation, e.g., description of the app itself and not only the industry branch of the app.

### **2.2 Privacy Concerns**

#### **2.2.1 Dimensions, Abstraction Levels and Measurement Instruments**

Most studies that examine privacy concerns use similar dimensions to measure users’ privacy concerns, mainly the development of concerns regarding the following aspects: the amount of personal data collected, data access through unauthorized persons, use of data for unauthorized purposes, use of inaccurate or false user data, missing control over personal information, and missing information

about privacy practices (cf. Smith, Milberg and Burke, 1996; Dinev and Hart, 2004; Malhotra, Kim and Agarwal, 2004; Buchanan, Paine, Joinson and Reips, 2007; Hong and Thong, 2013).

Most of these measurement instruments are originally developed for a measurement of online (and sometimes also offline) privacy concerns on a general abstraction level without specifically referring to an industry or website type context nor with a reference to a specific situation (cf. Smith et al., 1996; Dinev and Hart, 2004; Malhotra et al., 2004; Hong and Thong, 2013). Although, there is an exception with the measurement instrument by Osatuyi (2015), which is based on the general instrument of Smith et al. (1996) but adapted to the social media context.<sup>2</sup> Another commonly used measurement instrument developed by Buchanan et al. (2007) also refers to distinct contexts. This instrument uses an index over different contexts and therefore it is equally intended to measure privacy concerns “in sum”, i.e., on a general abstraction level.

Now that we have shown that privacy concerns are originally designed to reflect concerns on a general abstraction level, we discuss how previous studies interpret privacy concerns. Oftentimes privacy concerns are interpreted as antecedent of perceived privacy risk (Malhotra et al., 2004; Kehr, Kowatsch, Wentzel and Fleisch, 2015), or as control variable for privacy behavior (Dinev, McConnell and Smith, 2015). Sometimes privacy concerns are also used to measure privacy costs in the privacy calculus (Mothersbaugh, Foxx, Beatty and Wang, 2012; Y. Li, 2012). These studies share the commonality that they expect users’ privacy concerns to reduce users’ willingness to disclose personal data (Smith et al., 2011; Y. Li, 2012). Despite most privacy concerns measurement instruments share similar dimensions, a common understanding of privacy concerns is oftentimes missing in privacy studies (Hong and Thong, 2013), which hampers to understand the resulting effect sizes in detail. This is even partly true for studies that develop a measurement instrument for privacy concerns and offer detailed descriptions of underlying dimensions, as their items do not always capture what they intend to measure (Hong and Thong, 2013).

According to Hong and Thong (2013), there are three types of wording common in privacy concern measurement items: i) perception of one’s concern for others’ behavior (e.g., I am concerned over companies collecting personal data, ii) perception of others’ behavior (e.g., companies collect much personal data), and iii) expectation of others’ behavior (e.g., companies should not collect personal data; for more details cf. Hong and Thong, 2013). While only the first wording type, i.e., perception of one’s concern for others’ behavior, is an adequate measurement for privacy concerns, as the other two wording types rather measure distinct constructs (Hong and Thong, 2013).

## 2.2.2 Privacy Concerns as a Self-Schema

To further confirm that the general abstraction level is the most adequate level to measure privacy concerns and should in turn lead to the largest effect size, we briefly elaborate a refined definition for privacy concerns. This also helps to enable a clearer distinction of privacy concerns from other constructs. For this definition, we draw on self-schema literature and emphasize that the general abstraction level is suited best for privacy concerns from another point of view:

According to Markus (1977), self-schemata are “*cognitive generalizations about the self*, derived from *past experience*, that organize and guide the processing of self-related information contained in the person’s social environment” (Markus, 1977, p. 63). Sheeran and Orbell (2000) add that “self-schemas reflect people’s understanding of invariances in their behavior which derives from both specific events and situations and repeated categorizations and evaluations of one’s actions over time. Self-schemas lend structure and coherence to the individuals self-related experiences and thus provide a basis for future judgments, inferences, and decisions about the self” (Sheeran and Orbell, 2000, p. 535). To sum up the essential points of a self-schema: i) it is about a self-perception or a self-assessment; ii) this

---

<sup>2</sup> This measurement instrument nevertheless was only used once in our identified privacy paradox studies.

self-assessment is cognitively generalized from experiences in specific situations in the past, and iii) serves as the basis for future decisions about the self.

The first point fits to privacy concerns, especially when considering the study of Hong and Thong (2013), where only the wording type “perception of one’s concern for others’ behavior” (e.g., “It usually bothers me when online companies ask me for personal information.” from Malhotra et al., 2004) is acknowledged as fitting to what should be measured with privacy concerns. With this type of wording, privacy concerns reflect only the perception of an individual about one’s self, for instance, whether one is inclined to become concerned about the abuse of personal data. Second, privacy concerns are, equally to a self-schema, generalized from prior privacy experiences (Smith et al., 1996; Dinev et al., 2015). Also, privacy concerns are originally intended to be measured on a general abstraction level (or at least abstracted to a context) but not regarding a specific situation (cf. Smith et al., 1996; Dinev and Hart, 2004; Malhotra et al., 2004; Buchanan et al., 2007; Hong and Thong, 2013; Kehr, Kowatsch, et al., 2015). Third, privacy concerns alter one’s future decision making by influencing one’s data disclosure behavior (Malhotra et al., 2004; Dinev et al., 2015).

Accordingly, we define privacy concerns as users’ generalized self-assessment regarding the disposition to develop concerns due to privacy issues. With this definition of privacy concerns, and when looking at the measurement items of original instruments, it becomes clear that privacy concerns are not intended to reflect how much information privacy one does perceive (cf. Buchanan et al., 2007), nor how much privacy costs respectively what degree of privacy risks are existent (cf. Malhotra et al., 2004). Our refined definition emphasizes that privacy concerns should be used to reflect how inclined users see themselves to generally develop concerns regarding data issues or data handling practices (cf. Hong and Thong, 2013).

### 2.2.3 Meaning of Abstraction Levels for the Effect of Privacy Concerns on Disclosure and Protection Behavior

Davazdahemami et al. (2018) provide evidence that the negative effect of privacy concerns on disclosure behavior is the strongest when independent and dependent variables are measured aligned, i.e., on the same abstraction level. Measuring the two variables on different abstraction levels (unaligned) weakens their correlation and in the most extreme form even results in non-significance. Thus, this abstraction level difference between independent and dependent variable could be one reason for obtaining paradoxical seeming results (Davazdahemami et al., 2018). However, Davazdahemami et al. (2018) do not discuss or predict effect size differences for aligned effects.

This is exactly the focus of our study, as we expect privacy concerns to exert the strongest negative effect on data disclosure when both constructs are measured aligned on a general abstraction level compared to when they are measured aligned on a contextual or situational abstraction level. We expect this as privacy concerns measurement instruments are validated and intended originally to be used on a general abstraction level. Furthermore, we expect this due to our previous described understanding of privacy concerns as a self-schema that has to be captured on a general abstraction level, as it emerges through generalization of various previous experiences. Thus, we hypothesize that privacy concerns exert a stronger effect on disclosure behavior, when both constructs are measured aligned on a general abstraction level, compared to when measured aligned on a contextual or situational level:

H1a: *Privacy concerns exert the strongest negative effect on disclosure behavior, when both constructs are measured aligned on a general abstraction level compared to when both constructs are measured aligned on a contextual level.*

H1b: *Privacy concerns have the strongest negative effect on disclosure behavior, when both constructs are measured aligned on a general abstraction level compared to when both constructs are measured aligned on a situational level.*

Regarding the second effect of privacy concerns, there is a wide consensus that privacy concerns increase protection behavior (Son and Kim, 2008; Lutz and Strathoff, 2014; Fatima et al., 2019). With protection behavior we refer to steps that increase one's privacy such as adapting privacy settings, using a virtual private network, deleting browser history as well as cookies, et cetera (Son and Kim, 2008; Lutz and Strathoff, 2014). In line with the above reasoning, that privacy concerns is a general self-schema, which is intended to be measured on a general level, we expect its' positive effect on protection behavior to be stronger when both constructs are measured aligned on a general abstraction level, compared to when measured aligned on a contextual or a situational level. Thus, we hypothesize:

H2a: *Privacy concerns exert the strongest positive effect on protection behavior, when both constructs are measured aligned on a general abstraction level compared to when both constructs are measured aligned on a contextual level.*

H2b: *Privacy concerns exert the strongest positive effect on protection behavior, when both constructs are measured aligned on a general abstraction level compared to when both constructs are measured aligned on a situational level.*

### **2.3 Privacy Calculus**

In the previous chapter, we argued that privacy concerns are not intended to reflect situational privacy costs, but rather reflect a self-schema in form of a general inclination to develop privacy concerns. Now we briefly discuss the privacy calculus and how situational privacy costs are considered. Drawing on the utility maximization theory, the privacy calculus assumes a weighting of individuals perceived benefits and their perceived costs which forms users' disclosure intention (Smith et al., 2011; Dinev et al., 2015). While users' perceived benefits increase disclosure intention, users' perceived costs reduce disclosure intention (Smith et al., 2011; Kehr, Kowatsch, et al., 2015). When it is observed that antecedents to disclosure behavior, e.g., privacy risks, have no effect on disclosure behavior, this can be seen as one manifestation of a privacy paradox (Norberg et al., 2007; Risius et al., 2020).

### **2.4 Privacy Risks**

In the context of the privacy calculus, the costs are primarily connected to privacy risks that are associated with a data disclosure (Malhotra et al., 2004; Smith et al., 2011; Kehr, Kowatsch, et al., 2015). Therefore, we expect perceived privacy risks best suited to reflect the cost side of the privacy calculus, especially in specific disclosure situations (cf. Malhotra et al., 2004; Kehr, Kowatsch, et al., 2015). To deepen the understanding of privacy risks and resulting effect sizes, we briefly introduce the risk construct and draw on traditional risk perception literature: perceived risk is defined as the perceived probability of an unfavorable outcome multiplied by the perceived severity of the respective outcome (Peter and Tarpey, 1975). If a risk is constituted by different sub-risks, or if several risks (i.e., possible unfavorable outcomes) exist, they are assumed to be calculated analogously and add up to the total perceived risk (Peter and Tarpey, 1975). This is in line with the context specific definition of perceived privacy risks by Smith et al. (2011): privacy risks comprise "the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm" (Smith et al., 2011, p. 1001).

To adequately reflect privacy costs associated with a disclosure decision the abstraction level needs to be aligned with the level of the dependent variable (cf. Davazdahemami et al., 2018), which we expect to be usually the case with the more (situation-)specific privacy risks (cf. Malhotra et al., 2004; Kehr, Kowatsch, et al., 2015).

This rather specific expected abstraction level for the measurement of privacy risks is also in line with risk literature in other research contexts: for a purchase decision perceived risk is defined as follows: "Perceived risk" refers to the nature and amount of risk perceived by a consumer in contemplating a

particular purchase decision” (Cox and Rich, 1964, p. 33). The part that has to be emphasized in this definition is a *particular decision*. Transferred to the privacy context this means a *particular* data disclosure decision, which means that it is referred to a situational abstraction level and not to a general level. Therefore, we want to emphasize the situational aspect and change the definition of privacy risks by Smith et al. (2011) for our study accordingly into: privacy risks comprise “the degree to which an individual believes that a high potential for loss [of privacy] is associated [with a particular data disclosure]” (Smith et al., 2011, p. 1001).

From another point of view, this situation specificity seems even more appropriate: to enable users to assess privacy risks as good as possible, they need detailed and rather holistic situational information (cf. Tsai, Egelman, Cranor and Acquisti, 2010). Also, effects between constructs measured aligned, i.e., on the same abstraction level, have the largest effect size compared to other abstraction level combinations (Davazdahemami et al., 2018). Based on this knowledge, we expect users to rely the strongest on their risk assessment, when privacy risks and disclosure behavior are measured aligned on a situational abstraction level, i.e., when users have situation-specific information and both variables are measured regarding the specific situation. Thus, we expect privacy risks to exert the strongest effect on disclosure behavior when measured aligned on a situational level, compared to when measured aligned on a general or a contextual level, i.e., without situation-specific information. We hypothesize accordingly:

H3a: *Privacy Risks exert the strongest negative effect on disclosure behavior, when both constructs are measured aligned on a situational abstraction level compared to when both constructs are measured aligned on a general level.*

H3b: *Privacy Risks exert the strongest negative effect on disclosure behavior, when both constructs are measured aligned on a situational abstraction level compared to when both constructs are measured aligned on a contextual level.*

## **2.5 Comparison of Privacy Concerns and Privacy Risks on a Situational Abstraction Level**

Based on the refined understanding of privacy concerns and privacy risks, a comparison of the effects of privacy concerns and privacy risks on disclosure behavior is possible. A brief emphasize on the differences between general privacy concerns and the more specific privacy risks is provided in the following. This is done to understand and predict the resulting effect size differences on an aligned situational abstraction level for their effects.

Privacy concerns reflect users’ general disposition to develop privacy concerns when certain data handling practices are applied (e.g., “It usually bothers me when commercial websites ask me for personal information” from Hong and Thong, 2013, p. 48) – therefore we could alternatively term this construct “disposition to develop privacy concerns” (cf. Malhotra et al., 2004; Kehr, Kowatsch, et al., 2015), “Personal/General Disposition”). In contrast, privacy risks are the manifestation of the general disposition to develop concerns in the form of a situation specific risk assessment as part of the privacy calculus (cf. Malhotra et al., 2004; Kehr, Kowatsch, et al., 2015).

Accordingly, when measuring privacy concerns respectively privacy risks, and disclosure behavior aligned on a situational level, we expect the following for the effect on disclosure behavior. We propose privacy risks to have a stronger negative effect compared to privacy concerns in such a situational-situational abstraction level combination. This is because privacy risks are rather situation specific cost assessments. In contrast, privacy concerns measurement instruments and its’ conceptualization are not intended for this abstraction level and rather measure the disposition to develop “concerns” in general, i.e., the general disposition to perceive a high amount of privacy risks. This makes privacy concerns an antecedent to perceived privacy risks (cf. Malhotra et al., 2004; Kehr, Kowatsch, et al., 2015). Therefore, we hypothesize:

H4: Privacy risks compared to privacy concerns have a stronger negative effect on disclosure behavior, when each construct is measured aligned on a situational abstraction level.

To sum up the hypotheses, Figure 1 provides an overview for all hypotheses in this study.

Hypothesis	Largest Expected Effect Size	Compared to
H1a:	Privacy Concerns (gen) → Disclosure Behavior (gen)	Privacy Concerns (cont) → Disclosure Behavior (cont)
H1b:	Privacy Concerns (gen) → Disclosure Behavior (gen)	Privacy Concerns (sit) → Disclosure Behavior (sit)
H2a:	Privacy Concerns (gen) → Protection Behavior (gen)	Privacy Concerns (cont) → Protection Behavior (cont)
H2b:	Privacy Concerns (gen) → Protection Behavior (gen)	Privacy Concerns (sit) → Protection Behavior (sit)
H3a:	Privacy Risks (sit) → Disclosure Behavior (sit)	Privacy Risk (gen) → Disclosure Behavior (gen)
H3b:	Privacy Risks (sit) → Disclosure Behavior (sit)	Privacy Risk (cont) → Disclosure Behavior (cont)
H4:	Privacy Risks (sit) → Disclosure Behavior (sit)	Privacy Concerns (sit) → Disclosure Behavior (sit)

Figure 1. Overview for the hypotheses in this study.

### 3 Method

The literature review of Kokolakis (2017), which included studies up to 2015, served as foundation for the literature analysis. We used all publications found in the structured literature search of Kokolakis (2017) and additionally updated the literature for the years 2015-2020 (as of March). In doing so, we followed the exact same procedure, i.e., we searched for “privacy paradox” in conferences and journals that are peer-reviewed and accessible via the Scopus database. This resulted in an initial amount of 279 papers. All papers that were "anonymous, erratum notifications and editorials" were removed after preliminary screening. Of these, only papers were considered relevant, which focused on some sort of paradox in the user privacy context (legal and ethical paradoxes were excluded) resulting in a total number of 129 papers. Due to the focus on the privacy paradox, which is commonly described as disclosing data despite high privacy concerns (Pavlou, 2011), or despite high privacy risks, or as a deviation between the stated intention and the actual behavior (Norberg et al., 2007), only publications were considered that examined such a paradox (118 papers).

In this study the research aim is to distinguish privacy concerns and privacy risks and their effects on disclosure and protection behavior while considering the influence of the applied abstraction levels. In order to not unnecessarily reduce the number of privacy paradox studies that examine such effects, we did not separately consider intentions, willingness, self-reported and actual behavior as we assessed all of these measurements to be acceptable reflect or predictors actual disclosure and protection behavior (Gerber et al., 2018). However, we acknowledge differences between these constructs (Gerber et al., 2018). Nevertheless, these differences are not in the scope of this work. For better comparability of study results, we excluded studies that only used a willingness-to-pay or willingness-to-accept construct to reflect privacy behavior as we assessed them to be more clearly distinct from the previous concepts (e.g., Beresford, Kübler and Preibusch, 2012). For the same reason, we also excluded one paper that only measured a continuance-to-disclose construct (Hew, Tan, Lin and Ooi, 2017).

In order to consider the abstraction levels on the resulting effect sizes better, we sorted out studies that do not quantitatively examine a direct effect of privacy concerns or privacy risks on a disclosure or protection behavior variable in a regression, structural equation model, or in an equal correlational procedure. This step was necessary to allow a comparison of effect sizes among different privacy paradox studies (31 papers remaining). To be able to assess the applied abstraction levels for the constructs, a sufficient description of the measurement instruments is necessary. Thus, we excluded papers in which measurement instruments were not sufficiently described and where the authors did not respond to our request for their measurement items. This led to a final sample of 27 publications for the meta-analysis (cf. Table 2). In this final sample 13 papers were coming directly from the literature review of Kokolakis (2017).

The classification of the abstraction levels for the constructs considered was performed independently by two researchers experienced in this field using the definition for the three abstraction levels provided in chapter 2.1. This resulted in a matching abstraction level classification of  $\kappa = 0.8$  for privacy concerns,  $\kappa = 1$  for privacy risks,  $\kappa = 0.83$  for disclosure behavior, and  $\kappa = 1$  for protection behavior. The non-matching cases were classified after a short discussion. As a preparation for the meta-analysis, all effect sizes were converted to standardized Pearson's  $r$  based on the procedures described in Peterson and Brown (2005) and Borenstein (2009). When in one study more correlations of the same variables were given, we aggregated the effect sizes with the R package "MAAd", based on Borenstein et al. (2009) with an assumed correlation among the outcome variables of  $r = 0.5$ . When a publication included more studies with different samples for each study, these studies were treated as separate studies. After doing so, mixed effects model meta-analysis was conducted with the R-package "metafor" and "compute.es" (cf. Del Re, 2015; Quintana, 2015; Balduzzi, Rucker and Schwarzer, 2019). To compare the estimated Pearson's  $r$  effect sizes we used the R-package "cocor" for an one-sided effect size comparison test with the assumption of independent groups (for details of the calculation for the independent group one-sided effect size comparison test, see Diedenhofen, 2016).

## 4 Results

This study explores whether the self-schema "privacy concerns" does affect disclosure and protection behavior stronger when the independent and dependent variables are measured aligned on the most abstract, i.e., general abstraction level compared to when measured aligned on a contextual (H1a respectively H2a) or situational abstraction level (H1b respectively H2b). In contrast, we expect privacy risks to impact disclosure behavior stronger when the independent and dependent variables are measured aligned on a situational level compared to when measured aligned on a contextual (H3a) or general abstraction level (H3b). We also compare the effect sizes of privacy risks and privacy concerns on disclosure behavior in an aligned situational abstraction level combination to verify which has the strongest negative effect (H4). Before splitting the effects according to their abstraction level combination, we confirm that there is no publication bias for the effects of privacy concerns and privacy risks on disclosure and protection behavior via funnel plots and rank correlation tests for funnel plot asymmetry ( $\tau_{PC-D(aggreated)} = -.007, p = .98$ ;  $\tau_{PC-PROT(aggreated)} = .164, p = .542$ ;  $\tau_{RISK-D(aggreated)} = -.2, p = .817$ ). Table 1 displays the detailed meta-analysis results for all abstraction level combinations in the identified quantitative privacy paradox literature. An overview of the studies included in the meta-analysis and their examined effects can be found in the appendix (cf. Table 2 and Figure 2-17).

On an aggregated level, i.e., where the publication sample is not split by abstraction level combinations, there is a significant but weak negative effect for privacy concerns on disclosure behavior ( $r = -.08, p < .05$ ). Privacy concerns also have a moderate positive effect on protection behavior ( $r = .347, p < .001$ ). Privacy risks have a moderate negative effect on disclosure behavior on an aggregated level ( $r = -.303, p < .001$ ).



Effects split by constructs and abstraction level combinations	Number of studies	Number of participants	Estimate for Pearson's r [95% CI]	Q-value (p-value)	One-sided r comparison [ $</>$ ]: z-value (p-value)
PC-D (aggregated)	24	12026	-.08 [-.147; -.013]*	335.02 ( $<.001$ )	
PC-PROT (aggregated)	11	6386	.347 [.23; .454]***	252.58 ( $<.001$ )	
RISK-D (aggregated)	5	841	-.303 [-.409; -.189]***	11.41 (.023)	
<b>PC(gen)-D(gen)</b>	<b>5</b>	<b>2245</b>	<b>-.237</b> <b>[-.34; -.127]***</b>	<b>22.65</b> <b>(<math>&lt;.001</math>)</b>	<b>PC-D (H1) reference &lt;</b>
PC(gen)-D(cont)	5	4498	-.13 [-.24; -.018]*	45.17 ( $<.001$ )	-4.253 ( $<.001$ )
PC(gen)-D(sit)	5	1267	-.042 [-.163; .08] n.s.	11.91 (.018)	-5.646 ( $<.001$ )
<b>PC(cont)-D(cont)</b>	<b>5</b>	<b>3296</b>	<b>.08</b> <b>[-.07; .227]n.s.</b>	<b>113.86</b> <b>(<math>&lt;.001</math>)</b>	<b>H1a: -11.747 (<math>&lt;.001</math>)</b>
PC(cont)-D(sit)	5	871	-.019 [-.098; .06] n.s.	5.63 (.229)	-5.551 ( $<.001$ )
<b>PC(sit)-D(sit)</b>	<b>2</b>	<b>431</b>	<b>-.164</b> <b>[-.255; -.07]***</b>	<b>.011 (.917)</b>	<b>H1b: -1.43 (.076)</b> <b>H4: -2.204 (.014)</b>
<b>PC(gen)-PROT(gen)</b>	<b>5</b>	<b>2110</b>	<b>.414</b> <b>[.206; .586]***</b>	<b>65.34</b> <b>(<math>&lt;.001</math>)</b>	<b>PC-PROT (H2) reference &gt;</b>
PC(cont)-PROT(gen)	1	1002	.155 [.102; .207]***	0 (1)	7.395 ( $<.001$ )
<b>PC(cont)-PROT(cont)</b>	<b>4</b>	<b>3023</b>	<b>.36</b> <b>[.16; .531]***</b>	<b>128.11</b> <b>(<math>&lt;.001</math>)</b>	<b>H2a: 2.251 (.012)</b>
<b>PC(sit)-PROT(sit)</b>	<b>1</b>	<b>251</b>	<b>.19</b> <b>[.068; .307]**</b>	<b>0</b> <b>(1)</b>	<b>H2b: 3.694 (<math>&lt;.001</math>)</b>
<b>RISK(gen)-D(gen)</b>	<b>1</b>	<b>369</b>	<b>-.15</b> <b>[-.248; -.049]*</b>	<b>0</b> <b>(1)</b>	<b>H3a: -2.308 (.011)</b>
<b>RISK(cont)-D(cont)</b>	<b>2</b>	<b>309</b>	<b>-.354</b> <b>[-.447; -.254]***</b>	<b>.22</b> <b>(.643)</b>	<b>H3b: .005 (.502)</b>
<b>RISK(sit)-D(sit)</b>	<b>2</b>	<b>163</b>	<b>-.354</b> <b>[-.483; -.209]***</b>	<b>1.13</b> <b>(0.287)</b>	<b>RISK-D (H3) reference &lt;</b> <b>RISK-D/PC-D (H4) reference &lt;</b>

Table 1. Complete meta-analysis results. Results for H1-H4 are in bold. Significance levels of Pearson's r estimates: n.s.  $p > .1$ , †  $p < .1$ , \*  $p < 0.05$ , \*\*  $p < .01$ , \*\*\*  $p < .001$ ; Construct Abbreviations: PC=Privacy Concerns, D=Disclosure Behavior, PROT=Protection Behavior, RISK=Privacy Risks. Abstraction Level Abbreviations: gen=general, cont=contextual, and sit=situational. The color grey symbolizes the reference abstraction level combination for comparing the estimates with a one-sided comparison regarding each effect: less for gen. PC-D (H1); greater for gen. PC-PROT (H2); less for sit. RISK-D (H3); greater for sit. RISK-D vs. sit. PC-D (H4); Q displays the amount of heterogeneity.

The majority of the privacy paradox studies applies a general abstraction level for privacy concerns, which is in line with our expectations. However, for privacy risks surprisingly few privacy paradox studies exist. In these studies, none of the three abstraction levels is clearly preferred for privacy risks.

When subdividing the studies by their abstraction level combination, heterogeneity is reduced compared to the respective aggregated effect. But this decrease in heterogeneity is only sufficient for

abstraction level combinations where the measurements are rather specific and less abstract. Especially for the risk and disclosure construct a rather specific abstraction level reduces heterogeneity successfully (see Table 1: Q-values with  $p > .05$  for  $PC_{cont-D_{sit}}$ ,  $PC_{sit-D_{sit}}$ ,  $Risk_{cont-D_{cont}}$  and  $Risk_{sit-D_{sit}}$ ).

In the following, the results for the effects of privacy concerns on disclosure behavior are discussed in more detail. The abstraction level combination with a general abstraction level for privacy concerns and disclosure behavior, i.e.,  $PC_{(gen)-D_{(gen)}}$ , has the strongest negative effect ( $r = -.237 [-.34; -.127]$ ). For some other abstraction level combinations, there are even non-significant results for the effect of privacy concerns on disclosure behavior ( $PC_{(gen)-D_{(sit)}}$ ,  $PC_{(cont)-D_{(cont)}}$ ,  $PC_{(cont)-D_{(sit)}}$ ). We accept H1a, because the effect of  $PC_{(cont)-D_{(cont)}}$  ( $r = .08 [-.07; .227]$ ) is not significant, and the effects' confidence interval (CI) does not overlap with the CI of  $PC_{(gen)-D_{(gen)}}$ . Additionally, the effect size comparison test confirms that the negative effect of  $PC_{(gen)-D_{(gen)}}$  is stronger than the effect of  $PC_{(cont)-D_{(cont)}}$  ( $z = -11.365, p < .001$ ).

However, comparing the effect sizes of  $PC_{(gen)-D_{(gen)}}$  ( $r = -.237 [-.34; -.127]$ ) and  $PC_{(sit)-D_{(sit)}}$  ( $r = -.164 [-.255; -.07]$ ) an overlap of their confidence intervals is observable. In contrast, the effect size comparison results in a difference that is significant at a 10% level ( $z = -1.43, p = .076$ ). Therefore, we accept H1b on a 10% level.

When looking at the effects of privacy concerns on protection behavior, every abstraction level combination has a positive and significant effect on protection behavior. The strongest effect can be observed for the abstraction level combination  $PC_{(gen)-PROT_{(gen)}}$  ( $r = .414 [.206; .586]$ ). The CI of this effect overlaps with the CIs of the effect  $PC_{(cont)-PROT_{(cont)}}$  ( $r = .36 [.16; .531]$ ) and  $PC_{(sit)-PROT_{(sit)}}$  ( $r = .19 [.068; .307]$ ). However, based on the effect size comparison test, the effect size of  $PC_{(gen)-PROT_{(gen)}}$  is significantly larger compared to  $PC_{(cont)-PROT_{(cont)}}$  (H2a;  $z = 2.251, p = .012$ ) and  $PC_{(sit)-PROT_{(sit)}}$  (H2b;  $z = 3.694, p < .001$ ). Thus, we accept H2a as well as H2b.

Regarding privacy risks, the effect the effect size of  $RISK_{(sit)-D_{(sit)}}$  ( $r = -.354 [-.483; -.209]$ ) is compared in H3a with the effect size of  $RISK_{(gen)-D_{(gen)}}$  ( $r = -.15 [-.248; -.049]$ ) and in H3b with the effect size of  $RISK_{(cont)-D_{(cont)}}$  ( $r = -.354 [-.447; -.254]$ ). All of these effects are negative and significant. Regarding the hypothesized differences in effect sizes, their CIs overlap. However, the effect size comparison test in H3a displays the negative effect of  $RISK_{(sit)-D_{(sit)}}$  to be significantly stronger ( $z = -2.308, p = .011$ ). Thus, we accept H3a. The effect size comparison test in H3b leads to a non-significant result ( $z = .005, p = .502$ ). Thus, we can not accept H3b as in both combinations the effect sizes are almost equally large. Additionally, it can be noted, that all papers that examined a direct effect of privacy risks on disclosure behavior have observed a significant direct effect. This is not the case for effects of privacy concerns on disclosure or protection behavior.

For H4, we compare the effect sizes for the situational-situational abstraction level combinations  $PC_{(sit)-D_{(sit)}}$  ( $r = -.164 [-.255; -.07]$ ) and  $RISK_{(sit)-D_{(sit)}}$  ( $r = -.354 [-.483; -.209]$ ). The CIs of these effects overlap but the effect size comparison test results in a significant larger effect size for the effect of  $RISK_{(sit)-D_{(sit)}}$  ( $z = -2.204, p = .014$ ). Thus, we accept H4.

## 5 Discussion, Implications and Limitations

### 5.1 Discussion and Implications

We find that most studies apply privacy concerns on a general level. In line with H1a and H1b the aligned abstraction level combination  $PC_{(gen)-D_{(gen)}}$  exerts the strongest negative effect of all aligned combinations regarding the effect of privacy concerns on disclosure behavior. Thus, H1a and H1b is accepted.

For the positive effect of privacy concerns on protection behavior, the aligned abstraction level combination  $PC_{(gen)-PROT_{(gen)}}$  exerts the strongest effect among all combinations. This difference was in each comparison statistically significant, leading to the acceptance of H2a and H2b. Additionally, most studies in our sample that examine effects of privacy concerns apply a general abstraction level

for this construct. Only two studies apply a situational abstraction level. This is in line with our understanding of privacy concerns as a general self-schema.

Regarding the effect of privacy risks on disclosure behavior, we find a larger effect size for  $RISK_{(sit)}-D_{(sit)}$  compared to  $RISK_{(gen)}-D_{(gen)}$ , thus we accept H3a. However, the effect sizes for  $RISK_{(sit)}-D_{(sit)}$  and  $RISK_{(cont)}-D_{(cont)}$  were equally strong. Thus, we cannot accept H3b. When comparing the effects  $RISK_{(sit)}-D_{(sit)}$  and  $PC_{(sit)}-D_{(sit)}$  privacy risks exert the stronger effect, thus we accept H4.

This work offers 4 specific contributions:

*First*, we provide a refined perspective on privacy concerns since we interpret privacy concerns as a self-schema that reflects users' disposition to develop concerns regarding privacy threats in general. Therefore, this construct should have the strongest effect on disclosure / protection behavior when the independent and dependent variable are aligned, i.e., measured on the same abstraction level and when privacy concerns are conceptualized and measured, as originally intended, on a general abstraction level. The obtained meta-analysis results confirm this effect size order.

This refined understanding for privacy concerns and the resulting effect sizes helps to interpret several study results more easily. For example, understanding privacy concerns as a general self-schema explains why it exerts a distinct effect in the study of Mothersbaugh et al. (2012) where two distinct disclosure situations exist. They compare a highly sensitive versus a low sensitive data disclosure. In the high sensitivity scenario, privacy concerns impact disclosure behavior negatively, as high inclination to develop privacy concerns lead to a high perception of privacy risks and a low willingness to disclose data. In the low sensitivity scenario, the effect of privacy concerns is positive, as to our understanding, a high general inclination to develop privacy concerns leads to a less negative or maybe even positive effect when the users are "positively surprised" in a specific situation where personal data is used sparingly or not at all (cf. Mothersbaugh et al., 2012). In contrast, a cost construct such as privacy risks, should exert only a negative effect on the disclosure behavior, as perceiving privacy risks is always connected to a reduced disclosure behavior (cf. Smith et al., 2011). Additionally, with our refined understanding it seems reasonable that privacy concerns exert only a weak or no significant direct effect on willingness to disclose as privacy concerns do primarily impact perceived privacy risks, which are the context or situation specific manifestation of privacy concerns. This explains that the direct effect of privacy concerns on disclosure willingness is rather weak or not significant at all when examining privacy risks in the same structural equation model (e.g., Kehr, Kowatsch, et al., 2015; Alashoor, Al-Maidani and Al-Jabri, 2018). However, privacy concerns do mostly at least indirectly impact users' disclosure behavior, e.g., through perceived privacy risks (e.g., Malhotra et al., 2004; Dinev et al., 2015; Kehr, Kowatsch, et al., 2015), applied protection settings (Chen, 2018; Zhang, Wang, Khansa and Kim, 2018), or via their trust (Mothersbaugh et al., 2012). Furthermore, this refined understanding of privacy concerns can help to explain some inconsistent results, even when privacy risks are not in the same model with privacy concerns and even when aligned abstraction level combinations are used. For instance, the non-significant and significant effects of privacy concerns on disclosure behavior can sometimes be explained due to a mix of the wording types in the measurement items, which leads to capturing distinct constructs (e.g., mix of "expectations of others' behavior" and "one's concern for others behavior" in Jiang et al., 2013; or in Heravi et al., 2018).

As our understanding is applicable for (most) previous studies and their results, we strongly suggest understanding privacy concerns in future studies as a general self-schema and interpret the results accordingly. With this refined conceptualization it becomes also obvious that the construct privacy concerns is especially important to examine cultural differences in regard to privacy needs, or as antecedent respectively as additional control variable for privacy risks research (e.g., Kehr, Kowatsch, et al., 2015; Heales, Cockcroft and Trieu, 2017).

The *second* contribution is a refined understanding of privacy risks. We interpret perceived privacy risks as a disclosure specific perception, which is a manifestation of the general disposition to develop privacy concerns. We observe that in line with H3a privacy risks have a weaker effect on disclosure behavior in the general-general abstraction level combination compared to the situational-situational

level combination. However, no difference between the contextual-contextual and situational-situational level can be observed leading to non-acceptance of H3b. Thus, these results confirm our expectations to the extent that privacy risks exert a stronger effect when it is somehow specified, independent whether a contextual or a even more particular situational abstraction level is applied. For privacy risks a contextual or situational abstraction level was mostly applied in the identified studies. In line with our understanding of privacy risks as a specific manifestation of the general inclination to develop privacy concerns, the effect size for the aligned situational and contextual abstraction level combination is larger than for the aligned general combination. Thus, we suggest using privacy risks to reflect privacy costs in a rather specific disclosure situation. Furthermore, all identified studies that include privacy risks applied for the dependent variable rather automatically the same abstraction level as for the privacy risks. Additionally, for privacy risks the problem of mixed item wording seems not as pronounced as it is for privacy concerns. Therefore, we strongly suggest using privacy risks to reflect privacy costs whenever possible. This could also help to increase comparability across studies in the future. However, only few quantitative privacy paradox studies examine privacy risks, which should change in the future as privacy risks have at least one significant effect on disclosure behavior in all papers we identified, independent of the abstraction level, which is in line with the privacy calculus (Smith et al., 2011; Y. Li, 2012; Dinev et al., 2015). We could not identify a privacy paradox study that examines the effect of privacy risks on protection behavior. Thus, we suggest to also consider privacy risks and its effects in privacy paradox research more detailed.

*Third*, we can confirm and extend the observation of Davazdahemami et al. (2018) with a more methodological meta-analysis approach. We confirmed that unaligned abstraction level combinations, i.e., different abstraction levels applied for dependent and independent variables, lead to rather weak or non-significant effects. This can be observed in our results especially for the effect of privacy concerns on disclosure behavior (e.g., Zafeiropoulou et al., 2013; Kehr, Kowatsch, et al., 2015; Pentina, Zhang, Bata and Chen, 2016). This helps to explain paradoxical situations, e.g., individuals do not necessarily act in every situation in accordance with their own general self-schema as situation specific information or circumstances make them act differently (e.g., Zafeiropoulou et al., 2013). However, the study of Davazdahemami et al. (2018) did not distinguish the conceptualization of privacy concerns and privacy risks, which we provided in this study. Also, a prediction was missing for the differences in effect sizes when independent and dependent variables are aligned, i.e., measured on the same abstraction levels. Such an effect size order prediction is only possible with the refined understanding provided in this study, which leads to our next contribution.

*Fourth*, we verified that our prediction for the effect size order based on the refined understanding of privacy concerns and privacy risks is mostly correct. In combination with the provided Pearson's  $r$  estimates, this could be helpful for future studies to estimate their needed sample size more accurately in advance (cf. Anderson, Kelley and Maxwell, 2017). Additionally, this study allows to better interpret and compare effect sizes of previous conducted privacy concerns and privacy risks studies.

Overall, the results are mostly in line with our interpretation of privacy concerns as general self-schema that reflect users' inclination to develop privacy concerns. While privacy risks are the more specific, either contextual or situational, manifestation of the privacy concerns. Therefore, we argue privacy risks are suited to reflect the privacy costs in a particular situation. With this study we raise awareness to consider abstraction levels to fit one's research aim and we discussed adequate application possibilities of privacy concerns and privacy risks. This helps to understand even paradoxical seeming results. We also observe that the effect of users' perceived privacy risks, especially its effects on protection behavior is underexamined in the identified literature, which could offer an interesting road for future research: to clarify if and under which circumstances situational perceived risks increase protection behavior.

## **5.2 Limitations**

Our findings should be examined in light of their limitations, which are discussed in this chapter. One limitation is that the structured literature review does not include all studies which examined the discussed effects quantitatively. Only those studies, that place themselves as a privacy paradox study are included. However, this limitation helps to prevent a publication bias towards significant effects and thus helps to obtain more precise effect size estimations.

One assumption of the conducted effect size comparison test assumes that all participants are distinct between the (sub-)samples. However, this is valid for most of the comparisons but in few comparisons some participants can be part of both (sub-)samples due to the meta-analysis procedure. Also, due to the nature of meta analysis, there is a high number of participants in some (sub-)samples which could lead to observe even the slightest differences as significant when applying the effect size comparison test. However, we verified the differences of the respective effects additionally based on the significance of the effects and the non-overlap of the effects' confidence intervals whenever possible. Nevertheless, the results of the effect size comparison test must be interpreted with caution.

In this meta-analysis, we attempted to reduce the heterogeneity in the study samples by dividing the distinct studies according to their abstraction level combinations. However, a high amount of heterogeneity is still existent in the subsamples, e.g., due to different covariates or different measurement instruments. It was not possible to further reduce the heterogeneity with additional subdividing due to the already very small number of papers in the subsamples, which is another limitation. Additionally, not all of the included studies used adequate item wording for measuring privacy concerns. Also, not all studies used the same measurement instruments for the variables or used the same statistical methods across studies, which could increase heterogeneity and distort the results (cf. Hong and Thong, 2013; Quintana, 2015). Thus, the results of the effect sizes must be interpreted extra carefully with the limitations in mind. To provide more reliable results, future meta-analyses should also include non-paradox studies to maintain a sufficient number of studies in the subsamples (and compare their results with our estimated effect sizes to assess their publication bias). A sufficient number of studies in a subsample should at best still be achieved after splitting the studies according to more relevant factors than the abstraction level in order to reduce heterogeneity to an acceptable level. Such factors could be the applied mental effort to assess privacy risks (cf. Dinev et al., 2015), adequate wording for privacy concerns (Hong and Thong, 2013), or the measurement type used for the privacy behavior construct (i.e., intention, willingness, self-report, or actual behavior), and consider the applied statistical methods as this could lead to distinct results (cf. Norberg et al., 2007; Junco, 2013; Staddon, Acquisti and LeFevre, 2013). Applying such an even more fine granular view could reduce heterogeneity significantly and allow an even better comparison of privacy studies.

## 6 Appendix

Study [sample size]	Significant direct effects [direction]	Significant total indirect effects [direction]	Non-Significant direct effects [direction]	Construct names (abstraction level; measurement type)
Aivazpour and Rao (2020) [n=242]	PC(gen) - D(sit) [-]; RISK(sit) - D(cont) [-]	PC(gen) - D(sit) [-]		PC: „General Privacy Concerns“ (gen);RISK: „Situation-Specific Perceived Risks“ (sit); D: "Intention to Disclose Private Information" (sit, int)
Alashoor et al. (2018) [n=273]	RISK(cont) - D(cont) [-]		PC(cont) - D(cont) [+]	PC: "Privacy Concerns" (cont);RISK: "Perceived Privacy Risk" (cont); D: "Disclosure Likelihood" (cont, int)
Chen (2018) [n <sub>s1</sub> =1141; n <sub>s2</sub> =1131]	PC(cont) - D1(cont) [-] (s1); PC(cont) - D2(cont) [+] (s2); 2x: PC(cont) - PROT1(cont) [+] (s1+s2)		PC(cont) - D1(cont) [-] (s2); PC(cont) - D2(cont) [+] (s1)	PC: "Privacy Concerns" (cont); D1: "Self-Disclosure" (cont, sr/int); D2: "Friending" (cont, sr); PROT1: "Limiting Profile Visibility" (cont, sr);
Davazdahemami et al. (2018) [n=180]	PC3(sit) - D(sit) [-]	PC2(cont) - D(sit) [-]; PC1(gen) - D(sit) [-];	PC2(cont) - D(sit) [-]; PC1(gen) - D(sit) [-]	PC1/2/3: "General/Contextual/Situative concerns for information privacy" (gen/cont/sit); D: "Willingness to share information" (sit, int)
Dienlin and Trepte (2015) [n=595]	PC(gen) - D3(cont) [-]; [+]; PROT1(cont, int) - PROT2(cont, sr) [+]	PC(gen) - D7(cont) [-]; PC(gen) - PROT1(cont) [+]; PC(gen) - D8(cont) [-]; PC(gen) - D9(cont) [-]; PC(gen) - PROT2(cont) [+]; PC(gen) - D10(cont) [-]	PC(gen) - D1(cont) [-]; PC(gen) - D2(cont) [-]; PC(gen) - D4(cont) [-]; PC(gen) - D5(cont) [-]; PC(gen) - D6(cont) [-]	PC: "Privacy concerns" (gen); D1: "Online Disclosure of the authentic first name" (cont, sr); D2: "Online disclosure of the authentic second name" (cont, sr); D3: "Online disclosure of the personal address" (cont, sr);D4: "Online disclosure of the cell-phone number" (cont, sr); D5: "Postings of political or religious views on Facebook" (cont, sr);D6: "Frequency of posts on SNSs" (cont, sr); D7:"Informational privacy intention" (cont, int); D8:"Informational privacy behavior" (cont, sr); PROT1:"Social privacy intention" (cont, int); PROT2:"Social privacy behavior" (cont, sr); D9:"Psychological privacy intention" (cont, int); D10:"Psychological privacy behavior" (cont, sr);
Dinev and Hart (2006) [n=369]	RISK(gen) - D(gen) [-]; PC(gen) - D(gen) [-]	RISK(gen) - D(gen) [-]		RISK: "Perceived Internet privacy risk" (gen);PC: "Internet privacy concerns" (gen); D: "Willingness to provide personal information to transact on the Internet" (gen, int)
Fatima et al. (2019) [n=37]	PC(gen) - PROT(gen) [+]; PROT(gen) - D1(gen) [+]		PC(gen) - D2(cont) [-]	PC: "Privacy concerns" (gen); D1: "Self-disclosure behavior" (gen, sr); D2: "Near-future intentions" (cont, int); PROT: "Distant-future intentions" (gen, int)
Gómez-Barroso, Feijóo and Palacios (2019) [n=1500]	PC(gen) - D(sit) [-]			PC: "Privacy Concern" (gen); D: "Information Disclosure" (gen, sr)
H. Li et al. (2017) [n=152]	PC(gen) - D(sit) [-]			PC: "General Privacy Concerns" (gen); D: "Behavioral Intention to Disclose Personal Information" (sit, int)
Hallam and Zanella (2017) [n=222]	PC(gen) - PROT(gen) [+];			PC: "Privacy concerns" (gen); PROT: "Privacy protection index" (gen, sr)
Heravi et al. (2018) [n=521]	PC(cont) - D(cont) [-]; PC(cont) - PROT(cont) [+]			PC: "Total information privacy concerns" (cont); D: "Total self-disclosure" (cont, sr); PROT: "Privacy protection behavior" (cont, sr)

Study [sample size]	Significant direct effects [direction]	Significant total indirect effects [direction]	Non-Significant direct effects [direction]	Construct names (abstraction level; measurement type)
Jiang et al. (2013) [n=251]	PC(sit) - D(sit) [-]; PC(sit) - PROT(sit) [+]			PC: "Privacy Concerns" (sit); D: "Self-disclosure" (sit, sr); PROT: "Misrepresentation" (sit, sr)
Kehr, Kowatsch, et al. (2015) [n <sub>s1</sub> =186; n <sub>s2</sub> =228]		2x: PC(cont) - D(sit) [-/-] (sample 1/2); 2x: RISK(sit) - D(sit) [-/-] (sample 1/2)	2x: PC(cont) - D(sit) [-/-] (sample 1/2)	PC: "General Privacy Concerns" (gen/cont)RISK: "Perceived Risks of Information Disclosure" (sit); D: "Intention to Disclose" (sit, int)
Kehr, Wentzel, Kowatsch and Fleisch (2015) [n=94]			2x: PC(cont) - D(sit) [+/+] (s1/s2); 2x: PC(cont) - CD(sit) [+/-] (s1/s2)	PC: "Perceived privacy concern" (cont); D: "Mobile apps use" (sit, sr); CD: "Mobile apps use intention" (sit, int)
Lee, Park and Kim (2013) [n=36]	RISK(cont) - D(cont) [-]			RISK: "Perceived total risk" (cont); D: "Intention to Share" (cont, int);
Lutz and Strathoff (2014) [n=1002]	PC(cont) - PROT(gen) [+]			PC: "Privacy Concerns" (cont); PROT: "Privacy Protection Behavior" (gen, sr)
Mosteller and Poddar (2017) [n=439]		PC(cont) - CD(cont) [+]	PC(cont) - CD(cont) [-]	PC: "Concerns for social media information privacy" (cont); CD: "Continuance intention to create UGC" (cont, int)
Mothersbaugh et al. (2012) [n=716]	PC(gen) - D2(sit) [-]; PC(gen) - D3(sit) [+]		PC(gen) - D1(sit) [-]	PC: "Consumer Online Privacy Concern" (gen); D1: "Willingness to Disclose Online" (sit, int); D2: D1 for High Data Sensitivity Scenario (sit, int); D3: D1 for Low Data Sensitivity Scenario (sit, int);
Norberg et al. (2007) [n <sub>1</sub> =83; n <sub>2</sub> =55]	D1(sit, int) - D2(sit, ab) [+]; RISK(sit) - D1(sit, int) [-]		RISK(sit) - D2(sit, ab) [-]	RISK: "Risk" (sit); D1: "Willing to disclose" (sit, int); D2: "Actually disclosed" (sit, behavior)
Pentina et al. (2016) [n=130]	PC(gen) - PROT(gen) [+]; PC(gen) - D2(cont) [-]; D2(cont, int) - D1(gen, sr) [+]		PC(gen) - D2(cont) [-]; PROT(gen) - D1(gen) [+]	PC: "Privacy concerns" (gen); D1: "Self-disclosure behavior" (gen, sr); D2: "Near-future intentions" (cont, int); PROT: "Distant-future intentions" (gen, int)
Sheehan and Hoy (1999) [n=889]	PC(gen) - D(gen) [-]; PC(gen) - PROT2/3/4(gen) [+]		PC(gen) - PROT1(gen) [+]	PC: "Total Privacy Concerns" (gen); D: "Registering for web site" (gen, int/sr); PROT1: "Providing inaccurate information" (gen, int/sr); PROT2: "Providing incomplete information" (gen, int/sr); PROT3: "Notifying ISP about unsolicited e-mail" (gen, int/sr); PROT4: "Requesting removal from mailing list" (gen, int/sr)
Son and Kim (2008) [n=523]	PC(gen) - D(gen) [-]; PC(gen) - PROT2-4(gen) [+]		PC(gen) - PROT1(gen) [+]	PC: "Information Privacy Concerns" (gen); D: "Refusal" (gen, int, reversed); PROT1: "Misrepresentation" (gen, int); PROT2: "Removal" (gen, int); PROT3: "Complaining Directly to Online Companies" (gen, int); PROT4: "Complaining Indirectly to 3rd-party Organizations" (gen, int)

Study [sample size]	Significant direct effects [direction]	Significant total indirect effects [direction]	Non-Significant direct effects [direction]	Construct names (abstraction level; measurement type)
Stutzman et al. (2012) [n=230]	PC(cont) - D(cont) [+]		PC(cont) - PROT(cont) [+];	PC: "Privacy concerns" (cont); D: "Facebook disclosures" (cont, sr); PROT: "Privacy behaviors" (cont, sr)
Taddicken (2014) [n=2739]	PC(gen) - D2(gen) [-];	PC(gen) - D1(gen) [+]	PC(gen) - D1(gen) [-]	PC: "Adapted Scale for Online Privacy Concern and Protection for Use on the Internet (APCP) (attitude)" (gen); D1: "Self-Disclosure" (gen; sr); D2: "General Willingness for Self-Disclosure" (gen; int)
Wang, Hu, Yan and Mei (2019) [n=913]	PC(gen) - D(cont) [-];			PC: "Privacy concern" (gen); D: "Self-disclosure intention" (cont, int)
Zafeiropoulou et al. (2013) [n=125]			PC(gen) - D(sit)	PC: "people's concerns over their online privacy in general" (gen); D: "Willingness to Share" (sit, int)
Zhang et al. (2018) [n=221]	PROT(cont) - D(cont) [-]	PC(cont) - D(cont) [-]		PC: "Privacy Concerns on Weibo.com" (cont); PROT: "Privacy Protection via Privacy Settings" (cont); D: "Peer-Rated Disclosure on Weibo.com" (cont, pr)

Table 2. Studies and their effects examined in our meta-analysis. Abbreviations: PC=Privacy Concerns, D=Disclosure Behavior, PROT=Protection Behavior, RISK=Privacy Risks; gen=general, cont=contextual, sit=situational; int=intention, sr=self-report, ab=actual behavior.<sup>3</sup>

<sup>3</sup> An extended version of this overview can be provided upon request (this includes effect sizes, mediators, measurement items with measurement sources, study design and context, etc.)



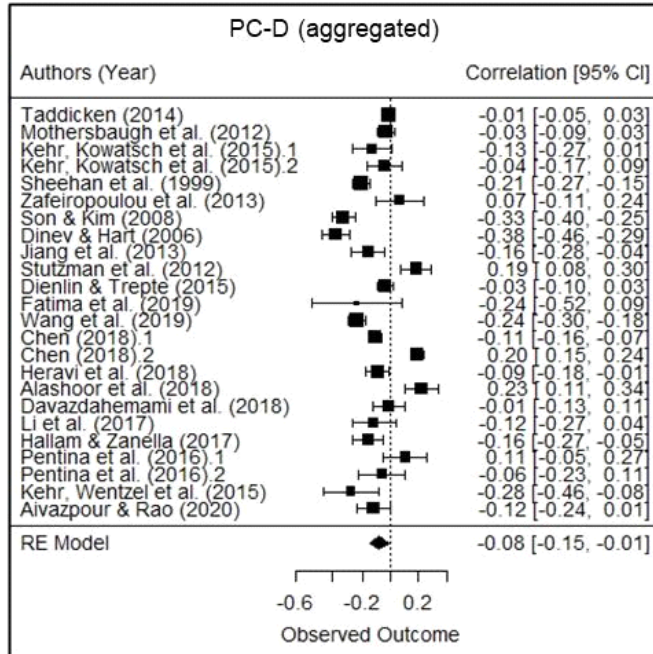


Figure 2. Forest plots of the aggregated effects of privacy concerns on disclosure behavior.

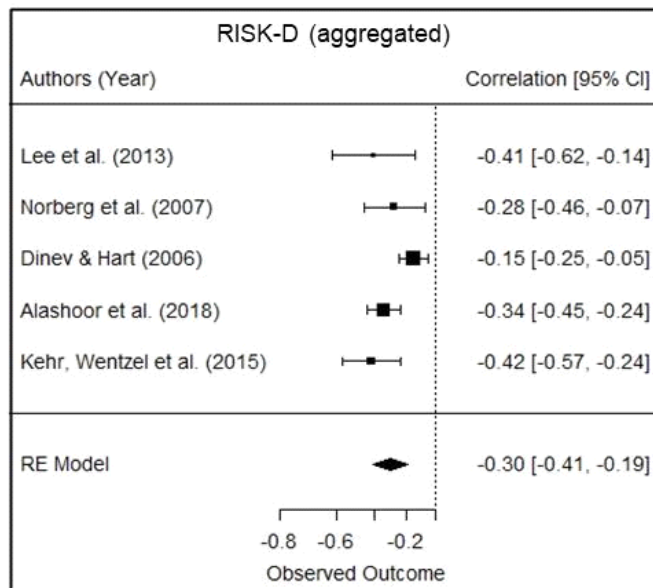


Figure 3. Forest plots of the aggregated effects of privacy risks on disclosure behavior.

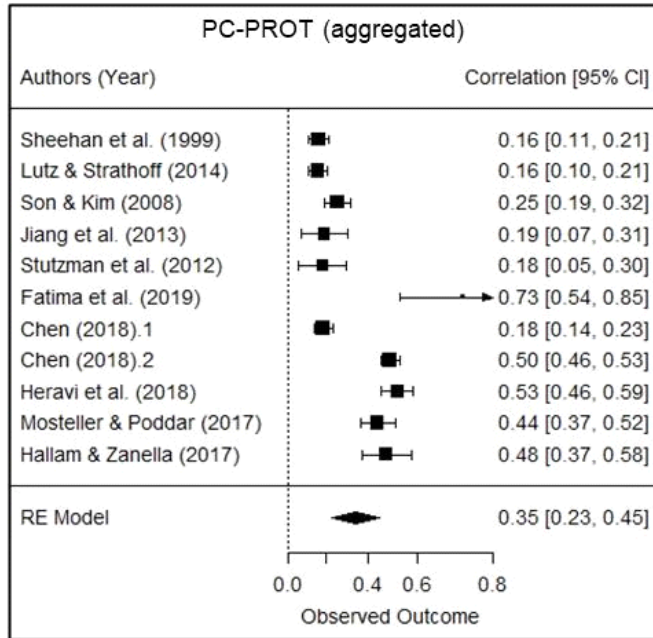


Figure 4. Forest plots of the aggregated effects of privacy concerns on protection behavior.

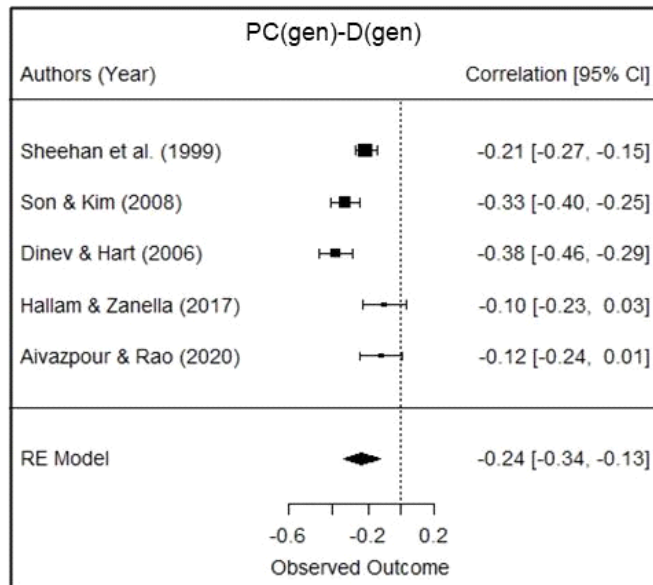


Figure 5. Forest plots of the effects of privacy concerns (general abstraction level) on disclosure behavior (general abstraction level).

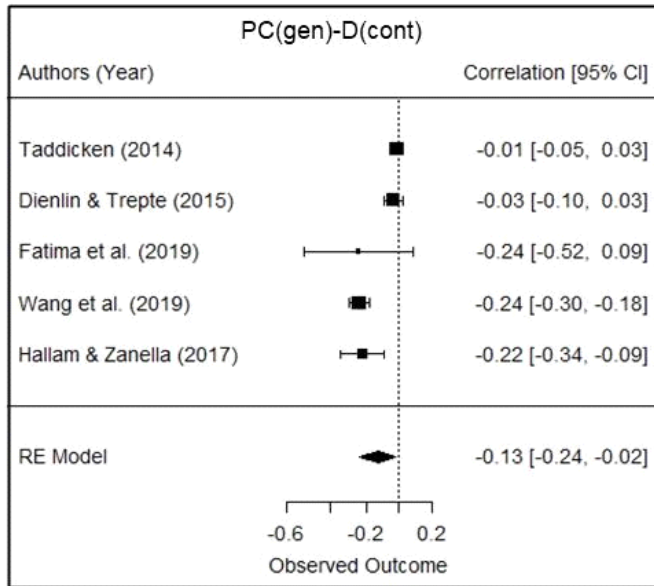


Figure 6. Forest plots of the effects of privacy concerns (general abstraction level) on disclosure behavior (contextual abstraction level).

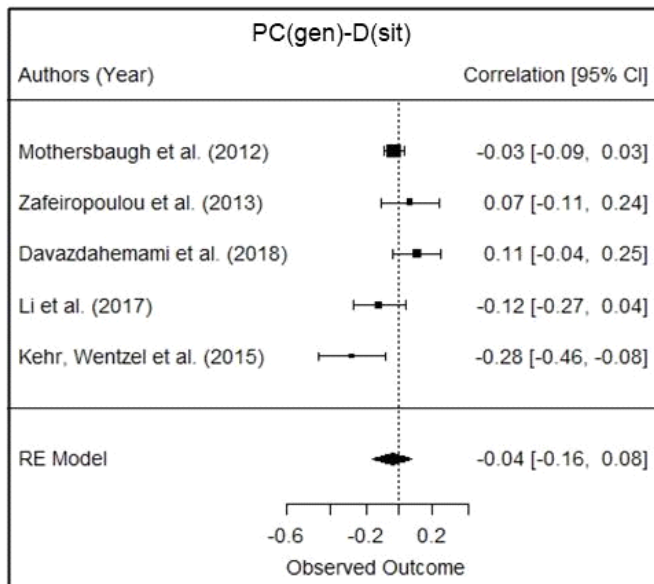


Figure 7. Forest plots of the effects of privacy concerns (general abstraction level) on disclosure behavior (situational abstraction level).

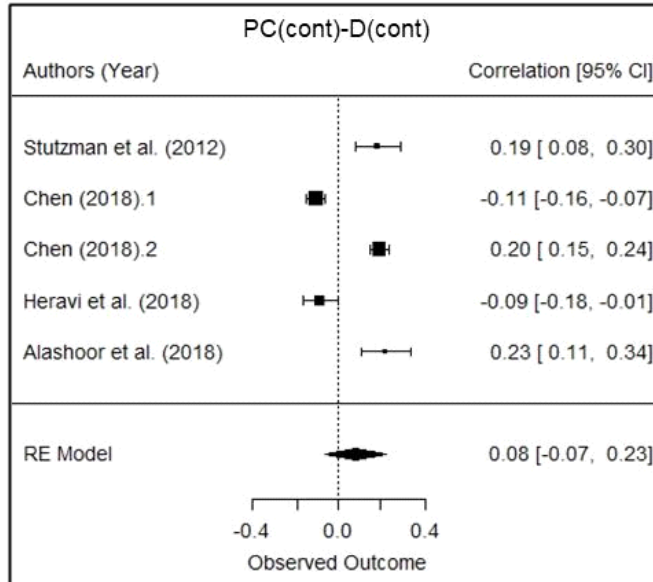


Figure 8. Forest plots of the effects of privacy concerns (contextual abstraction level) on disclosure behavior (contextual abstraction level).

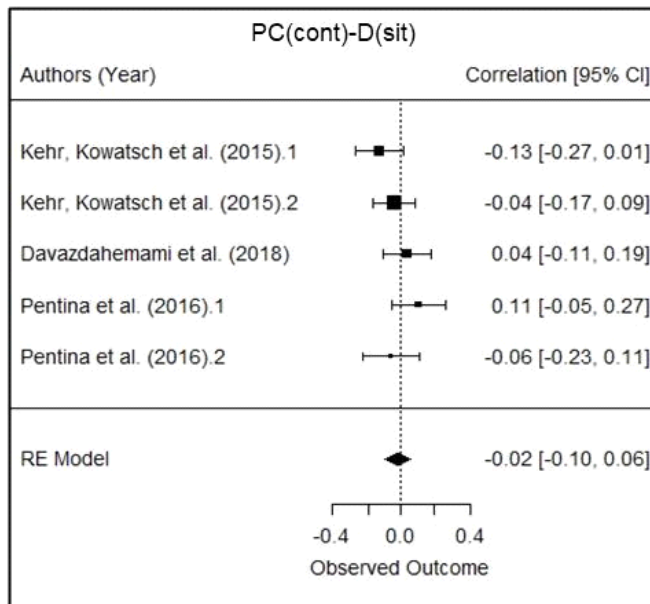


Figure 9. Forest plots of the effects of privacy concerns (contextual abstraction level) on disclosure behavior (situational abstraction level).

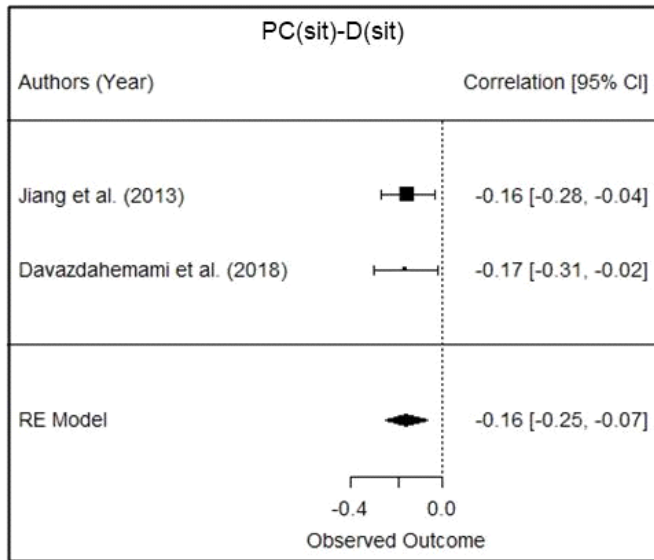


Figure 10. Forest plots of the effects of privacy concerns (situational abstraction level) on disclosure behavior (situational abstraction level).

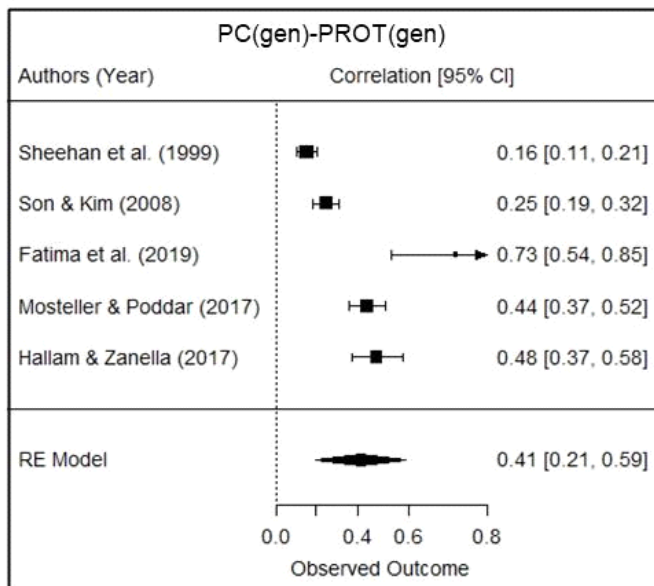


Figure 11. Forest plots of the effects of privacy concerns (general abstraction level) on protection behavior (general abstraction level).

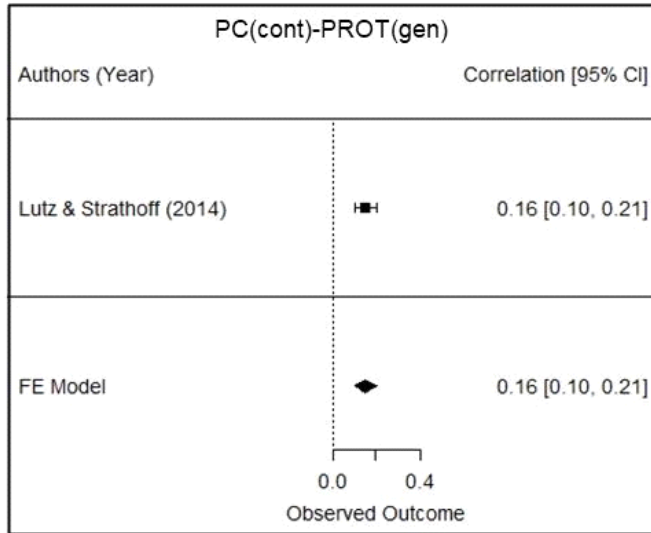


Figure 12. Forest plots of the effects of privacy concerns (contextual abstraction level) on protection behavior (general abstraction level).

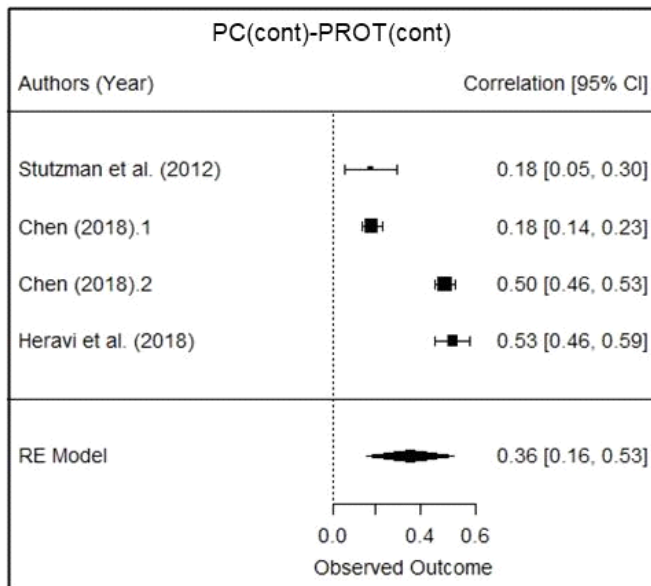


Figure 13. Forest plots of the effects of privacy concerns (contextual abstraction level) on protection behavior (contextual abstraction level).

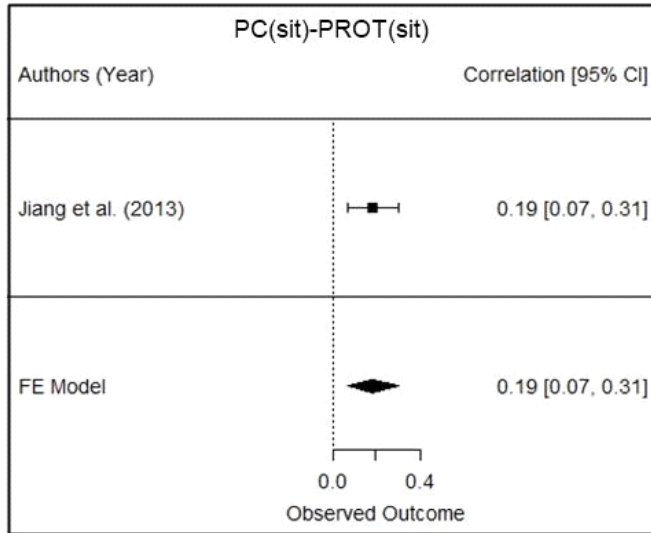


Figure 14. Forest plots of the effects of privacy concerns (situational abstraction level) on protection behavior (situational abstraction level).

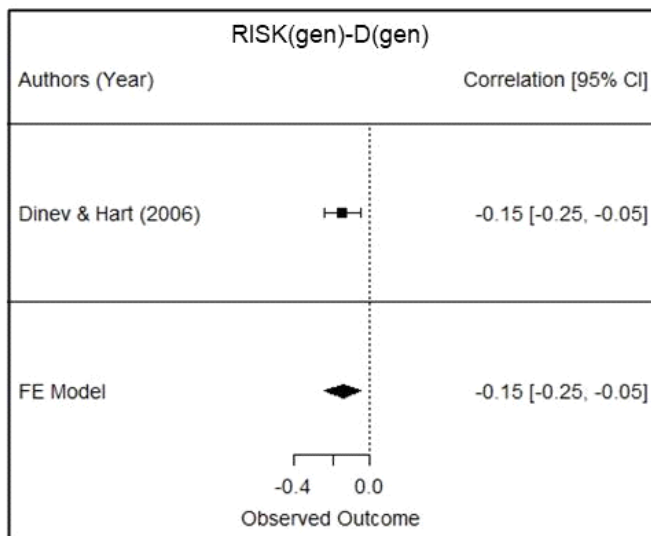


Figure 15. Forest plots of the effects of privacy risks (general abstraction level) on disclosure behavior (general abstraction level).

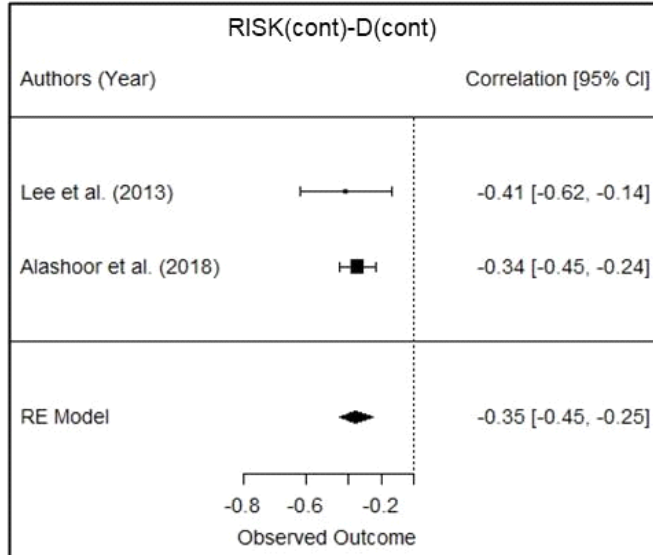


Figure 16. Forest plots of the effects of privacy risks (contextual abstraction level) on disclosure behavior (contextual abstraction level).

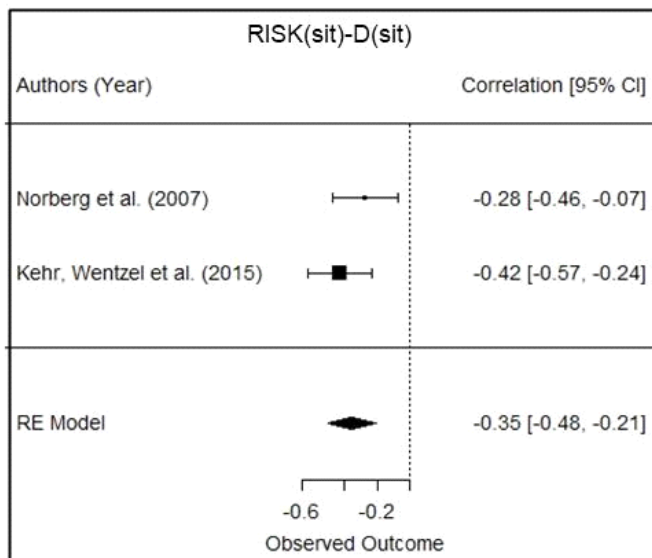


Figure 17. Forest plots of the effects of privacy risks (situational abstraction level) on disclosure behavior (situational abstraction level).



## References

- Aivazpour, Z. and V. S. (Chino) Rao. (2020). 'Information Disclosure and Privacy Paradox: The Role of Impulsivity'. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 51(1), 14–36.
- Alashoor, T., N. Al-Maidani and I. Al-Jabri. (2018). 'The Privacy Calculus under Positive and Negative Mood States'. In: *Proceedings of the 39th International Conference on Information Systems*. San Francisco: ICIS.
- Anderson, S. F., K. Kelley and S. E. Maxwell. (2017). 'Sample-Size Planning for More Accurate Statistical Power: A Method Adjusting Sample Effect Sizes for Publication Bias and Uncertainty'. *Psychological Science*, 28(11), 1547–1562.
- Balduzzi, S., G. Rücker and G. Schwarzer. (2019). 'How to perform a meta-analysis with R: a practical tutorial'. *Evidence-Based Mental Health*, 22(4), 153–160.
- Beresford, A. R., D. Kübler and S. Preibusch. (2012). 'Unwillingness to pay for privacy: A field experiment'. *Economics Letters*, 117(1), 25–27.
- Borenstein, M. (2009). 'Effect Sizes for Continuous Data'. In: H. Cooper, L. Hedges, & J. Valentine, *The handbook of research synthesis and meta-analysis* (2nd ed., pp. 221–235). New York: Russel Sage Foundation.
- Buchanan, T., C. Paine, A. N. Joinson and U.-D. Reips. (2007). 'Development of measures of online privacy concern and protection for use on the Internet'. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165.
- Chen, H.-T. (2018). 'Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management'. *American Behavioral Scientist*, 62(10), 1392–1412.
- Cox, D. F. and S. U. Rich. (1964). 'Perceived Risk and Consumer Decision-Making: The Case of Telephone Shopping'. *Journal of Marketing Research*, 1(4), 32–39.
- Davazdahemami, B., B. Hammer, A. Luse and P. Kalgotra. (2018). 'The Role of Parallelism in Resolving the Privacy Paradox of Information Disclosure in Social Networks'. In: *Proceedings of the 39th International Conference on Information Systems*. San Francisco: ICIS.
- Del Re, A. C. (2015). 'A Practical Tutorial on Conducting Meta-Analysis in R'. *The Quantitative Methods for Psychology*, 11(1), 37–50.
- Diedenhofen, B. (2016). Package 'cocor'. URL: <https://cran.uni-muenster.de/web/packages/cocor/cocor.pdf> (visited: 17.11.2020)
- Dienlin, T. and S. Trepte. (2015). 'Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors: The relation between privacy attitudes and privacy behaviors'. *European Journal of Social Psychology*, 45(3), 285–297.
- Dinev, T. and P. Hart. (2004). 'Internet privacy concerns and their antecedents - measurement validity and a regression model'. *Behaviour & Information Technology*, 23(6), 413–422.
- Dinev, T. and P. Hart. (2006). 'An Extended Privacy Calculus Model for E-Commerce Transactions'. *Information Systems Research*, 17(1), 61–80.
- Dinev, T., A. R. McConnell and H. J. Smith. (2015). 'Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box'. *Information Systems Research*, 26(4), 639–655.
- Fatima, R., A. Yasin, L. Liu, J. Wang, W. Afzal and A. Yasin. (2019). 'Sharing information online rationally: An observation of user privacy concerns and awareness using serious game'. *Journal of Information Security and Applications*, 48, 102351.
- Gartner. (2019a). 'Gartner Says Traditional Data and Analytics Strategies Cannot Satisfy Digital Business Demands'. URL: <https://www.gartner.com/en/newsroom/press-releases/2019-10-23-gartner-says-traditional-data-and-analytics-strategies-cannot-satisfy-digital-business-demands> (visited: 17.11.2020)
- Gartner. (2019b). 'How to Balance Personalization With Data Privacy'. URL: <https://www.gartner.com/smarterwithgartner/how-to-balance-personalization-with-data-privacy/> (visited: 17.11.2020)

- Gerber, A. S. and N. Malhotra. (2008). 'Publication Bias in Empirical Sociological Research: Do Arbitrary Significance Levels Distort Published Results?' *Sociological Methods & Research*, 37(1), 3–30.
- Gerber, N., P. Gerber and M. Volkamer. (2018). 'Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior'. *Computers & Security*, 77, 226–261.
- Gómez-Barroso, J. L., C. Feijóo and J. F. Palacios. (2019). 'Acceptance of Personalised Services and Privacy Disclosure Decisions: Results from a Representative Survey of Internet Users in Spain'. In: A. Lazazzara, R. C. D. Nacamulli, C. Rossignoli, & S. Za (Eds.), *Organizing for Digital Innovation* (pp. 63–76). Cham: Springer.
- Hallam, C. and G. Zanella. (2017). 'Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards'. *Computers in Human Behavior*, 68, 217–227.
- Heales, J., S. Cockcroft and V.-H. Trieu. (2017). 'The Influence of Privacy, Trust, and National Culture on Internet Transactions'. In: G. Meiselwitz (Ed.), *Social Computing and Social Media. Human Behavior* (pp. 159–176). Cham: Springer International Publishing.
- Heravi, A., S. Mubarak and K.-K. Raymond Choo. (2018). 'Information privacy in online social networks: Uses and gratification perspective'. *Computers in Human Behavior*, 84, 441–459.
- Hew, J.-J., G. W.-H. Tan, B. Lin and K.-B. Ooi. (2017). 'Generating travel-related contents through mobile social tourism: Does privacy paradox persist?' *Telematics and Informatics*, 34(7), 914–935.
- Hong, W. and J. Y. L. Thong. (2013). 'Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies'. *MIS Quarterly*, 37(1), 275–298.
- Jiang, Z. (Jack), C. S. Heng and B. C. F. Choi. (2013). 'Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions'. *Information Systems Research*, 24(3), 579–595.
- Jozani, M., E. Ayaburi, M. Ko and K.-K. R. Choo. (2020). 'Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective'. *Computers in Human Behavior*, 107, 106260.
- Junco, R. (2013). 'Comparing actual and self-reported measures of Facebook use'. *Computers in Human Behavior*, 29(3), 626–631.
- Kehr, F., T. Kowatsch, D. Wentzel and E. Fleisch. (2015). 'Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus'. *Information Systems Journal*, 25(6), 607–635.
- Kehr, F., D. Wentzel, T. Kowatsch and E. Fleisch. (2015). 'Rethinking Privacy Decisions: Pre-Existing Attitudes, Pre-Existing Emotional States, and a Situational Privacy Calculus'. In: *Proceedings of the 23th European Conference on Information Systems*. Münster: Association for Information Systems.
- Kokolakis, S. (2017). 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon'. *Computers & Security*, 64, 122–134.
- Lee, H., H. Park and J. Kim. (2013). 'Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk'. *International Journal of Human-Computer Studies*, 71(9), 862–877.
- Li, H., X. (Robert) Luo, J. Zhang and H. Xu. (2017). 'Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors'. *Information & Management*, 54(8), 1012–1022.
- Li, Y. (2012). 'Theories in online information privacy research: A critical review and an integrated framework'. *Decision Support Systems*, 54(1), 471–481.
- Lutz, C. and P. Strathoff. (2014). 'Privacy Concerns and Online Behavior Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses'. *SSRN Electronic Journal*.
- Malhotra, N. K., S. S. Kim and J. Agarwal. (2004). 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model'. *Information Systems Research*, 15(4), 336–355.

- Markus, H. (1977). 'Self-schemata and processing information about the self.' *Journal of Personality and Social Psychology*, 35(2), 63–78.
- Mosteller, J. and A. Poddar. (2017). 'To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors'. *Journal of Interactive Marketing*, 39, 27–38.
- Mothersbaugh, D. L., W. K. Foxx, S. E. Beatty and S. Wang. (2012). 'Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information'. *Journal of Service Research*, 15(1), 76–98.
- Norberg, P. A., D. R. Horne and D. A. Horne. (2007). 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors'. *Journal of Consumer Affairs*, 41(1), 100–126.
- Okazaki, S., M. Eisend, K. Plangger, K. de Ruyter and D. Grewal. (2020). 'Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review'. *Journal of Retailing*.
- Osatuyi, B. (2015). 'Empirical Examination of Information Privacy Concerns Instrument in the Social Media Context'. *AIS Transactions on Replication Research*, 1, 1–14.
- Pavlou, P. (2011). 'State of the Information Privacy Literature: Where are We Now and Where Should We Go?' *MIS Quarterly*, 35(4), 977–988.
- Pentina, I., L. Zhang, H. Bata and Y. Chen. (2016). 'Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison'. *Computers in Human Behavior*, 65, 409–419.
- Peter, J. P. and L. X. Tarpey. (1975). 'A Comparative Analysis of Three Consumer Decision Strategies'. *Journal of Consumer Research*, 2(1), 29–37.
- Peterson, R. A. and S. P. Brown. (2005). 'On the Use of Beta Coefficients in Meta-Analysis'. *Journal of Applied Psychology*, 90(1), 175.
- Quintana, D. S. (2015). 'From pre-registration to publication: a non-technical primer for conducting a meta-analysis to synthesize correlational data'. *Frontiers in Psychology*, 6.
- Risius, M., A. Baumann and H. Krasnova. (2020). 'Developing a New Paradigm: Introducing the Intention-Behaviour Gap to the Privacy Paradox Phenomenon'. In: *Proceedings of the 28th European Conference on Information Systems*. Online: ECIS.
- Sheehan, K. B. and M. G. Hoy. (1999). 'Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns'. *Journal of Advertising*, 28(3), 37–51.
- Sheeran, P. and S. Orbell. (2000). 'Self-schemas and the theory of planned behaviour'. *European Journal of Social Psychology*, 30(4), 533–550.
- Smith, H. J., T. Dinev and H. Xu. (2011). 'Information privacy research: an interdisciplinary review'. *MIS Quarterly*, 35(4), 989–1016.
- Smith, H. J., S. J. Milberg and S. J. Burke. (1996). 'Information Privacy: Measuring Individuals' Concerns about Organizational Practices'. *MIS Quarterly*, 20(2), 167–196.
- Son, J.-Y. and S. S. Kim. (2008). 'Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model'. *MIS Quarterly*, 32(3), 503–529.
- Staddon, J., A. Acquisti and K. LeFevre. (2013). 'Self-Reported Social Network Behavior: Accuracy Predictors and Implications for the Privacy Paradox'. In: *2013 International Conference on Social Computing* (pp. 295–302).
- Stutzman, F., J. Vitak, N. B. Ellison, R. Gray and C. Lampe. (2012). 'Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook'. In: *Proceedings of the 6th International AAAI Conference on Weblogs and Social Media* (pp. 330–337).
- Taddicken, M. (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), 248–273.
- Tsai, J. Y., S. Egelman, L. Cranor and A. Acquisti. (2010). 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study'. *Information Systems Research*, 22(2), 254–268.
- Wang, L., H.-H. Hu, J. Yan and M. Q. Mei. (2019). 'Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media'. *Journal of Enterprise Information Management*, 33(2), 353–380.

- Zafeiropoulou, A. M., D. E. Millard, C. Webber and K. O'Hara. (2013). 'Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?' In: *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 463–472). Paris: ACM.
- Zhang, J., W. Wang, L. Khansa and S. Kim. (2018). 'Actual Privacy Self-Disclosure on Online Social Network Sites: Reflective-Impulsive Model'. In: *Proceedings of the 39th International Conference on Information Systems* (p. 14). San Francisco.

# **The Effects of Positive Feelings and Arousal on Privacy Decision-Making**

**Author:** Tobias Steudner, University of Passau, Germany

**Presented at:** 23<sup>rd</sup> Biennial Conference of the International Telecommunications Society, 2021, online conference due to COVID-19

**Published in:** Proceedings of the 23<sup>rd</sup> Biennial Conference of the International Telecommunications Society, 2021

## **Abstract**

The goal of this study is to contribute to the underexplored interplay of unrelated positive feelings and arousal and their effects on users' willingness to provide personal data. To this end, we conduct an online survey (n=368) based on a hypothetical social network sweepstake scenario in which personal data, such as a photo, must be disclosed for participation. We perform structural equation modeling based on an extended privacy calculus model. Drawing on the feelings-as-information theory, more positively valenced feelings, even when evoked by an unrelated stimulus, should lead to a higher willingness to disclose personal data and participate in the sweepstake. We examine how arousal influences this effect as well as users' willingness to disclose. We find three significant crossover interactions for unrelated positive feelings and arousal, i.e., for more positively valenced feelings under higher arousal levels users are more willing to disclose data which is in line with the feelings-as-information theory. Surprisingly, less positively valenced feelings under low arousal levels also lead to a higher willingness to disclose personal data. We explain these results by additionally drawing on the affect regulation theory, which assumes that individuals try to protect their feelings in positive affective states and take actions in order to improve their feelings in less positive affective states. We interpret the arousal level as a "switch" that helps to determine which theory is suited best to predict the direction of the effect of unrelated positive feelings and thus, explain the observed crossover interactions: for high arousal levels, the feelings-as-information theory and for low arousal levels, the affect regulation theory fits best.

## THE EFFECTS OF POSITIVE FEELINGS AND AROUSAL ON PRIVACY DECISION-MAKING

Tobias Steudner

University of Passau,  
Chair of Business Information Systems,  
Passau, Germany,  
tobias.steudner@uni-passau.de

### Abstract

*The goal of this study is to contribute to the underexplored interplay of unrelated positive feelings and arousal and their effects on users' willingness to provide personal data. To this end, we conduct an online survey (n=368) based on a hypothetical social network sweepstake scenario in which personal data, such as a photo, must be disclosed for participation. We perform structural equation modeling based on an extended privacy calculus model. Drawing on the feelings-as-information theory, more positively valenced feelings, even when evoked by an unrelated stimulus, should lead to a higher willingness to disclose personal data and participate in the sweepstake. We examine how arousal influences this effect as well as users' willingness to disclose. We find three significant crossover interactions for unrelated positive feelings and arousal, i.e., for more positively valenced feelings under higher arousal levels users are more willing to disclose data which is in line with the feelings-as-information theory. Surprisingly, less positively valenced feelings under low arousal levels also lead to a higher willingness to disclose personal data. We explain these results by additionally drawing on the affect regulation theory, which assumes that individuals try to protect their feelings in positive affective states and take actions in order to improve their feelings in less positive affective states. We interpret the arousal level as a "switch" that helps to determine which theory is suited best to predict the direction of the effect of unrelated positive feelings and thus, explain the observed crossover interactions: for high arousal levels, the feelings-as-information theory and for low arousal levels, the affect regulation theory fits best.*

*Keywords: Arousal, Emotions, Feelings, Personal Data Disclosure, Privacy Calculus.*

## 1 Introduction

For every organization, it is important to know their users well to be able to personalize services and offer high value (Gartner, 2019). As a basis for successful value creation with personalized services it is necessary to acquire personal information: digital companies collect personal data, e.g., by analyzing user behavior on their websites (Weise, 2019) or by acquiring data more directly by organizing sweepstakes (Sendinblue, 2019), which can attract new users while also offering the possibility to learn more about them. It is especially important to know how users behave when disclosing personal data to be successful in data collection and personalization efforts. An often used theory to explain users' disclosure intention is the privacy calculus which assumes a weighing of benefits and privacy risks associated with the disclosure of personal data (Smith, Dinev and Xu, 2011). The privacy calculus is based on the theory of reasoned action, which assumes a purely "rational assessment" (Ajzen and Fishbein, 1980; Y. Li, 2012; Dinev, McConnell and Smith, 2015). This may be better described as a high-cognitive-effort decision-making process (Dinev et al., 2015).

However, to only consider high-cognitive-effort processing seems inadequate to explain disclosure decisions (Dinev et al., 2015). Thus, Dinev et al. (2015) call for more consideration of low-cognitive-effort processing in the disclosure making process. Likewise, many dual-process-theories suggest that both high-cognitive-effort processing as well as low-cognitive-effort processing play an important role in decision-making (Denes-Raj and Epstein, 1994; Slovic, Finucane, Peters and MacGregor, 2004; Kahneman, 2012; Evans and Stanovich, 2013). Some studies have already considered low-cognitive-effort processing, mostly with focus on emotional states that are directly related to the disclosure decision (e.g., Anderson and Agarwal, 2011; Wakefield, 2013; Kehr, Kowatsch, Wentzel and Fleisch, 2015; H. Li, Luo, Zhang and Xu, 2017).

We want to further contribute to this underexplored research field by focusing on the influence of unrelated feelings, i.e., feelings that were evoked by a decision-unrelated stimulus, as an instance of low-cognitive-effort processing. Previous studies showed that individuals oftentimes misattribute their feelings, which could make even unrelated feelings a factor that impacts privacy decisions (Schwarz and Clore, 1983; Antonetti and Valor, 2020). The *feelings-as-information theory* assumes that positive feelings lead to a more positive judgement even regarding objects or assessments that are not related to the feelings or its stimulus (Schwarz and Clore, 1983, 2003). According to this theory, positively valenced feelings, even when unrelated to the disclosure decision, could be the reason for distorted disclosure behavior whereby the individuals oftentimes tend to provide more personal data than intended (cf. Smith et al., 2011; Dinev et al., 2015). To better understand this issue, the focus of this study is on feelings that are unrelated to the disclosure decision. This focus complements the privacy research on feelings that are related to the disclosure decision (e.g., Anderson and Agarwal, 2011; Wakefield, 2013; Li et al., 2017).

Another aspect we want to address in the context of online privacy and low-cognitive effort processing is the impact of arousal: in other research fields the impact of arousal on decision-making is already acknowledged, for example the effect of arousal on individuals' risk perception in daily life (Hogarth, Portell, Cuxart and Kolev, 2011). Previous research also indicates that higher arousal levels increase individuals' decision-making based on low-cognitive-effort heuristics (cf. Lambert et al., 2003; Arieli and Loewenstein, 2006; Ditto et al., 2006), e.g., drawing on positive feelings for decision-making. However, only few and rather recent studies in the privacy context start to consider arousal as an important factor that alters individuals' personal data disclosure decision-making (e.g., Coker and McGill, 2020). Therefore, we are interested in the effects of positively valenced unrelated feelings and arousal on users' data disclosure decision-making, which leads to the following research question:

*How do positively valenced unrelated feelings and arousal levels impact individuals' willingness to disclose personal data?*

In order to address this research question, we conducted an online survey (n=368), in which the participants were given a hypothetical scenario to disclose personal data to participate in a social network site's (SNS) sweepstake. The participants were split into two groups. In the treatment group participants recalled an autobiographical happy event before the sweepstake scenario in order to evoke positive feelings unrelated to the disclosure task (cf. Martin, 1990). To explore the main and interaction effects of unrelated positive feelings and arousal levels on users' willingness to disclose and participate in a SNS-sweepstake, we use an extended form of the privacy calculus for the structural equation model. We find that positively valenced feelings as well as arousal levels directly increase perceived benefits. We also find significant crossover interaction effects of unrelated positive feelings and arousal on the disclosure willingness as well as on its antecedents in form of perceived privacy risks, and perceived risk severity.

In sum, we contribute to a refined understanding of the interplay of positive unrelated feelings and arousal levels: in this study, arousal levels determine whether the effect of unrelated positive feelings increase or decrease users' disclosure willingness. This confirms the need for future research to consider both, feelings and arousal levels, as only taken together, a more precise prediction of users' behavior can be made. Furthermore, we inform practitioners about the possibility to increase users' disclosure willingness by increasing the arousal level and evoking positively valenced feelings with an unrelated stimulus. However, we also discuss possible countermeasures for users that allow them to make decisions without being biased towards overdisclosure by those evoked feelings. With these discussed countermeasures, our study serves as a thought-provoking impulse for legislators to also consider non-cognitive factors, like unrelated feelings or arousal levels, which additionally could be considered to prevent individuals from overdisclosure of personal data.

## 2 Theoretical Background and Hypotheses Development

### 2.1 Privacy Calculus and Privacy Concerns

The privacy calculus is the dominant theory to explain users' personal data disclosure behavior (Smith et al., 2011; Dinev et al., 2015). The privacy calculus draws on the *maximum utility theory*, which means that users strive for the option with the highest utility among two or more possible decisions (Y. Li, 2012). Therefore, users intend to disclose their data only when they perceive a higher utility for disclosure compared to no-disclosure. The calculated utility results from a weighing of perceived benefits (e.g., monetary rewards or social benefits like easier communication with friends) and perceived costs. Costs in the context of data disclosures are mainly reflected by the privacy risks (e.g., loss of personal data or getting spam-mails) associated with data disclosure (Awad and Krishnan, 2006; Bansal, Zahedi and Gefen, 2010; Y. Li, 2012).

For this weighing task of benefits and privacy risks, a high-cognitive-effort calculation is mostly assumed, which is a limitation of the privacy calculus (Dinev et al., 2015). This cognitive aspect can be exemplarily illustrated when looking at how traditional literature explains individuals' risk assessments: the perceived risk of experiencing an unfavorable outcome is calculated by individuals with their perceived probability of the uncertain outcome multiplied by the perceived severity of the respective outcome (Sieber and Lanzetta, 1964; Cunningham, 1967). Thus, the higher the probability and/or the severity in the mind of the users, the higher the perceived privacy risk (Keith, Thompson and Greer, 2012). Therefore, we consider in our base model not only users' perceived benefit and perceived privacy risk, but we also include perceived severity and probability as antecedent for perceived privacy risk.

Besides perceived privacy risk, users' privacy concerns also decrease their disclosure willingness (Y. Li, 2012; Dinev et al., 2015). However, previous studies found mixed results regarding privacy concerns. Some studies found a direct effect on disclosure willingness (e.g., H. Li et al., 2017), while other studies found only an indirect effect on disclosure willingness which was mediated by perceived



privacy risks (e.g., Keith et al., 2012; Kehr et al., 2015). We interpret privacy concerns as a rather general, non-situational construct and thus, as an antecedent to privacy risks. However, we additionally test the direct effect of privacy concerns on willingness to disclose and participate in the sweepstake. This leads to the base model displayed in Figure 1.

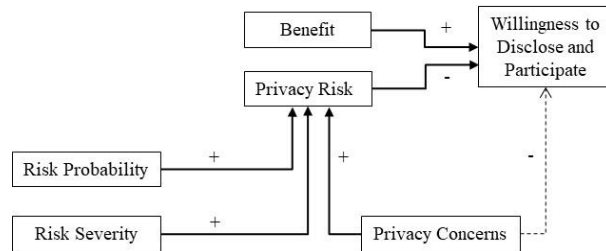


Figure 1. Structural equation base model

## 2.2 Low-Cognitive-Effort Processing

An attempt to understand users' data disclosure behavior in more detail is to not only consider their highly effortful cognitive utility assessments, but instead to also consider simpler assessments that only demand low cognitive effort (Dinev et al., 2015). Many researchers provide evidence for two processing systems (Epstein, 1994; Slovic et al., 2004; Kahneman, 2012; Evans and Stanovich, 2013). For example, Kahneman (2012) explains that there are two processing systems that both impact decision-making but behave completely differently: i) type one is intuitive, fast and automatic, requiring only low cognitive effort and ii) the second type is reasoning, slow and requires high cognitive effort like the above described privacy calculus or the risk assessment based on probability and severity displayed in our base-model.

But such a risk assessment, for instance, can also be done by the more intuitive processing system of type one which requires only low cognitive effort. Therefore, this system can depend on individuals' feelings, affective states or their intuitive reactions towards a certain situation (e.g., a data disclosure in form of a SNS-sweepstake participation) and its available cues (Loewenstein, Weber, Hsee and Welch, 2001; Slovic et al., 2004).

### 2.2.1 Feelings

There is a wide range of affective phenomena which also leads to some confusion or ambiguous use of certain terms, such as affect, mood, emotions and feelings (Rosenberg, 1998; Zhang, 2013). In this study, mood, feelings, and emotions are considered as a more specific manifestation of the umbrella term *affective state*. There is consensus that most affective states can be describe by their *valence*, i.e., the degree of pleasantness and unpleasantness, and their *arousal level*, i.e., their activation value (Russell, 2003; Zhang, 2013). A certain *mood* has oftentimes no specific stimulus and the affective state remains for a longer duration (Russell, 2003; Zhang, 2013). In contrast, we interpret emotion based on previous literature as an affective state induced by a certain stimulus. Thus, emotions are a reaction towards an object, or a certain behavior. Such evoked emotions have a shorter duration than a mood (Russell, 2003; Clore and Schnall, 2005; Scherer, 2005). We use the terms emotions and *feelings* as interchangeable synonyms of these short-lived feelings that are evoked by a certain stimulus (cf. Zhang, 2013).

The importance of feelings is discussed in Loewenstein et al.'s (2001) *risk as feelings theory*. This theory assumes that objectively relevant as well as non-relevant situational cues like the vividness or immediacy of the respective unfavorable outcome can impact individuals' feelings and their decision-making process.

Besides Loewenstein et al. (2001), other researchers confirm that low-cognitive-effort processes, e.g., in form of feelings, can influence decisions as well as the underlying cognitive evaluations (Schwarz and Clore, 1983; Petty and Cacioppo, 1986; Kahneman, 2012; Zhang, 2013). For example, positive feelings increase the decision intention itself (Wakefield, 2013). Positive feelings can also influence the cognitive evaluation process: positive emotions can decrease perceived privacy risk (Loewenstein et al., 2001; Chaudhuri, 2002; H. Li, Sarathy and Xu, 2011; Kehr et al., 2015; Bidler, 2020) and increase privacy protection beliefs or perceived benefit (H. Li et al., 2011; Kehr et al., 2015; Bidler, 2020).

### 2.2.2 Unrelated Feelings

Previous research has shown that feelings are often misattributed by individuals but nevertheless serve as robust and important determinants of assessments (Schwarz and Clore, 1983; Higgins, 1998; Dunn and Schweitzer, 2005). In this regard, the *feelings-as-information theory*, also known as the *mood-as-information theory*, was developed (Schwarz and Clore, 1983, 2003). This theory assumes that individuals use their feelings as source of information for the assessment of the current situation. This means, individuals assess an object more positively when they have more positively valenced feelings (Schwarz and Clore, 1983, 2003). In line with the feelings-as-information theory, more recent research, for example by Antonetti and Valor (2020), suggests that feelings toward a certain target A can spill over to another target B. Thus, feelings can influence judgements and decision-making processes despite being evoked by decision unrelated stimuli (cf. Schwarz and Clore, 2003; Dunn and Schweitzer, 2005; Harlé and Sanfey, 2007). Based on the feelings-as-information theory, we hypothesize that feelings evoked by stimuli unrelated to a certain personal data disclosure can influence users' willingness to disclose.

For example, individuals who obtained a product as a gift from a smiling person they liked, had a more positive attitude towards the product than persons who obtained the product from a person they did not like (Howard and Gengler, 2001). Similar results were obtained by Bidler et al. (2020) in the privacy context: positive affective reactions towards data disclosures inflate unrelated benefits and decrease unrelated risks. Thus, we argue that the effects of positively valenced feelings unrelated to the decision are similar to the effects of decision related positive feelings (cf. chapter 2.2.1). Therefore, we hypothesize that positively valenced unrelated feelings increase disclosure willingness as well as perceived benefit and decrease perceived privacy risk regarding a data disclosure in form of a SNS sweepstake participation:

*H1a: Positively valenced unrelated feelings increase users' willingness to disclose.*

*H2a: Positively valenced unrelated feelings increase users' perceived benefit.*

*H3a: Positively valenced unrelated feelings decrease users' perceived privacy risk.*

We expect that feelings can equally influence the antecedents of perceived privacy risk. Slovic et al. (2004) discuss that feelings impact the perception of probabilities, which is exemplarily illustrated in the studies by Slovic, Monahan and MacGregor (2000) and Yamagishi (1997). They show that giving information about the probability of a certain risk in form of the number of affected individuals compared to a percentual share will lead to a higher risk perception for the more affect-laden information in form of a proportion. The more affect-laden number of affected individuals leads to a higher risk perception. Equally, warnings in form of affect-laden scenarios are more influential than warnings in form of relative frequencies (Hendrickx, Vlek and Oppewal, 1989). Also, individuals provided with narrative information (rather affect-laden) can better predict outcomes than individuals provided with bars and data tables (Sanfey and Hastie, 1998). More evidence for the effects of the low-cognitive-effort system can be found in the study of Hogarth, Portell and Cuxart (2007): happy feelings reduce perceived risk probability and severity. Thus, we hypothesize analogously to the aforementioned hypotheses, that even unrelated positive feelings can decrease perceived risk severity and probability (cf. Howard and Gengler, 2001; Bidler, 2020):

*H4a: Positively valenced unrelated feelings decrease users' perceived privacy risk probability.*

*H5a: Positively valenced unrelated feelings decrease users' perceived privacy risk severity.*

### 2.2.3 Arousal

In order to understand individuals' reliance on the low-cognitive-effort system, arousal could help as this seems to alter individuals' assessments (Lambert et al., 2003; Ditto et al., 2006; Coker and McGill, 2020). Arousal is mostly described as an intensity dimension belonging to an emotional response (Deng and Poole, 2010). In line with this, we interpret high levels of arousal as an activation state of the organism, e.g., wide-awake (Deng and Poole, 2010). One mechanism that explains stronger reliance on low-cognitive-effort processing could lie in an increased arousal level. An increased arousal level could make low-cognitive-effort processing, respectively affective assessments, for decision-making more salient than analytical high-cognitive-effort processing (Svenson and Maule, 1993; Finucane, Alhakami, Slovic and Johnson, 2000; Lambert et al., 2003; Coker and McGill, 2020; Kim et al., 2020). For example, the reliance on stereotypical thinking is increased under high arousal levels (Lambert et al., 2003). Also, sexual arousal in males lead to an increased perception of womens' attractiveness, increased willingness to engage in morally questionable behavior or willingness to engage in unsafe sex (Ariely and Loewenstein, 2006). Similarly, individuals are more willing to have unsafe sex when they see a video instead of a description, i.e., when they were stronger aroused sexually (Ditto et al., 2006). Another study shows that individuals are more willing to risk their time to win cookies when they can see and smell them, i.e., when they are more strongly aroused, compared to individuals who cannot see and smell the cookies (Ditto et al., 2006). In the privacy context, an increased disclosure behavior is associated with higher levels of arousal (Coker and McGill, 2020). Thus, we expect that higher arousal reinforces the effects of positively valenced feelings and hypothesize accordingly (see also Figure 2):

*H1b: Positively valenced unrelated feelings increase users' disclosure willingness stronger under high arousal levels than under low arousal levels.*

*H2b: Positively valenced unrelated feelings increase users' perceived benefit stronger under high arousal levels than under low arousal levels.*

*H3b: Positively valenced unrelated feelings decrease users' perceived privacy risk stronger under high arousal levels than under low arousal levels.*

*H4b: Positively valenced unrelated feelings decrease users' perceived privacy risk probability stronger under high arousal levels than under low arousal levels.*

*H5b: Positively valenced unrelated feelings decrease users' perceived privacy risk severity stronger under high arousal levels than under low arousal levels.*

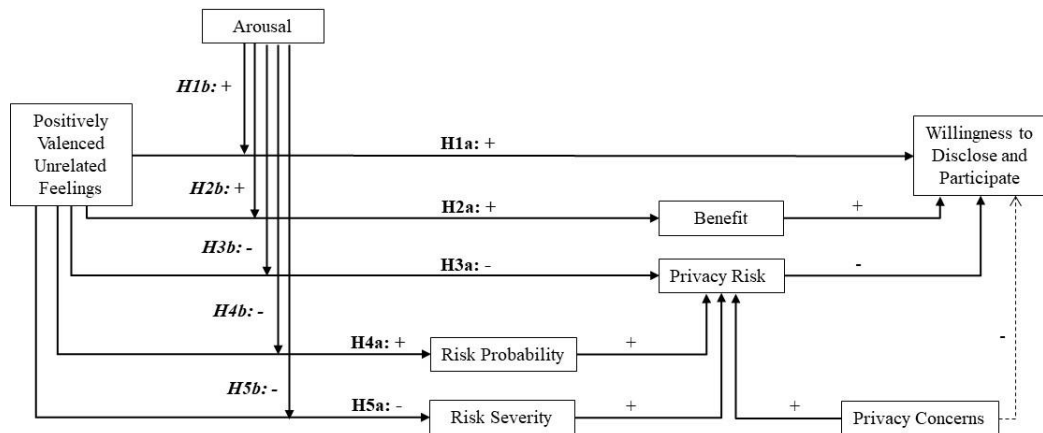


Figure 2. Structural equation model with an overview of the hypotheses. The direct effects of arousal on benefit, privacy risk, risk probability and risk severity are also tested, as it is necessary in order to test the interaction effects. For simplicity, these direct effects of arousal are not displayed in the model despite being tested.

### 3 Sample and Setup

Our survey was structured as follows: first, participants submitted demographic information, i.e., their age, sex, but also whether they have an Instagram account and are interested in the 1. or 2. Fussball-Bundesliga. Only when they were above 18 years old and had an Instagram account and were also interested in the 1. or 2. Bundesliga (due to the sweepstake context), they were able to continue the survey. A pre-test was conducted to verify the understandability of the survey. Afterwards, the survey data was collected from October until early November 2020 in cooperation with a panel provider in Germany.

We split the participants in two groups: in the treatment group (“happy” group) we let the participants recall a positive experience that made them feel happy. They were encouraged to imagine their experience as vividly as possible and to focus on the feelings that were evoked in this situation. They were asked to narrate their experience with up to 150 words. This method is known as autobiographical recall and is used to evoke positive affective states (Martin, 1990). It is thought to be a more effective manipulation of feelings than music and guided imagery combined and additionally, it is suited to be applied in an online survey (Westermann, Spies, Stahl and Hesse, 1996; Jallais and Gilet, 2010). We also verified that these positively valenced feelings were evoked by situations which were not related to the context of this study by reading their experience description before analyzing the data. After the feeling manipulation, we measured participants’ positively valenced unrelated feelings (PVUF) (Klapwijk and Van Lange, 2009) and arousal levels (AR) with a common semantical measurement instrument (Deng and Poole, 2010). The control group was not encouraged to re-experience a positive situation of their life. Instead, participants’ positive feelings and their arousal level was measured instantly, i.e., without any induction.

After these measurements, both groups were shown the exact same hypothetical scenario: participants had to imagine that the panel provider recommends an Instagram sweepstake, in which they can win one of two soccer jerseys of their favorite 1. or 2. Fussball-Bundesliga club. Additionally, the respective Instagram post was shown to the participants. The sweepstake is from a goalkeeper young talent training organization. It is a common Instagram sweepstake in which the Instagram account has to be followed and the post has to be liked as well as commented in order to participate. Additionally, for participation, one has to share a photo of oneself as a fan of one’s favorite club with the organization’s Instagram account. To make the hypothetical scenario as realistic as possible, an image

of the organization's official Instagram account was displayed. As an optional information source, participants could access even more information about the company, (i.e., information about the founder and employees as well as the company's aim).

After displaying the scenario to the participants, we measured their willingness to disclose and participate in the sweepstake (WDP), the perceived benefits (BENE) and privacy risks (RISK) associated with the participation, the perceived risks probability (PROB) and severity (SEV), and additionally their general privacy concerns (PC). For detailed measurement instrument information see Table 2 in the Appendix.

We ensured that the participants carefully read the questions and items of the survey. We obtained 368 valid observations that met the described criteria ("happy" group:  $n=177$ ; control group:  $n=191$ ; with an average age of 39 and with 50% females in total; for details on the participants' distribution see Table 3 in the Appendix).

## 4 Results

We verify via Fisher's permutation test that there are no differences between the two groups regarding sex ( $\Delta=.01$ ,  $p=.833$ ), age ( $\Delta=1.28$ ,  $p=.385$ ), general privacy concerns ( $\Delta=.07$ ,  $p=.617$ ), and arousal levels ( $\Delta=.09$ ,  $p=.547$ ). With the same method, we confirm the autobiographical manipulation in the happy group to be successful, i.e., that participants in the happy group have more positively valenced unrelated feelings ( $\Delta=.34$ ,  $p=.007$ ). We analyze the data with SmartPLS (version 3.3.2), which applies the partial least squares method (Wold, 1966; Joe F. Hair, Ringle and Sarstedt, 2011). Partial least squares structural equation modeling is particularly suited for predictive as well as exploratory research as done in this study. Furthermore, there are no distributional requirements for this method (Joe F. Hair et al., 2011). We use this method to test the measurement model as well as the hypothesized structural model (cf. R. P. Bagozzi and Yi, 1989; Gefen, Straub and Boudreau, 2000; J. F. Hair, Hult, Ringle and Sarstedt, 2016).

### 4.1 Measurement Model Assessment

We test for i) internal consistency reliability, ii) convergent validity, and iii) discriminant validity (J. F. Hair, Sarstedt, Ringle and Gudergan, 2017).

i) Cronbach's  $\alpha$  as well as composite reliability for all constructs are above the lower threshold of 0.7 (Richard P. Bagozzi and Yi, 2012), thus internal consistency reliability is achieved.

ii) In order to verify convergent validity, we assess the item loadings as well as the average variance extracted (AVE). The outer loadings of the items on their respective constructs should exceed 0.7 (Richard P. Bagozzi, Yi and Phillips, 1991; Joe F. Hair et al., 2011) but at least be above 0.4 (Henseler, Ringle and Sarstedt, 2015). All items' outer loadings are above 0.7, except for two items in the privacy concern measurement instrument. These two items have outer loadings above 0.6. This is still acceptable, as those items capture different aspects of privacy concerns and those items were taken from a well-established measurement instrument. The AVE for the constructs should exceed the threshold of 0.5 to confirm convergent validity (Joe F. Hair et al., 2011), which applies to all constructs.

iii) We confirm discriminant validity, by verifying that the following three criteria are met: all item loadings are greater than the respective cross-loadings on other constructs (Richard P. Bagozzi and Yi, 2012), the Fornell-Larcker criterion is met (Fornell and Larcker, 1981), and the constructs' heterotrait-monotrait ratios (HTMT) are even below the conservative threshold of 0.85 (Henseler et al., 2015).

## 4.2 Structural Model Assessment

Next, we assess the structural model and the hypothesized relationships. To verify that no collinearity issues are present between the exogenous latent variables, the variance inflation factors (VIFs) must be below the threshold of 5 for each construct (Thatcher and Perrewe, 2002). All VIF values are even below 1.43 (cf. Appendix Table 6 for details).

We perform a bootstrap procedure with 5,000 bootstrap samples to evaluate the significance of the path coefficients (two-sided).

The structural model is displayed in Figure 3. All path coefficients in the base-model have the expected directions and are highly significant. Regarding the direct effect of general privacy concerns on willingness to participate, we observe no direct significant effect. Instead, we only find an indirect significant effect of privacy concerns on the participation willingness, which is in line with our assumption, mediated by perceived privacy risks. Details of the path coefficient results are provided in Table 4 in the Appendix.

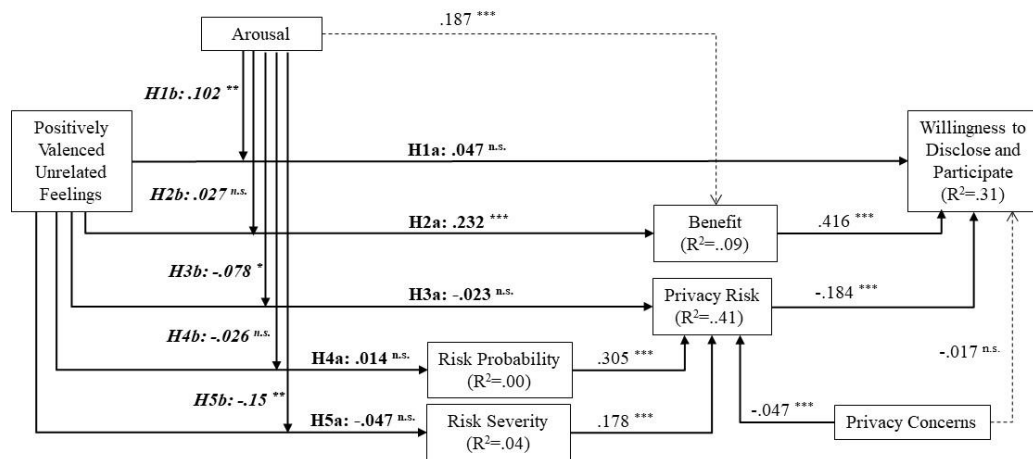


Figure 3. SEM results. Unhypothesized relationships are in dotted lines. Significance levels: n.s.,  $p > .05$ ; \*  $p \leq .05$ ; \*\*  $p \leq .01$ ; \*\*\*  $p \leq .001$ . The direct effects of arousal on privacy risk, risk probability and risk severity are also tested and are not-significant (see Table 4 in the Appendix). For simplicity, the non-significant direct effects of arousal are not displayed in this model despite being tested.

In Table 1, we additionally provide the effect sizes ( $f^2$ ). All effects in the base model are above the lower threshold of 0.02 (Cohen, 1988). Thus, our further analyses focus only on the hypothesized effects. We reject hypothesis 1a, as more positively valenced unrelated feelings do not significantly increase users' willingness to participate ( $r = .047$ ,  $p = .344$ ,  $f^2 = .003$ ). However, we find a significant interaction effect of arousal and positive feelings ( $r = .102$ ,  $p = .007$ ,  $f^2 = .018$ ). The size of the interaction effect remains slightly below Cohen's threshold of 0.02 for direct effects (Cohen, 1988; J. F. Hair et al., 2016). However, all observed interaction effect sizes in this study are still above the average interaction effect size published in psychological journals (Aguinis, Beaty, Boik and Pierce, 2005; Kenny, 2015). Regarding our interaction effects, the observed effect sizes should be rather interpreted as medium to large (cf. Kenny, 2015). Therefore, we accept H1b. When examining the slope (Figure 4, left), we observe that when users experience more positively valenced unrelated feelings, their willingness to participate increases under high arousal, but decreases under low arousal levels. Furthermore, in Figure 4 (left) a crossover interaction effect is observable (Loftus, 1978). This means that under less positively valenced feelings, the effect of arousal is inverted: with less

positively valenced feelings, higher arousal leads to a reduced willingness to participate while under low arousal levels, this results in an increase for users' willingness to participate.

Table 1. Resulting effect sizes. Bold:  $f^2 > .02$ ; italic:  $.02 > f^2 > .01$

IV	DVs					
	AR	PROB	SEV	RISK	BENE	WDP
PVUF		.000	.002	.001	<b>.059</b>	.003
AR		.000	.001	.000	<b>.037</b>	.009
PVUFxAR		.001	<b>.029</b>	<i>.012</i>	.001	<i>.018</i>
PROB				<b>.145</b>		
SEV				<b>.039</b>		
PC				<b>.151</b>		
RISK						<b>.035</b>
BENE						<b>.221</b>

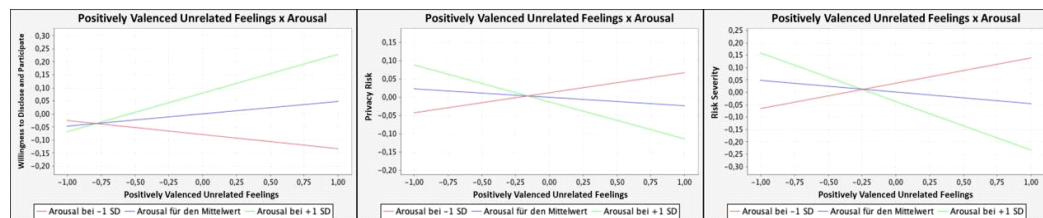


Figure 4. Slope analysis of interaction effects. Left: H1b; middle: H3b; right H5b.

More positively valenced unrelated feelings increase users' perceived benefit significantly ( $r = .232$ ,  $p < .001$ ,  $f^2 = .059$ ), thus we accept H2a. We find no significant interaction effect of positively valenced feelings and arousal ( $r = .027$ ,  $p = .575$ ,  $f^2 = .001$ ). Thus, we reject H2b. However, instead of an interaction effect of arousal, we observe a direct increasing effect of arousal on users' perceived benefits ( $r = .187$ ,  $p < .001$ ,  $f^2 = .037$ ).

We reject H3a as more positive feelings do not significantly decrease users' perceived privacy risk ( $r = -.023$ ,  $p = .619$ ,  $f^2 = .001$ ). Regarding H3b, we find a significant interaction effect of arousal and positive feelings, which leads to a reduced privacy risk perception under more positively valenced feelings and high arousal levels ( $r = -.078$ ,  $p = .045$ ,  $f^2 = .012$ ). Again, the interaction effect size is slightly below Cohens threshold of .02, but still higher than the average reported interaction effect sizes in social sciences (Cohen, 1988; Aguinis et al., 2005; Kenny, 2015). Therefore, we also accept H3b. Slope analysis (Figure 4, middle) shows that this is a crossover interaction effect (Loftus, 1978): more positively valenced feelings together with high arousal levels lead to a reduced privacy risk perception while under lower arousal levels this results in higher privacy risk perceptions. For less positively valenced feelings, the influence of arousal is inverted: under high arousal levels, users' privacy risk perception is increased while under low arousal levels, users perceive a decreased privacy risk.

We reject H4a as more positively valenced unrelated feelings do not decrease users' perceived risk probability ( $r = .014$ ,  $p = .809$ ,  $f^2 < .001$ ). In this regard, positive feelings and arousal have no significant interaction effect ( $r = -.026$ ,  $p = .677$ ,  $f^2 = .001$ ), thus we also reject H4b.

We also could not observe an effect of unrelated positive feelings on users' perceived risk severity ( $r = -.047$ ,  $p = .405$ ,  $f^2 = .002$ ). Therefore, we reject H5a. However, arousal and unrelated positive feelings have a significant interaction effect on perceived risk severity ( $r = -.150$ ,  $p = .004$ ,  $f^2 = .029$ ). When analyzing the slope (Figure 4, right), we observe again a crossover interaction effect (Loftus, 1978): more positively valenced feelings together with high arousal levels lead to a reduced risk severity perception while under low arousal levels this results in higher perceived risk severity. For

less positively valenced feelings the influence of arousal is inverted: under high arousal levels, an increase in perceived risk severity is observable while under low arousal levels, this results in a decreased risk severity perception.

## 5 Discussion

The results confirm our base model. We also verify that general privacy concerns do impact a specific disclosure decision only indirectly via perceived privacy risk. Regarding our main effect hypotheses, only the direct effect of positive feelings on perceived benefit (H2a) is significant. The direct effects of positive feelings on willingness to disclose and participate (H1a), on perceived privacy risk (H3a), on perceived privacy risk probability (H4a), and on perceived privacy risk severity (H5a) are not significant. However, the significant crossover interaction effects of positively valenced feelings and arousal (cf. Figure 4 and 5) on disclosure willingness (H1b), perceived privacy risk (H3b), and perceived risk severity (H5b) explain the non-significance of their respective direct effects (Loftus, 1978; Williams, 2015). These crossover interaction effects of positively valenced unrelated feelings and arousal are as follows: *under high arousal levels*, more positively valenced feelings lead to a decrease in users' perceived risk severity as well as perceived privacy risk, and to an increase in users' disclosure willingness. In contrast, *under low arousal levels*, more positively valenced feelings have the opposite effect, i.e., they lead to an increase in perceived risk severity and perceived privacy risk and lead to a decrease in disclosure willingness. However, for the observed crossover interaction effect on disclosure willingness, the increase in users' willingness to disclose under low arousal levels with less positively valenced feelings is weaker compared to the increase in users' willingness to disclose under high arousal levels with more positively valenced feelings.

The direct effects of arousal and positive feelings (H4a) as well as their interaction effect on perceived risk probability are not significant. Thus, perceived risk probability is the only tested construct on which unrelated positive feelings and arousal levels had no significant impact at all.

The remaining insignificant interaction effect is in H2b, which is the interaction effect on perceived benefit. The effects on perceived benefit are somehow exceptional, as the only significant direct effect of positively valenced feelings is on perceived benefit (H2a). Furthermore, in this case we observe the only significant direct effect of arousal, which increases perceived benefit. It seems that positive feelings and arousal are differently related to the benefit side of the privacy calculus compared to the privacy risk side. This could be related to the fact that when individuals apply simpler heuristics they generally tend to focus on the benefit side (Ditto et al., 2006). Also previous research has shown that higher arousal increases individuals' prize valuation respectively individuals bidding pricing in online auctions, which is explained with "auction fever" (cf. Adam et al., 2015). Taken together, these previous studies could help to explain why we find significant direct effects instead of an interaction effect in this regard. Nevertheless, to understand the reasons for the different impact of unrelated positive feelings and arousal on perceived benefits compared to the risk side of the privacy calculus, further research is necessary.

In sum, our results show that even unrelated positive feelings and the associated arousal levels can impact users' disclosure and participation willingness as well as its antecedents. Thus, it is indeed important to consider both constructs, positive feelings as well as arousal levels, and their interaction effects.

However, the most interesting observation in our study is that all significant interaction effects are crossover interactions (H1b, H3b, H5b), i.e., the arousal level serves as a "switch" for the effect: the effect sign is inverted when we compare the effect of unrelated positive feelings for users under high versus low arousal levels. A possible explanation for this observation could be that at different levels of arousal, different and sometimes contradictory theories fit best:



The highly aroused users behave as we expected: in line with the feelings-as-information theory (cf. Schwarz and Clore, 1983, 2003) positive feelings serve as informational input respectively as a basis for users' decision-making. As we assumed, users base their decision more strongly on these emotional information when highly aroused, which is in line with findings that higher arousal support simpler heuristics (Kim et al., 2020). In this case, individuals' positive feelings under high arousal increase more strongly their willingness to disclose and participate in the sweepstake (or reduce their risk perception more strongly) than when the individuals are not aroused. Equally, individuals with less positively valenced feelings under high arousal have a decreased willingness (higher risk perception) compared to individuals with low arousal levels.

However, this would only explain why the participation willingness is higher (or lower regarding risk perceptions) for users with high arousal levels. It does not explain why users' participation willingness (risk perception) increases (decreases) despite less positively valenced feelings under lower arousal levels.

This observation could be best explained by adopting an additional perspective: the *mood-maintenance theory* (Isen, 2000) assumes that positive feelings promote behavior that protects the current positive emotional state. The more developed *affect regulation theory* goes one step further and assumes that individuals in a positive affective state try to protect these positive feelings while individuals in a bad affective state take actions to improve their feelings (Andrade, 2005). Therefore, one explanation could be that unrelated positive feelings are seen under low arousal levels with less positively valenced feelings (more positively valenced feelings) as a good that could be won (lost) when disclosing personal data, e.g., in a sweepstake. For example, the latent possibility that personal data submitted during such a sweepstake participation could be misused could make users (under highly positively valenced feelings and low arousal levels) to anticipate that their positive feelings will vanish as this latent risk is in the back of their minds. In turn, this increases their risk perception and decreases their disclosure willingness. Vice versa, users with less positively valenced feelings under low arousal could expect that their feelings will become more positive when they get the benefit, i.e., win the prize of the sweepstake, and thus are rather willing to disclose. This perspective could also partially explain some previous observations that indicate that under low arousal states individuals ignore their positive feelings, or that these positive feelings do not lead to more optimistic assessments (Svenson and Maule, 1993; Ditto et al., 2006; Kim et al., 2020). It must be noted again, although this theory adequately explains and predicts users' disclosure behavior under low arousal levels, exactly the opposite disclosure behavior is observed for the high arousal level. For high arousal levels, only the feelings-as-information theory correctly explains and predicts users' disclosure behavior.

Therefore, it does seem as if users' arousal level serves as a switch that determines which of the theories explains and predicts users' disclosure behavior best:

i) *Low Arousal Level*. The affect regulation theory (Andrade, 2005) seems to fit best under low arousal levels as individuals with more positively valenced feelings want to keep their good "positive feelings" and have a lower motivation to engage in risky behavior. In contrast, users with currently less positively valenced feelings want to improve their feelings and thus are rather willing to disclose personal data respectively are more privacy risk prone. Thus, with this view we can explain that individuals with more positively valenced feelings under low arousal levels should assess the privacy risk as higher and they should be less willing to disclose their personal data compared to others and vice versa for users with less positively valenced feelings. This is exactly what we observed in our data for the interaction effect of more positively valenced unrelated feelings under low arousal levels for users' perceived privacy risk (H3b), perceived risk severity (H5b), and for their willingness to participate (H1b). However, for users under high arousal levels the affect regulation theory does not explain or predict users' disclosure behavior correctly.

ii) *High Arousal Level*. Whereas the feelings-as-information theory (Schwarz and Clore, 1983, 2003) fits best to explain and predict the disclosure behavior for highly aroused users. According to this

theory, users should perceive less privacy risk and be more willing to disclose their data with more positively valenced feelings since these are used as informational input that promotes optimistic assessments. This is exactly what we initially hypothesized and also observed for users under high arousal levels.

## **5.1 Limitations**

Our results have to be viewed in light of their limitations: in our survey, only individuals who had an Instagram account and were interested in soccer were allowed to participate in the survey. Thus, our sample may not reflect the population as these participants could have, for instance, a generally higher willingness to share their data. Another aforementioned aspect are the rather small effect sizes which are above or only slightly below the 0.02 threshold of Cohen (1988). This was expected due to the nature of interaction effects, for instance, the median of published interaction effect sizes in psychological journals is  $f^2 = .002$  ( $f^2_{\text{mean}} = .009$ ; Aguinis et al., 2005; Kenny, 2015). All our interaction effect sizes are above .009. Thus, our interaction effect sizes should be interpreted as medium to large effect sizes (Aguinis et al., 2005; Kenny, 2015).

We only measured users' willingness to participate and not real behavior, which is not always in accordance with their stated intentions (cf. Norberg, Horne and Horne, 2007). Manipulating and actually measuring feelings as well as arousal levels in a real-life social network sweepstake setting would be the best option regarding external validity. However, it is hard to evoke only specific feelings in a real world setting as there are many confounding influences. Moreover, the measurement in a real-life setting is difficult on its own, but especially in times of the Covid-19 pandemic. Therefore, to measure only intentions or willingness to disclose is common practice in the privacy field as these are important and valid predictors for actual behavior (cf. Ajzen and Fishbein, 1980; Smith et al., 2011; Kehr et al., 2015; Gerber, Gerber and Volkamer, 2018; Al-Natour, Cavusoglu, Benbasat and Aleem, 2020).

Also, we did not invoke different levels of arousal in the participants. Instead, we only measured the arousal levels, which are similar for both groups. We argue that the sole measurement is sufficient for our study as the participants in the control group clearly can have different arousal levels depending on the situation, or the time of the survey participation. For example, participants in the "happy" group can recall different events in their life. For example, the recalled positive experience could either be a thrilling bungee jump experience or a relaxing sauna visit. Both would lead to more positively valenced feelings but different arousal levels. Thus, we argue that our study design seems to be sufficient as a basis for more detailed research on this topic. Nevertheless, we suggest a targeted manipulation of arousal levels in future studies so that the arousal levels differ between groups. Such a study design could be helpful to examine the effects of arousal in more detail.

## **5.2 Implications and Future Research**

Our study offers several important contributions for theory:

Firstly, we contribute in a theoretical way to the scarce privacy literature that examines effects of unrelated feelings. We argue that unrelated feelings are especially important in the digital context, for example through unrelated stimuli in form of music, pictures, or social network posts and news that are just one click away to evoke certain feelings (Harlé and Sanfey, 2007; Hill, Rand, Nowak and Christakis, 2010; Thelwall, 2010; Kramer, Guillory and Hancock, 2014) and in turn impact personal data disclosure decision-making. This makes it essential to explore effects of unrelated feelings in more detail.

Therefore, this study helps to build a basic understanding of their effects. We showed that positively valenced unrelated feelings as well as arousal levels directly increase users' benefit perception without having a significant interaction effect. In contrast, we found that there is no direct effect of more

positively valenced feelings and arousal levels on perceived privacy risk, risk severity, risk probability, and on disclosure willingness. However, we showed that there are significant crossover interaction effects of positively valenced unrelated feelings and arousal levels on perceived risk severity and the total perceived risk and disclosure willingness but not the perceived risk probability. Future studies are necessary to understand in detail why and how arousal and positively valenced feelings affect benefit perception differently than risk perception.

Another contribution regarding the characteristics of the significant interaction effects is that they are crossover interaction effects. This means that more positively valenced feelings increase disclosure willingness and decrease privacy risk perception only in combination with high arousal levels, while under low arousal levels this results in the opposite effect. With this, it seems we discovered a new phenomenon in privacy decision-making, that is eventually only true for positive feelings evoked by decision unrelated stimuli but not for feelings that are evoked by decision related stimuli: to the best of our knowledge, all studies find clear evidence that decision related positive emotions only increase disclosure willingness and decrease perceived privacy risk (Anderson and Agarwal, 2011; H. Li et al., 2011; Wakefield, 2013). However, it is still possible that in these studies most participants were highly aroused, leading to a disclosure willingness increasing instead of decreasing effect for more positively valenced feelings. This would be in perfect accordance with our results, but we assume that not all participants were highly aroused in these studies. Instead, we could imagine that the inversion of the effect for positively valenced feelings under low arousal compared to high arousal levels will only happen for positive feelings that are evoked by decision unrelated stimuli. To address this issue, future studies should consider users' arousal levels in their studies to verify under which circumstances these crossover interaction effects happen. Additionally, privacy studies should also distinguish between feelings that are evoked by stimuli related and unrelated to disclosure decisions.

We also provide a first explanation for the observed crossover interaction effects. To do so, we combine perspectives of the feelings-as-information theory (Schwarz and Clore, 2003, 2003) with perspectives of the affect regulation theory (Andrade, 2005) by using users' arousal levels as a switch to decide which theory explains and predicts users' decision-making best. However, future studies should verify if our assumed explanation for the effect inversion can be used for prediction, i.e., that the affect regulation theory (Andrade, 2005) is appropriate for low arousal conditions while the feelings-as-information theory (Schwarz and Clore, 2003, 2003) is appropriate for high arousal conditions.

This study bears two important contributions for practice as well:

*First*, organizations that rely on personal data can increase potential users' data disclosure willingness when the organizations evoke positive feelings and high arousal levels right before the disclosure decision, even if the stimulus is unrelated to the disclosure decision. For example, this could be achieved by playing positive and arousing music, displaying a certain positive and arousing picture or simply by providing an exciting positive story (Westermann et al., 1996; Jallais and Gilet, 2010; Kramer et al., 2014; Kim et al., 2020). Similarly, it also could help to choose the right disclosure ad position and the right timing. Especially new in our study compared to previous research is, that we show that it is not necessarily sufficient to increase users' disclosure willingness by only evoking positive feelings. To evoke more positively valenced feelings and high levels of arousal at the same time seems to be the most effective way to increase users' disclosure and participation willingness. Under low arousal levels at worst more positively valenced feelings could lead to a decreased disclosure willingness.

This knowledge could be misused by organizations as users may make unwanted decisions when they are confronted with extremely feelings evoking stimuli. Therefore, we want to point out that there is a potential countermeasure for users to protect themselves from such distorted decision-making: individuals should think about their own feelings and find out the reason respectively the stimulus which evoked those feelings and realize that this stimulus is not associated with the decision. Studies in different contexts showed that this helped individuals who were confronted with positive feelings

inducing stimuli, to make decisions that resembles decision-making of individuals in the control group (cf. Schwarz and Clore, 1983; Ciarrochi, Caputi and Mayer, 2003). Furthermore, based on our results, individuals with very positively valenced feelings should try to calm down when they are very excited before making disclosure decisions in order to prevent overdisclosure of personal data. Nevertheless, future studies should examine how effective these countermeasures are in the online privacy context.

*Second*, this study could help policymakers as well. The meaningful interactions of positively valenced unrelated feelings and arousal levels in data disclosure decisions indicate that it is maybe not sufficient to protect internet users by only regulating the content and transparency, for example regarding organizations’ data consent forms. It is known that it could be effective for users’ protection to regulate the graphical representation, i.e., its visibility, of such a form, too (cf. Hendrickx et al., 1989; Tsai, Egelman, Cranor and Acquisti, 2011; Bornschein, Schmidt and Maier, 2020). Our results indicate that it could be beneficial to adapt regulations for the graphical representation of data consent forms by considering the feelings and arousal levels evoked (cf. Schaub, Balebako, Durity and Cranor, 2015; Kim et al., 2020). To prevent users from overdisclosure there could be distinct representations of a data consent based on users self-decided “feeling state”: for instance, users with very positively valenced feelings could get displayed a certain form with especially calming colours. However, for legislators our study does not provide specific overdisclosure countermeasures. In this regard, our work rather serves as a thought-provoking impulse for lawmakers, in which way users could be protected from overdisclosure of personal data by displaying that also non-cognitive factors, such as unrelated feelings and arousal levels, impact users’ disclosure willingness.

## 6 Appendix

Table 2. Measurement items, Cronbach’s  $\alpha$  and Composite-Reliability for all constructs. Loadings of items are in brackets.

<b>Positively Valenced Unrelated Feelings (PVUF)</b>	
Shortened from Klapwijk and Van Lange (2009); Cronbach’s $\alpha$ : .81; Composite-Reliability: .86; 7-Point Likert scale with anchors 1 = “strongly disagree” and 7 = “strongly agree”.	
<i>I feel right now:</i>	
PVUF1 (.8)	Happy
PVUF2 (.85)	Proud
PVUF3 (.9)	Enthusiastic
<b>Arousal (AR)</b>	
Shortened from Deng and Poole (2010); Cronbach’s $\alpha$ : .84; Composite-Reliability: .9; 7-Point semantic differential with the following endpoints:	
<i>I am currently:</i>	
AR1 (.87)	unaroused - aroused
AR2 (.92)	calm - excited
AR3 (.82)	relaxed - stimulated
<b>Willingness to Disclose and Participate in the Sweepstake (WDP)</b>	
Adapted from Anderson and Agarwal (2011); Cronbach’s $\alpha$ : .96; Composite-Reliability: .98; 7-Point semantic differential with the following endpoints:	
<i>To what extent would you be willing to participate in the raffle?</i>	
WDP1 (.97)	unlikely - likely
WDP2 (.98)	not probable - probably
WDP3 (.94)	unwilling - willing

<b>Privacy Concerns (PC)</b>	
Shortened from Hong and Thong (2013); Cronbach's $\alpha$ : .85; Composite-Reliability: .89; 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree".	
PC1 (.66)	It usually bothers me when companies/organizations ask me for personal information.
PC2 (.85)	I am concerned that companies/organizations would share my personal information with other companies/organizations without my authorization.
PC3 (.61)	I am concerned that companies/organizations do not devote enough time and effort to verify the accuracy of my personal information in their databases.
PC4 (.84)	I am concerned that companies/organizations do not devote enough time and effort to prevent unauthorized access to my personal information.
PC5 (.79)	It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by companies/organizations.
PC6 (.76)	It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by companies/organizations.
<b>Perceived Benefit (BENE)</b>	
Adapted from Voss, Spangenberg, & Grohmann (2003), Cronbach's $\alpha$ : .83; Composite-Reliability: .89; 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree"	
<i>The Bundesliga jerseys as prizes in the raffle I perceive as:</i>	
BENE1 (.82)	Functional
BENE2 (.84)	Practical
BENE3 (.74)	Necessary
BENE4 (.87)	Helpful
<b>Perceived Privacy Risk (RISK)</b>	
Adapted from Dinev, Xu, Smith, & Hart (2013), Dinev & Hart (2006), Featherman & Pavlou (2003); Cronbach's $\alpha$ : .94; Composite-Reliability: .95; 7-Point Likert scale with anchors 1 = "strongly disagree" and 7 = "strongly agree".	
<i>The Bundesliga jerseys as prizes in the raffle I perceive as:</i>	
RISK1 (.92)	It is very risky in this data collection to reveal personal information.
RISK2 (.93)	The disclosure of personal information in this data collection is associated with a high potential risk of losing privacy.
RISK3 (.9)	My disclosed personal information may be used improperly in this data collection.
RISK4 (.91)	The disclosure of personal information in this data collection could cause many unexpected problems.
<b>Risk Probability (PROB)</b>	
Adapted from Bolton, Cohen and Bloom (2006); Percentual slider scale from 0% - 100%	
<i>Please rate how likely you think it is that the information you disclosed in this sweepstake will be published on someone else's website, accessible to everyone?</i>	
<b>Risk Severity (SEV)</b>	
Adapted from Bolton et al. (2006); 7-Point semantic differential with 1 = "not at all serious" and 7 = "very serious".	
<i>Please rate how bad it would be for you if the data you disclosed in this sweepstakes were published on someone else's website, accessible to everyone?</i>	
SEV	unwilling - willing

Table 3. Age, sex, and group distribution in the sample.

	18-29		30-39		40-49		50-59		60+		Sum
	M	F	M	F	M	F	M	F	M	F	
<b>"Happy" group</b>	28	28	24	19	15	20	14	12	9	8	177
<b>Control group</b>	23	27	25	26	11	22	19	16	17	5	191
<b>Sum</b>	51	55	49	45	26	42	33	28	26	13	368

Table 4. Path Coefficient results.

Effect	Path Coefficient (Standard Deviation)	p-Value
AR -> BENE	.187 (.051)	.000
AR -> WDP	.08 (.044)	.07
AR -> PROB	-.014 (.06)	.815
AR -> RISK	-.012 (.041)	.766
AR -> SEV	-.037 (.053)	.48
BENE -> WDP	.416 (.047)	.000
PVUFxAR -> PROB	-.026 (.063)	.677
PVUFxAR -> BENE	.027 (.048)	.575
PVUF -> BENE	.232 (.049)	.000
PVUF -> WDP	.047 (.05)	.344
PVUF -> PROB	.014 (.056)	.809
PVUF -> RISK	-.023 (.046)	.619
PVUF -> SEV	-.047 (.056)	.405
PVUFxAR -> SEV	-.15 (.052)	.004
PVUFxAR -> RISK	-.078 (.039)	.045
PVUFxAR -> WDP	.102 (.038)	.007
PC -> WDP	-.017 (.056)	.755
PC -> RISK	.348 (.049)	.000
PROB -> RISK	.305 (.045)	.000
RISK -> WDP	-.184 (.056)	.001
SEV -> RISK	.178 (.048)	.000

Table 5. Loadings and cross loadings of the items.

Items	Constructs								
	PVUF	AR	PVUFxAR	PROB	SEV	PC	RISK	BENE	WDP
AR1	.052	.865	.133	.016	-.051	-.158	-.092	.181	.173
AR2	.030	.917	.185	-.056	-.077	-.121	-.101	.189	.202
AR3	-.135	.818	.130	.000	-.039	-.082	-.040	.113	.131
PVUF1	.796	-.181	.096	.009	-.056	-.073	-.051	.112	.070
PVUF2	.847	-.031	.002	.043	-.054	-.006	-.071	.185	.125
PVUF3	.899	.105	.112	-.016	-.049	-.062	-.030	.254	.189
WDP1	.169	.187	.196	-.142	-.083	-.177	-.292	.470	.972
WDP2	.165	.192	.198	-.145	-.091	-.185	-.275	.478	.978
WDP3	.145	.198	.193	-.176	-.106	-.228	-.322	.473	.944
BENE1	.185	.131	.085	-.101	-.051	-.093	-.187	.819	.366
BENE2	.221	.136	.049	-.068	-.107	-.141	-.216	.843	.414
BENE3	.151	.164	.040	.029	-.007	-.109	-.064	.737	.378
BENE4	.204	.193	.095	-.052	-.052	-.141	-.180	.869	.444
PVUFxAR	.083	.175	1.000	-.031	-.180	-.132	-.180	.083	.203
PC1	-.099	-.112	-.089	.160	.239	.656	.352	-.125	-.202
PC2	-.064	-.188	-.160	.213	.452	.847	.437	-.124	-.189
PC3	.022	-.015	-.034	.191	.289	.611	.363	-.066	.016
PC4	-.049	-.044	-.162	.213	.428	.836	.442	-.149	-.250
PC5	.004	-.157	-.045	.112	.405	.793	.379	-.076	-.082
PC6	-.036	-.122	-.070	.146	.357	.760	.370	-.120	-.162
RISK1	-.021	-.091	-.141	.395	.423	.464	.919	-.179	-.272
RISK2	-.014	-.107	-.156	.380	.411	.505	.931	-.151	-.283
RISK3	-.077	-.077	-.193	.397	.403	.461	.898	-.200	-.292
RISK4	-.094	-.073	-.168	.414	.383	.467	.910	-.202	-.277
SEV	-.061	-.067	-.180	.256	1.000	.485	.443	-.068	-.097
PROB	.011	-.019	-.031	1.000	.256	.231	.433	-.059	-.160

Table 6. Inner VIF values of the constructs.

Independent Variables	Dependent Variables				
	PROB	SEV	RISK	BENE	WDP
PVUF	1.007	1.007	1.011	1.007	1.067
AR	1.032	1.032	1.049	1.032	1.082
PVUFxAR	1.039	1.039	1.070	1.039	1.068
PROB			1.089		
SEV			1.374		
PC			1.353		1.389
RISK					1.420
BENE					1.138

Table 7. Heterotrait-Monotrait Ratio (HTMT) of the constructs.

	PVUF	AR	PVUFx AR	PROB	SEV	PC	RISK	BENE
AR	.175							
PVUFxAR	.091	.188						
PROB	.030	.030	.031					
SEV	.069	.070	.180	.256				
PC	.095	.167	.135	.250	.523			
RISK	.071	.101	.186	.449	.458	.584		
BENE	.260	.220	.090	.084	.073	.176	.224	
WDP	.169	.216	.207	.163	.098	.221	.324	.547

Table 8. Correlations between constructs and square root of the AVEs on the diagonal.

	PVUF	AR	PVUFx AR	PROB	SEV	PC	RISK	BENE	WDP
PVUF	.848								
AR	-.002	.868							
PVUFxAR	.083	.175	1						
PROB	.011	-.019	-.031	1					
SEV	-.061	-.067	-.18	.256	1				
PC	-.053	-.143	-.132	.231	.485	.756			
RISK	-.056	-.095	-.18	.433	.443	.519	.914		
BENE	.234	.192	.083	-.059	-.068	-.149	-.2	.818	
WDP	.165	.2	.203	-.16	-.097	-.204	-.307	.491	.964

Für unsere Forschung ist es wichtig, dass Sie sich in die folgende Situation hineinversetzen.

Bitte lesen Sie sich die folgenden Informationen und die dargestellte Situation genau durch, da Sie im Folgenden Fragen hierzu beantworten müssen.

Sie befinden sich in folgender hypothetischer Situation:

mingle weist Sie mittels der folgenden Nachricht auf ein Gewinnspiel hin:

Sie können an einem Gewinnspiel teilnehmen, bei dem Sie ein Fußballtrikot der 1. oder 2. Bundesliga Ihres Lieblingsvereins mit dem Flock Ihres Liebesspielers gewinnen können. Mehr Informationen finden Sie in dem hier verlinkten Instagram-Beitrag:

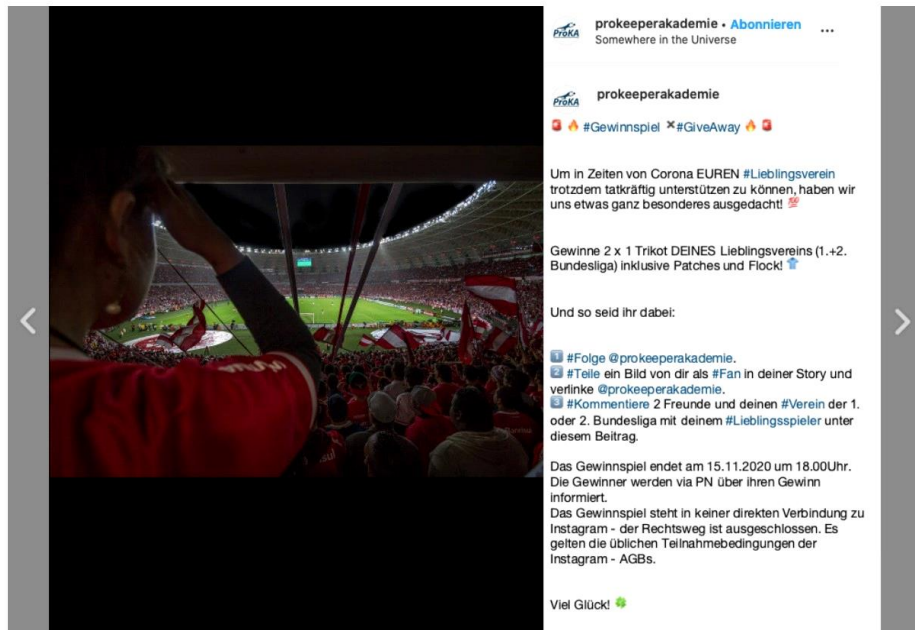


Figure 5. Scenario - Instagram sweepstake post.

Translation of the hypothetical situation:

“mingle informs you about a lottery by means of the following message:

You can participate in a sweepstake where you can win a 1st or 2nd Bundesliga soccer jersey of your favorite club with the flock of your favorite player.“

Translation of the displayed Instagram post:

“In order to be able to support YOUR favorite club in times of Corona, we have come up with something very special!

Win 2 x 1 jersey of YOUR favorite club (1.+2. Bundesliga) including patch and flock!

And this is how you are in:

1. #follow @prokeeperakademie.
2. share a picture of you as a #fan in your story and link @prokeeperakademie.
3. #comment 2 friends and your #club of the 1st or 2nd Bundesliga with your #favorite player under this post.

The sweepstake ends on 15.11.2020 at 6pm. The winners will be informed via PN about their prize.

The sweepstakes is in no direct connection with Instagram - the legal process is excluded. The usual conditions of Instagram - T&Cs apply.

Good luck!”



Der Beitrag gehört zur folgenden Instagram-Seite, auf diese werden Sie nach einem Klick auf das Bild in der Nachricht weitergeleitet:

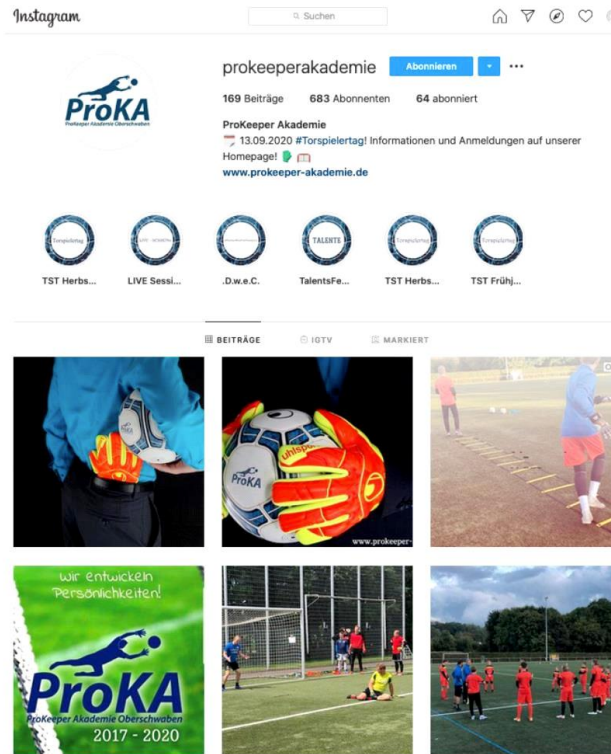


Figure 6. Scenario - Instagram account of the sweepstake organizer.

## References

- Adam, M. T. P., J. Krämer and M. B. Müller. (2015). 'Auction Fever! How Time Pressure and Social Competition Affect Bidders' Arousal and Bids in Retail Auctions'. *Journal of Retailing*, 91(3), 468–485.
- Aguinis, H., J. C. Beaty, R. J. Boik and C. A. Pierce. (2005). 'Effect Size and Power in Assessing Moderating Effects of Categorical Variables Using Multiple Regression: A 30-Year Review.' *Journal of Applied Psychology*, 90(1), 94–107.
- Ajzen, I. and M. Fishbein. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, New Jersey: Pearson.
- Al-Natour, S., H. Cavusoglu, I. Benbasat and U. Aleem. (2020). 'An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps'. *Information Systems Research*, 31(4), 1037–1063.
- Anderson, C. L. and R. Agarwal. (2011). 'The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information'. *Information Systems Research*, 22(3), 469–490.
- Andrade, E. B. (2005). 'Behavioral Consequences of Affect: Combining Evaluative and Regulatory Mechanisms'. *Journal of Consumer Research*, 32(3), 355–362.
- Antonetti, P. and C. Valor. (2020). 'A theorisation of discrete emotion spillovers: an empirical test for anger'. *Journal of Marketing Management*, 1–27.
- Ariely, D. and G. Loewenstein. (2006). 'The heat of the moment: the effect of sexual arousal on sexual decision making'. *Journal of Behavioral Decision Making*, 19(2), 87–98.

- Awad, N. F. and M. S. Krishnan. (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.
- Bagozzi, R. P. and Y. Yi. (1989). 'On the Use of Structural Equation Models in Experimental Designs'. *Journal of Marketing Research*, 26(3), 273–284.
- Bagozzi, Richard P. and Y. Yi. (2012). 'Specification, evaluation, and interpretation of structural equation models'. *Journal of the Academy of Marketing Science*, 40(1), 8–34.
- Bagozzi, Richard P., Y. Yi and L. W. Phillips. (1991). 'Assessing Construct Validity in Organizational Research'. *Administrative Science Quarterly*, 36(3), 421–458.
- Bansal, G., F. "Mariam" Zahedi and D. Gefen. (2010). 'The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online'. *Decision Support Systems*, 49(2), 138–150.
- Bidler, M. (2020). *Consumers' Privacy-related Decision Making in the Digital Landscape*. University of Passau.
- Bolton, L. E., J. B. Cohen and P. N. Bloom. (2006). 'Does Marketing Products as Remedies Create 'Get Out of Jail Free Cards'?'. *Journal of Consumer Research*, 33(1), 71–81.
- Bornschein, R., L. Schmidt and E. Maier. (2020). 'The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices'. *Journal of Public Policy & Marketing*, 39(2), 135–154.
- Chaudhuri, A. (2002). 'A study of emotion and reason in products and services'. *Journal of Consumer Behaviour*, 1(3), 267–279.
- Ciarrochi, J., P. Caputi and J. D. Mayer. (2003). 'The distinctiveness and utility of a measure of trait emotional awareness'. *Personality and Individual Differences*, 34(8), 1477–1490.
- Clore, G. L. and S. Schnall. (2005). 'The Influence of Affect on Attitude'. In: *Handbook of Attitudes and Attitude Change* (pp. 437–480).
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, N.J: L. Erlbaum Associates.
- Coker, B. and A. L. McGill. (2020). 'Arousal increases self-disclosure'. *Journal of Experimental Social Psychology*, 87.
- Cunningham, S. (1967). 'The Major Dimensions of Perceived Risk'. In: *Risk Taking and Information Handling in Consumer Behavior* (pp. 82–108). Boston: Harvard University.
- Denes-Raj, V. and S. Epstein. (1994). 'Conflict Between Intuitive and Rational Processing: When People Behave Against Their Better Judgment'. *Journal of Personality and Social Psychology*, 66(5), 819–829.
- Deng and Poole. (2010). 'Affect in Web Interfaces: A Study of the Impacts of Web Page Visual Complexity and Order'. *MIS Quarterly*, 34(4), 711–730.
- Dinev, T. and P. Hart. (2006). 'An Extended Privacy Calculus Model for E-Commerce Transactions'. *Information Systems Research*, 17(1), 61–80.
- Dinev, T., A. R. McConnell and H. J. Smith. (2015). 'Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box'. *Information Systems Research*, 26(4), 639–655.
- Dinev, T., H. Xu, J. H. Smith and P. Hart. (2013). 'Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts'. *European Journal of Information Systems*, 22(3), 295–316.
- Ditto, P. H., D. A. Pizarro, E. B. Epstein, J. A. Jacobson and T. K. MacDonald. (2006). 'Visceral influences on risk-taking behavior'. *Journal of Behavioral Decision Making*, 19(2), 99–113.
- Dunn, J. R. and M. E. Schweitzer. (2005). 'Feeling and Believing: The Influence of Emotion on Trust.' *Journal of Personality and Social Psychology*, 88(5), 736–748.
- Epstein, S. (1994). 'Integration of the Cognitive and the Psychodynamic Unconscious'. *American Psychologist*, 49(8), 709–724.
- Evans, J. S. B. and K. E. Stanovich. (2013). 'Dual-Process Theories of Higher Cognition: Advancing the Debate'. *Perspectives on Psychological Science*, 8(3), 223–241.
- Featherman, M. S. and P. A. Pavlou. (2003). 'Predicting e-services adoption: a perceived risk facets perspective'. *International Journal of Human-Computer Studies*, 59(4), 451–474.
- Finucane, M. L., A. Alhakami, P. Slovic and S. M. Johnson. (2000). 'The Affect Heuristic in Judgments of Risks and Benefits'. *Journal of Behavioral Decision Making*, 13(1), 1–17.
- Fornell, C. and D. F. Larcker. (1981). 'Evaluating Structural Equation Models with Unobservable Variables and Measurement Error'. *Journal of Marketing Research*, 18(1), 39–50.
- Gartner. (2019). 'How to Balance Personalization With Data Privacy'. URL: [www.gartner.com/smarterwithgartner/how-to-balance-personalization-with-data-privacy/](http://www.gartner.com/smarterwithgartner/how-to-balance-personalization-with-data-privacy/) (accessed: 05.11.2020)

- Gefen, D., D. Straub and M.-C. Boudreau. (2000). 'Structural Equation Modeling and Regression: Guidelines for Research Practice'. *Communications of the Association for Information Systems*, 4, Article 7.
- Gerber, N., P. Gerber and M. Volkamer. (2018). 'Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior'. *Computers & Security*, 77, 226–261.
- Hair, J. F., G. T. M. Hult, C. Ringle and M. Sarstedt. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications.
- Hair, J. F., M. Sarstedt, C. M. Ringle and S. P. Gudergan. (2017). *Advanced Issues in Partial Least Squares Structural Equation Modeling*. SAGE Publications.
- Hair, Joe F., C. M. Ringle and M. Sarstedt. (2011). 'PLS-SEM: Indeed a Silver Bullet'. *Journal of Marketing Theory and Practice*, 19(2), 139–152.
- Harlé, K. M. and A. G. Sanfey. (2007). 'Incidental sadness biases social economic decisions in the Ultimatum Game.' *Emotion*, 7(4), 876–881.
- Hendrickx, L., C. Vlek and H. Oppewal. (1989). 'Relative importance of scenario information and frequency information in the judgment of risk'. *Acta Psychologica*, 72(1), 41–63.
- Henseler, J., C. M. Ringle and M. Sarstedt. (2015). 'A new criterion for assessing discriminant validity in variance-based structural equation modeling'. *Journal of the Academy of Marketing Science*, 43(1), 115–135.
- Higgins, E. T. (1998). 'The Aboutness Principle: A Pervasive Influence on Human Inference'. *Social Cognition*, 16(1), 173–198.
- Hill, A. L., D. G. Rand, M. A. Nowak and N. A. Christakis. (2010). 'Emotions as infectious diseases in a large social network: the SISa model'. *Proceedings of the Royal Society B: Biological Sciences*, 277(1701), 3827–3835.
- Hogarth, R. M., M. Portell and A. Cuxart. (2007). 'What Risks Do People Perceive in Everyday Life? A Perspective Gained from the Experience Sampling Method (ESM)'. *Risk Analysis*, 27(6), 1427–1439.
- Hogarth, R. M., M. Portell, A. Cuxart and G. I. Kolev. (2011). 'Emotion and reason in everyday risk perception'. *Journal of Behavioral Decision Making*, 24(2), 202–222.
- Hong, W. and J. Y. L. Thong. (2013). 'Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies'. *MIS Quarterly*, 37(1), 275–298.
- Howard, D. J. and C. Gengler. (2001). 'Emotional Contagion Effects on Product Attitudes'. *Journal of Consumer Research*, 28, 189–201.
- Isen, A. M. (2000). 'Some Perspectives on Positive Affect and Self-Regulation'. *Psychological Inquiry*, 11(3), 184–187.
- Jallais, C. and A.-L. Gilet. (2010). 'Inducing changes in arousal and valence: Comparison of two mood induction procedures'. *Behavior Research Methods*, 42(1), 318–325.
- Kahneman, D. (2012). *Thinking, fast and slow*. London: Penguin Books.
- Kehr, F., T. Kowatsch, D. Wentzel and E. Fleisch. (2015). 'Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus'. *Information Systems Journal*, 25(6), 607–635.
- Keith, Thompson and Greer. (2012). 'Examining the Rationality of Information Disclosure through Mobile Devices'. Presented at the Thirty Third International Conference on Information Systems, Orlando, Florida.
- Kenny, D. A. (2015). 'Moderator Variables'. URL: <http://davidakenny.net/cm/moderation.htm> (accessed: 10.11.2020)
- Kim, Y., K. Park, Y. Kim, W. Yang, D. Han and W.-S. Kim. (2020). 'The Impact of Visual Art and High Affective Arousal on Heuristic Decision-Making in Consumers'. *Frontiers in Psychology*, 11, Article 565829.
- Klapwijk, A. and P. A. M. Van Lange. (2009). 'Promoting cooperation and trust in 'noisy' situations: The power of generosity.' *Journal of Personality and Social Psychology*, 96(1), 83–103.
- Kramer, A. D. I., J. E. Guillory and J. T. Hancock. (2014). 'Experimental evidence of massive-scale emotional contagion through social networks'. *Proceedings of the National Academy of Sciences*, 111(24), 8788–8790.
- Lambert, A. J., B. K. Payne, L. L. Jacoby, L. M. Shaffer, A. L. Chasteen and S. R. Khan. (2003). 'Stereotypes as dominant responses: On the 'social facilitation' of prejudice in anticipated public contexts.' *Journal of Personality and Social Psychology*, 84(2), 277–295.
- Li, H., X. (Robert) Luo, J. Zhang and H. Xu. (2017). 'Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors'. *Information & Management*, 54(8), 1012–1022.
- Li, H., R. Sarathy and H. Xu. (2011). 'The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors'. *Decision Support Systems*, 51(3), 434–445.
- Li, Y. (2012). 'Theories in online information privacy research: A critical review and an integrated framework'. *Decision Support Systems*, 54(1), 471–481.

- Loewenstein, G. F., E. U. Weber, C. K. Hsee and N. Welch. (2001). 'Risk as feelings.' *Psychological Bulletin*, 127(2), 267–286.
- Loftus, G. R. (1978). 'On interpretation of interactions'. *Memory & Cognition*, 6(3), 312–319.
- Martin, M. (1990). 'On the induction of mood'. *Clinical Psychology Review*, 10(6), 669–697.
- Norberg, P. A., D. R. Horne and D. A. Horne. (2007). 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors'. *Journal of Consumer Affairs*, 41(1), 100–126.
- Petty, R. E. and J. T. Cacioppo. (1986). 'The Elaboration Likelihood Model of Persuasion'. *Advances in Experimental Social Psychology*, 19, 113–205.
- Rosenberg, E. L. (1998). 'Levels of Analysis and the Organization of Affect'. *Review of General Psychology*, 2(3), 247–270.
- Russell, J. A. (2003). 'Core affect and the psychological construction of emotion.' *Psychological Review*, 110(1), 145–172.
- Sanfey, A. and R. Hastie. (1998). 'Does Evidence Presentation Format Affect Judgment? An Experimental Evaluation of Displays of Data for Judgments'. *Psychological Science*, 9(2), 99–103.
- Schaub, F., R. Balebako, A. L. Durity and L. F. Cranor. (2015). 'A Design Space for Effective Privacy Notices\*'. In: E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (1st ed., pp. 365–393). Cambridge University Press.
- Scherer, K. R. (2005). 'What are emotions? And how can they be measured?' *Social Science Information*, 44(4), 695–729.
- Schwarz, N. and G. L. Clore. (1983). 'Mood, misattribution, and judgments of well-being: Informative and directive functions of affective states.' *Journal of Personality and Social Psychology*, 45(3), 513–523.
- Schwarz, N. and G. L. Clore. (2003). 'Mood as Information: 20 Years Later'. *Psychological Inquiry*, 14(3–4), 296–303.
- Sendinblue. (2019). 'How to Run Giveaways Post-GDPR'. URL: <https://www.sendinblue.com/blog/how-to-run-giveaways-post-gdpr/> (accessed: 10.11.2020)
- Sieber, J. E. and J. T. Lanzetta. (1964). 'Conflict and conceptual structure as determinants of decision-making behavior'. *Journal of Personality*, 32(4), 622–641.
- Slovic, P., M. L. Finucane, E. Peters and D. G. MacGregor. (2004). 'Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality'. *Risk Analysis*, 24(2), 311–322.
- Slovic, P., J. Monahan and D. G. MacGregor. (2000). 'Violence risk assessment and risk communication: The effects of using actual cases, providing instruction, and employing probability versus frequency formats.' *Law and Human Behavior*, 24(3), 271–296.
- Smith, H. J., T. Dinev and H. Xu. (2011). 'Information privacy research: an interdisciplinary review'. *MIS Quarterly*, 35(4), 989–1016.
- Svenson, O. and A. J. Maule. (1993). *Time Pressure and Stress in Human Judgment and Decision Making*. Springer Science & Business Media.
- Thatcher, J. B. and P. L. Perrewe. (2002). 'An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy'. *MIS Quarterly*, 26(4), 381–396.
- Thelwall, M. (2010). 'Emotion homophily in social network site messages'. *First Monday*, 15(4).
- Tsai, J. Y., S. Egelman, L. Cranor and A. Acquisti. (2011). 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study'. *Information Systems Research*, 22(2), 254–268.
- Voss, K. E., E. R. Spangenberg and B. Grohmann. (2003). 'Measuring the Hedonic and Utilitarian Dimensions of Consumer Attitude'. *Journal of Marketing Research*, 40(3), 310–320.
- Wakefield, R. (2013). 'The influence of user affect in online information disclosure'. *The Journal of Strategic Information Systems*, 22(2), 157–174.
- Weise, K. (2019). 'Amazon Knows What You Buy. And It's Building a Big Ad Business From It.' URL: <https://www.nytimes.com/2019/01/20/technology/amazon-ads-advertising.html> (accessed: 10.11.2020)
- Westermann, R., K. Spies, G. Stahl and F. W. Hesse. (1996). 'Relative effectiveness and validity of mood induction procedures: a meta-analysis'. *European Journal of Social Psychology*, 26(4), 557–580.
- Williams, R. (2015). 'Interpreting Interaction Effects; Interaction Effects and Centering'.
- Wold, H. (1966). 'Estimation of principal components and related models by iterative least squares'. *Multivariate Analysis*, 391–420.
- Yamagishi, K. (1997). 'When a 12.86% mortality is more dangerous than 24.14%: implications for risk communication'. *Applied Cognitive Psychology*, 11(6), 495–506.
- Zhang, P. (2013). 'The Affective Response Model: A Theoretical Framework of Affective Concepts and Their Relationships in the ICT Context'. *MIS Quarterly*, 37(1), 247–274.

## Appendix

In cooperation with Prof. Dr. Jan H. Schumann, Prof. Dr. Thomas Widjaja, Dr. Margarita Bidler and Tobias Steudner a structured literature review was conducted and used as basis to write a research proposal approved by the Deutsche Forschungsgemeinschaft (DFG) as well as to write a published book contribution (cf. Specht-Riemenschneider et al., 2019). The following description of the procedure for the structured literature review as well as a brief overview of the results are taken directly from the DFG research proposal:

*We conducted a structured literature review (in accordance with Tranfield, Denyer, & Smart, 2003 and Webster & Watson, 2002) and we searched for studies on data disclosure within marketing and information systems journals ranked A+, A, and B in the VHB JOURQUAL ranking.<sup>9</sup> We conducted structured keyword searches for “data,” “information,” and “priva\*,” combined with terms that represent data handling (e.g., concern\*, disclos\*, shar\*, use, trust\*, protect\*, calcul\*, deci\*, control\*, reveal\*, trad\*, expos\*, provi\*, collect\*, inva\*, gather\*) in the title and keywords. Starting with a data set of 1,607 papers, we screened the title, abstract, and keywords to select all papers that actually focus on data disclosure. In a second phase, we analyzed the remaining papers in detail and excluded publications that use the term “privacy” without deeper explanation of the underlying decision-making process. As a result, we obtained and analyzed a sample of 90 publications published between 1991 and early 2017, as listed in the following table.*

---

<sup>9</sup> For more information see <http://vhbonline.org/vhb4you/jourqual/vhb-jourqual-3/gesamtliste/>

Table 1. Structured literature review for a DFG research proposal as well as for a book contribution

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Angst, C.M., and Agarwal, R. (2009)/ MIS Quarterly/A+	Argument Frame Issue Involvement Privacy Concern Ability Pre-Attitude	<u>Mediator:</u> Post-attitude <u>Moderators:</u> Privacy Concern Issue Involvement	Opt-In Intention	Elaboration Likelihood Model Concernsfor Information Privacy (CFIP)	Conference participants (N=67, N/A) Online survey (N=299, N/A)/Q/SEM
Al-Natour, S., Benbasat, I., and Centefelli, R. (2009)/ International Conference on Information Systems/A	Perceived Responsiveness	<u>Mediators:</u> Perceived Performance Expectancy Perceived Information Misuse Risk	Intention to Disclose sensitive / non-sensitive Information	Social exchange Theory Social penetration Theory	E-commerce shoppers (N=47, N/A)/Q/PLS
Bansal, G., Zahedi, F., and Gefen, D. (2015)/ Decision Support Systems/ B	Sensitivity of Information Type of Information	<u>Mediator:</u> Trust <u>Moderators:</u> Previous Online Privacy Invasion Risk Beliefs	Willingness to Disclose Reaction to Privacy Threats	Utility Theory Prospect Theory	Students (N=367)/ Q/ EFA
Bansal, G., Zahedi, F., and Gefen, D. (2008)/ International Conference on Information Systems/A	Understandability Adequacy Website Information Quality Third Party Assurance Availability of Company Information Website Design Quality Website Reputation Experience with the Website	<u>Mediator:</u> Trust in the Website <u>Moderator:</u> Privacy Concerns	Intention to Disclose	Elaboration Likelihood Model	Students (N=674, USA)/Q/SEM
Bansal, G., Zahedi, F., and Gefen, D. (2010)/ Decision Support Systems/B	Poor Health Status Previous Online Privacy Invasion Prior Positive Experience with the Website <u>Personality:</u> Extroversion Agreeableness Emotional Instability Conscientiousness Intellect	<u>Mediators:</u> Perceived Health Information Sensitivity Health Information Privacy Concerns Risk Beliefs (Health Info Trust in the Health Website	Intention to Disclose	Utility Theory Trust Theory	Students (N=367, USA)/Q/CFA and SEM

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Bansal, G., Zahedi, F., and Gefen, D. (2015)/ European Journal of Information Systems/A	Adequacy (Collection, Errors, Secondary Use, Improper Access) Availability of Company Information Website Information Quality Design Appeal Reputation	<u>Mediator:</u> Trust in the Website <u>Moderators:</u> Privacy Concerns Prior Positive Experience Reputation	Intention to Disclose	Elaboration Likelihood Model	Students (N=667, USA)/Q/SEM
Baruh, L., Secinti, E., and Cemalcilar, Z. (2017)/ Journal of Communication/ B	Privacy Concerns Privacy Literacy Information Sharing	<u>Moderators:</u> Culture (Indulgence, Privacy Protection Laws) Gender Data Collection Mode	Online Service Use Use Intention Protective Measures Information Sharing Intention SNSs Use Privacy Literacy	Privacy Paradox CPM Theory	A total of 166 studies from 34 countries (N=75,269)/ Q/ ANOVA
Bazarova, N.N., and Choi, Y.H. (2014)/ Journal of Communication/B	Facebook Communication Forms	<u>Mediator:</u> Disclosure Goal <u>Moderator:</u> Gender	Self-Disclosure Goals Disclosure Intimacy	Theory of Self- Disclosure	Students (N=81)/ Q/ R
Bélangier, F., and Crossler, R. (2011)/ MIS Quarterly/A+	Group Dynamics Individual Differences Organizational Environment	<u>Mediators:</u> Group, Individual & Organization Information Privacy Concerns <u>Moderator:</u> Government Involvement	Societal Information Privacy Concerns	-	Literature review
Bélangier, F., Hiller, J., and Smith, W. (2002)/ The Journal of Strategic Information Systems/A	<u>Trustworthiness:</u> Third Party Privacy Seals Privacy Statements Third Party Security Seals Security Features <u>Web Features:</u> Pleasure Privacy Security	-	Purchase Intentions Willingness to Give Private Information	-	Students (N=140, USA)/Q/R
Berendt, B., Günther, O., and Spielermann, S. (2005)/ Communications of the ACM/B	<u>Privacy attitudes:</u> Privacy Fundamentalist Profiling Averse Marginally Concerned Identity Concerned	-	Privacy Behavior	-	Laboratory experiment participants (N=206, N/A)/Q/R/ C

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Bleier, A., and Eisenbeiss, M. (2015)/ Journal of Retailing/ A	Ad Personalization	Mediators: Usefulness Reactance Privacy Concerns Moderator: Trust	Click-through rate	Stimulus- Organism- Response (S-O-R)	Students (N=304, N/A)/ Q/ CFA
Chen (2013)/ Decision Support Systems/B	Personality Traits Networking Service Attributes Perceived Internet Risk	Mediator: Attitude Moderator: Privacy Value	Self-Disclosure Behaviors	Model of Users' Information Disclosure Behavior	Students (N=222, USA)/Q/PLS
Chen, J., Ping, W., Xu, Y., and Tan, B.C.Y. (2009)/ International Conference on Information Systems/A	Social Network Overlap Decisional Control Information Exclusivity	Mediator: Privacy Concerns Moderators: Social Network Overlap Information Exclusivity	Information Privacy Protective Responses	Communication Privacy Management (CPM) Theory	Students (N=156, N/A)/Q/ANCOVA/ R
Chen, J., Ping, W., Xu, Y., Tan, B.C.Y. (2015)/ IEEE Transactions on Engineering Management/B	Decisional Control	Moderators: Social Network Overlap Image Discrepancy	Information Privacy Concerns About Peer Disclosure	Communication Privacy Management (CPM) Theory Impression Management Theory	Students (N=139, N/A)/Q/ANCOVA
Choi/Lee/Land (2016)/ Information and Management/B	Information Collection Profile Control	Moderator: General Privacy Concerns Mediator: Transactional Privacy Concerns	Willingness to Delegate Profile to Facebook App	Communication Privacy Management (CPM) Theory	Students (N=284, N/A)/Q/ANOVA /PLS
Culnan, M. (1993)/ MIS Quarterly/A+	Concerns for Privacy Attitudes Toward Direct Mail Marketing Demographics	-	Attitudes Toward Secondary Information Use	-	Students (N=126, N/A)/Q/DA
Culnan, M., and Williams, C. (2009)/ MIS Quarterly/A+	Unauthorized Access Information Reuse	-	Privacy	-	-



Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Dhillon, G., Bardacino, J., and Hackney, R. (2002)/ International Conference on Information Systems/A	Maximize Encryption Enhance Customer ID Verification Minimize Sharing of Customer Information Minimize Post Transaction Record Keeping Minimize Profiting from Customer Personal Information Understand the Magnitude of Customer Privacy Fears	Maximize Security and Protection Online Ensure Buyer Anonymity & E- mail Address Confidentiality Minimize shopper profiling & Collection of Information Unrelated to Transaction Respect for Customer Data Improve Privacy Guarantees etc. <u>Mediators:</u> Institutional Trust Privacy Concerns <u>Moderator:</u> Culture	Maximize Internet Commerce Privacy	Value-Focused Thinking Approach	Participants with prior shopping experience (N=92, USA and UK)/Q/C
Dinev, T., Belloffo, M., Hart, P., Russo, V., Serra, I., and Colautti, C. (2006)/ European Journal of Information Systems/A	Propensity to Trust Perceived Risk	<u>Mediators:</u> Internet Privacy Concerns Internet Trust <u>Moderator:</u> Culture	E-Commerce Use	Hofstede's Cultural Theory Fukuyama's Theory of Trust	Survey participants (N=1311, Italy and USA)/Q/SEM
Dinev, T., and Hart, P. (2006)/ Information Systems Research/A+	Perceived Internet Privacy Risk Personal Internet Interest	<u>Mediators:</u> Internet Privacy Concerns Internet Trust	Willingness to provide personal Information	Theory of Reasoned Action Theory of Planned Behavior	Survey participants (N=369, USA)/Q/SEM
Dinev, T., and Hart, P. (2006)/ International Journal of Electronic Commerce/B	Internet Literacy Social Awareness	<u>Mediator:</u> Privacy Concerns	Intention to Transact	-	Students (N=422, USA)/Q/SEM
Dinev, T., Hart, P., and Mullen, M.R. (2008)/ The Journal of Strategic Information Systems/A	Internet Privacy Concerns Perceived Need for Government Surveillance Government Intrusion Concerns	-	Willingness to Provide Personal Information	Privacy Calculus Asymmetric Information Theory	Survey participants (N=422, USA)/Q/CFA/SEM
Dinev, T., McConnell, A.R., and Smith, H.J. (2015)/ Information Systems Research/A+	Privacy Experiences/Awareness Personality/Demographic Differences Culture	<u>Mediators:</u> Trust Privacy Concerns Privacy Calculus <u>Moderator:</u> Level of Effort	Behavioral Reactions	Privacy Calculus Elaboration Likelihood Model Antecedents - Privacy Concerns - Outcomes (APCO) Model	-

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Dohicar, S., and Jordaan, Y. (2007)/ Journal of Advertising/ B	Privacy Concern	Building Trust through direct Communication	Consumer Behavior	Integrated Marketing Communication Privacy Segmentation Index (PSI)	Survey participants (N=800)/ Q/ ANOVA
Gerlach, J., Widjaja, T., and Buxmann, P. (2015)/ The Journal of Strategic Information Systems/A	Privacy Policy Permissiveness	Mediator: Perceived Privacy Risk	Willingness to Disclose	-	Internet users (N=1116, Germany)/Q/R
Goodwin (1991)/ Journal of Public Policy and Marketing/ B	Control Over Disclosure of Information to Others Not Present During Transaction Control Over Unwanted Physical Presence of Others	-	Privacy State	Taxonomy of Privacy states	Literature review
Gu, J., Xu, Y. C., Xu, H., Zhang, C., and Ling, H. (2017)/ Decision Support Systems/ B	Perceived App Popularity Perceived Permission Sensitivity Permission Justification	Mediator: Privacy Concerns Moderator: Mobile Privacy Victim Experience	Download Intention	Privacy Calculus Elaboration Likelihood Model	Students (N=165, China)/Q/ANOVA /CFA/ PLS
Hann, I.H., Hui, K.L., Lee, S.Y.T., and Png, I.P.L. (2002)/ International Conference on Information Systems/A	Benefits (Monetary Reward, Time Saving) Gender Prior Contextual Knowledge Individualism Trust Propensity	-	Preferences over Websites	-	Students (N=184, N/A)/FG/CJ/Q/R
Hann, I.H., Hui, K.L., Lee, S.Y.T., and Png, I.P.L. (2007)/ Journal of Management Information Systems/A+	Financial Reward Visit Frequency Error Improper Access Unauthorized Secondary Use	-	Motivation Score	Expectancy Theory of Motivation Information-processing Theory of Motivation	Survey participants (N=268, USA and Singapore)/C/J/Q/R
Hoffman, D.L., Novak, T.P., and Peralta, M. (1999)/ Communications of the ACM/ B	Control Over Information Privacy Secondary Use of Information Control Trust	-	Online-Shopping Concerns	-	Survey participants: Survey 1 (N=1555, USA)/Q/ N/A Survey 2 (N=14014, USA)/Q/ N/A

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Hong, W., and Thong, J.Y.L. (2013)/ MIS Quarterly/A+	Awareness <u>Interaction Management:</u> Collection Secondary Usage Control <u>Information Management:</u> Errors Improper Access	Internet Privacy Concerns	Trusting Beliefs Risk Beliefs	Privacy Concerns	Survey participants from Hong Kong: Study 1 (commercial Websites) N=968 Study 2 (government Websites) N=961 Study 3 (commercial Websites) N=992 Study 4 (government Websites) N=887/ L/CFA and SEM
Hui, K.L., Teo, H.H., and Lee S.Y.T. (2007)/ MIS Quarterly/A+	Information Sensitivity Monetary Incentive Information Request <u>Privacy Assurance:</u> Privacy Seal Privacy Statement	-	Disclosure	Contemporary Choice Theory Internet Privacy Concerns	Students (N=109, Singapore)/Q/R
Jiang/Heng/Choi (2013)/ Information Systems Research/A+	Perceived Anonymity of Self Perceived Anonymity of Others Perceived Media Richness Perceived Intrusiveness	<u>Mediator:</u> Privacy Concerns Social Rewards	Self-Disclosure Misrepresentation	Privacy Calculus	Students (N=251, Singapore)/Q/PLS/ CFA
Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. (2015)/ Information Systems Journal/A	General Privacy Concerns General Institutional Trust Information Sensitivity	<u>Mediators:</u> Perceived Risks of Information Disclosure Perceived benefits of Information Disclosure Perceived Privacy <u>Moderator:</u> Affect	Intention to Disclose	Privacy Calculus	Survey participants (N=414, USA and Switzerland)/Q/SEM
Keith, M.J., Babb, J.S., Lowry, P.B., Furner, C., and Abdallat, A. (2015)/ Information Systems Journal/A	<u>Trust Model:</u> Self-Efficacy Structural Assurances Disposition to Trust <u>Privacy Calculus Model:</u> Self-Efficacy Privacy Concerns	<u>Trust Model:</u> <u>Mediator:</u> Coping effort <u>Privacy Calculus Model:</u> <u>Mediators:</u> Perceived Risk Perceived Benefit	<u>Trust Model:</u> Trusting beliefs <u>Privacy Calculus Model:</u> Disclosure	Social Cognitive Theory	Study 1: Students (N=509, USA)/Q/PLS Study 2: Students (N=380, USA)/Q/PLS
Krasnova, H., Hildebrand, T., and Guenther, O. (2009)/ International Conference on Information Systems/A	Price Network Popularity Profile Customizability Availability of Privacy Controls Level of Information Use by provider	-	Decision to Join an Online Social Network	Privacy Calculus	Survey participants (N=168, France, Germany, Russia, and UK)/C/J/Q/C

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010)/ Journal of Information Technology (Palgrave Macmillan)/A	Perceived Control Convenience Relationship Building Self-presentation Enjoyment	Mediators: Trust in Provider Trust in other Members Perceived Privacy Risk	Self-Disclosure	Privacy Calculus Social exchange Theory	Facebook and StudiVZ users (N=259, N/A)/Q/CFA/SEM
Lee, Im, Taylor (2008)/ Psychology and Marketing/ B	Self-presentation Relationship Management Keeping up With Trends Information Sharing Information Storage Entertainment Showing off	Voluntary Self-Disclosure	Relationship Management Psychological Well-being Habitual Behaviour	Voluntary Self- Disclosure Model	Respondents who have their own personal web space (N=259)/ Q/ EFA
Li (2012)/ Decision Support Systems/B	Procedural Fairness Social Presence Personalities Perceived Benefits Perceived Behavioral Control (Privacy Self-efficacy) Subjective Norm for Disclosure	Mediators: Social Contract (Trust) Social Response Information Boundary Threat Appraisal Coping Appraisal Perceived Costs/Risks Attitude toward Disclosure Perceived Behavioral Control (Privacy Self-efficacy) Intention to Disclose	Disclosure Behavior	Privacy Calculus Agency Theory Theory of Reasoned Action Theory of Planned Behavior	Literature review
Li, H., Gupta, A., Sarathy, R., and Zhang, J. (2014)/ Decision Support Systems/B	Privacy Control	Mediators: Perceived Benefit Trust Belief Perceived Privacy Risk Moderator: Previous Privacy Invasion	Intention to Use Standalone Personal Health Records	Social Contract Theory Privacy Calculus	Students (N=192, USA)/Q/PLS/SEM
Li, Lin (2006)/ Decision Support Systems/ B	Environmental Uncertainty Intra-Organizational Facilitators Inter-Organizational Relationships	-	Information Sharing Information Quality	Supply Chain Management	Respondents with knowledge about SCM (N=196)/ Q/ RA
Li, Lin, Wang (2015)/ Information and Management/B	Gender Age Account Rating Friend Number Blog Number Blog Length	-	Privacy Disclosure pattern: Disclosing Breadth Disclosing Depth Highly Sensitive Disclosure Less Sensitive Disclosure	Communication Privacy Management (CPM) Theory	Blog postings from the social network site "Renren" (N=1216, China)/Q/GLM

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Li, H., Sarathy, R., and Xu, H. (2011) Decision Support Systems/B	<u>Emotions (Affect-based)</u> Joy Fear <u>Fairness Levers:</u> Perceived Relevance of Information Awareness of Privacy Statement General Privacy Concern	<u>Mediators:</u> Privacy Protection Belief Privacy Risk Belief <u>Moderator:</u> Sensitivity of Information	Behavioral Intention	Privacy Calculus Social Contract Theory Stimulus-Organism-Response (S-O-R)	Students (N=175, USA)/Q/PLS
Li, T., and Unger, T. (2012)/ European Journal of Information Systems/A	<u>Privacy:</u> Privacy Concerns Privacy Protection <u>Perceived Quality of Personalization</u>	<u>Mediators:</u> Likelihood of Using Online Personalization <u>Moderators:</u> Industry Domain Past Experience Perceived Quality of Personalization	User Contribution (Willingness to Pay a Premium, Willingness to Provide Information)	Privacy Calculus	Survey participants (N= 169, N/A)/Q/PLS/ R
Liu, C., Marchewka, J., Lu, J., and Yu, C.S. (2004)/ Information and Management/B	<u>Privacy:</u> Notice Access Choice Security	<u>Mediator:</u> Trust	<u>Behavioral Intention for Online Transactions:</u> Repeat Purchase Visit Again Recommend to Others Positive Remarks Use of Instant Messaging	Privacy-Trust-Behavioral Intention Model	Students (N=212, USA)/Q/MANOVA/ SEM
Lowry, P.B., Cao, J., and Everard, A. (2011)/ Journal of Management Information Systems/A	Masculinity Uncertainty Avoidance Power Distance Collectivism	<u>Mediators:</u> Information Privacy Concerns Desire for Awareness Attitude toward Instant Messaging Technology Behavioral Intention <u>Mediator:</u> Online Privacy Concern <u>Moderator:</u> Information Sensitivity	User Action (Fabricate, Protect, or Withhold Information)	Theory of Reasoned Action Social Exchange Theory Power-Responsibility Equilibrium Framework	Students (N=486, USA and China)/Q/MANOVA/ PLS Survey participants (N= 180)/ Q/ MANOVA
Lwin, M., Wirtz, J., and Williams, J.D. (2007)/ Journal of the Academy of Marketing Science/ A	Corporate Business Policy Regulatory Perceptions Congruency (Relevance of Data to Transaction)	<u>Mediators:</u> Trusting Beliefs Risk Beliefs	Behavioral Intention	Social Contract Theory Theory of Reasoned Action	Household interview participants (N=742, USA)/L/CFA/ SEM
Malhotra, N.K., Kim, S., and Agarwal, J. (2004)/ Information Systems Research/A+	<u>Internet Users' Information Privacy Concerns:</u> Collection Control Awareness				

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Martin, K.D., and Murphy, P.E. (2017)/ Journal of the Academy of Marketing Science/A	Ethical Frameworks Global Variation Legal and Policy Implications Consumer Antecedents Consumer Outcomes Organizational Outcomes Privacy Enhancing Factors Privacy Failure	-	Privacy Research in Marketing	-	Literature review
Midha (2012)/ Decision Support Systems/B	Consumer Privacy Empowerment	<u>Mediator:</u> Privacy Concerns <u>Moderator:</u> Gender	Trust	Social Constructionist Theory	Online consumers (N=322, USA)/Q/CFA
Milne, G. R., and Rohm, A. J. (2000)/ Journal of Public Policy & Marketing/B	Data Collection Awareness Knowledge About Name Removal Mechanisms	-	Privacy Concerns	Privacy Framework	Mailing lists (N=1508)/ Q/ RA
Milgten, C. L., and Peyrat-Guillard, D. (2014)/ European Journal of Information Systems/A	Control Protection & Regulation Trust Responsibility	<u>Mediator:</u> Privacy Concerns <u>Moderators:</u> National Culture Age	Disclosure Behavior Protection Behavior	Hofstede's Cultural Theory	Participants (N=139, Romania, Greece, France, Estonia, Spain, Poland & Germany)/ FG/Q/CATA
Miyazaki, A. D., and Fernandez, A. (2000)/ Journal of Public Policy & Marketing/B	Disclosure of Privacy Statements and Practices by Online Retailers	-	Information Privacy	Information Privacy	Websites of enterprises (N=381, USA)/ Q/ N/A
Nicolaou, A. I., Ibrahim, M., and van Heck, E. (2013)/ Decision Support Systems/ B	Information Quality	<u>Mediators:</u> Perceived Performance Risk Perceived Exchange Risk Expected Transaction Performance Competence Trust Goodwill Trust	Intention to Continue Use of Data Exchange	Expectation-Disconfirmation Framework	Business professionals (N=221)/ Q/ LISREL
Okazaki, S., Li, H., and Hirose, M. (2009)/ Journal of Advertising/B	Prior Negative Experience	<u>Mediators:</u> Trust Privacy Concerns <u>Moderators:</u> Perceived Risk Perceived Ubiquity Sensitivity of Information Request	Degree of Regulatory Control	Social Contract Theory	Survey participants (N=510/Q/PLS)

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Okazaki, S., Navarro-Bailón, M. A., and Molina-Castillo, F. J. (2012)/ International Journal of Electronic Commerce/ B	Social Anxiety Situational Involvement	<u>Moderator:</u> Social Anxiety	Privacy Concerns Intention to: -Protect -Fabricate -Withhold -Loyalty	Utility Maximization Theory	Survey participants (N=667, Japan)/Q/CFA /ANOVA
Pan, Y., and Zinkhan, G.M. (2006)/ Journal of Retailing/ A	Presence of an Online Privacy Policy	<u>Moderator:</u> Privacy Risk	Consumer Trust Consumer Response Intention	Situational Normality Social Contract Theory	Potential subjects from telephone directory (N=525)/ Q/ EFA, ANOVA, ANCOVA
Park, I. (2009)/ International Conference on Information Systems/A	Privacy Concerns	<u>Mediators:</u> Information Systems Reactance Procedural Justice	Perceived Usefulness Information Systems Satisfaction	Psychological Reactance Theory	Bank employees (N=251, Corea)/Q/PCA/SEM
Park, C., Jun, J., and Lee, T. (2015)/ International Marketing Review/ B	Privacy Concerns Consumer Innovativeness Propensity to Share Information	<u>Mediators:</u> Intensity of Use of Social Network Sites <u>Moderator:</u> Culture	Social Capital	Social Network Use	Smartphone users (N=977)/ Q/ SEM
Phelps, J., Nowak, G., and Ferrell, E. (2000)/ Journal of Public Policy and Marketing/ B	Type of Personal Information Requested Amount of Information Control Offered Potential Consequences and Benefits Consumer Characteristics	Beliefs regarding marketers' Information Practices Companies' Use of Personal Information	Behavioral and Future Attitudinal Responses	Privacy Concerns	Catalog shoppers, randomly selected residences (N=1000)/ Q/ CFA
Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., and Hofacker, C.F. (2010)/ International Journal of Electronic Commerce/B	Trust Compensation	<u>Moderator:</u> Trust	Willingness to Provide Information Behavioral Information Disclosure Sensitive Information	-	Lab experiment participants (N=187, Italy)/Q/ANCOVA
Roback, D., and Wakefield, R.L. (2013)/ ACM SIGMIS Database/B	Socialness Perceived Ease of Use Privacy Control	<u>Mediators:</u> Enjoyment Perceived Usefulness Privacy Risk <u>Mediators:</u> Privacy Protection Belief Privacy Risk Belief <u>Moderator:</u> Perceived Relevance	Intentions to Use Location-based applications Behavioral Intention	Social Exchange Theory	Students (N=222, USA)/Q/PLS/ SEM
Sarathy, R., and Li, H. (2007)/ International Conference on Information Systems/A	Perceived Relevance Perceived Usefulness Monetary Rewards	<u>Mediators:</u> Privacy Protection Belief Privacy Risk Belief <u>Moderator:</u> Perceived Relevance	Behavioral Intention	Social Contract Theory Theory of Reasoned Action	Students (N=182, USA)/Q/PLS/ R

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Sheehan, K.B., and Hoy, M.G. (1999)/ Journal of Advertising/ B	Privacy Concerns	-	Registering for Website Providing Inaccurate / Incomplete Information Reading Unsolicited e-mail Notifying ISP about Unsolicited e- mail Requesting removal from mailing list Sending highly Negative Response ("flame")	Privacy Concerns	Individuals with personal e-mail addresses (N=889)/ Q
Sheehan, K.B., and Hoy, M.G. (2000)/ Journal of Public Policy and Marketing/ B	Control Awareness of Information Collection Usage Beyond Original Transaction	-	Privacy Concerns	Core Principles of Information Collection Online	Individuals with personal email addresses (N=889)/ Q/ ANOVA, EFA
Smith, H., Dinev, T., and Xu, H. (2011)/ MIS Quarterly/A+	Privacy Experiences Privacy Awareness Personality Differences Demographic Differences Culture/Climate Regulation Privacy Notice/Seal Privacy Calculus	<u>Mediators:</u> Privacy Concerns Trust	Behavioral Reactions	-	Literature review
Smith, H., Milberg, S., and Burke, S. (1996)/ MIS Quarterly/A+	Collection Errors Unauthorized Secondary Use Improper Access	-	Privacy Concerns	Personality Theory	Focus group participants (N=2318, USA)/L/CFA
Son, J., and Kim, S.S. (2008)/ MIS Quarterly/A+	Information Privacy Concerns Perceived Justice Societal Benefits from Complaining	-	<u>Information Provision:</u> Refusal Misinterpretation <u>Private Action:</u> Removal Negative Word-of-mouth <u>Public Action:</u> Complaining directly Complaining to Third-Party Organizations	Social Justice Theory	Survey participants (N=523, USA)/Q/CFA /SEM
Stewart, K.A., and Segars, A.H. (2002)/ Information Systems Research/A+	Computer Anxiety	<u>Mediators:</u> Concerns for Information Privacy instrument	Behavioral Intention	Concerns for Information Privacy (CFIP)	Consumer survey participants (N=355, USA)/ Q/CFA



Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Sutanto, J., Palime, E., Tan, C., and Phang, C.W. (2013)/ MIS Quarterly/A+	Provision of a Personalization Feature	Mediators: Perceived Intrusion Perceived Personalization Benefits Psychological Comfort with the Application	Intention to Save Advertisements	Uses and Gratification Theory Information Boundary Theory	Field experiment participants (mobile phone Users) (N=691, N/A)/Q/R
Tam, E., Hui, K., and Tan, B. (2002)/ International Conference on Information Systems/A	Monetary Savings Time Savings Pleasure Novelty Self-enhancement Social Adjustment Altruism	-	Disclosure	Social Exchange Theory Expectancy Theory Economic Utility Theory	Students (N=371, N/A)/Q/PCA
Tang, Z., Hu, Y., and Smith, M. (2008)/ Journal of Management Information Systems/A	Caveat Emptor Seal-of-approval Programs Mandatory Standards	-	Trust	Game Theory (Hidden Information) Privacy Concerns	Game theoretical Model
Tow, N.W.-F.H., Dell, P., and Venable, J. (2010)/ Journal of Information Technology (Palgrave Macmillan)/A	Online Experience Prior Knowledge from Media and Friends Knowledge about Privacy controls	Mediator: Value (Personal Attitude Preference and Comfort Level)	Behavior (Acting Online, Information Willing to Share, Action Taken to Protect)	-	Interview participants (N=25, Australia)/Q/Domain Analysis
Tucker, C.E. (2014)/ Journal of Marketing Research/ A+	Privacy Concerns	Perceived Control	Clickrate on Online Advertising	Effectiveness of Personalizing Ad Text	Facebook users (N=7,560 N/A)/Q/ R
Van Slyke, C., Shim, J.T, Johnson, R., and Jiang, J.J. (2006)/ Journal of the Association for Information Systems/A	Concerns for Information Privacy Familiarity	Mediators: Risk perception Trust Moderator: Familiarity	Willingness to Transact	Privacy Concerns	Consumers from Amazon.com and Half.com (N=1,000, N/A)/L/PCA/ SEM
Wakefield (2013)/ The Journal of Strategic Information Systems/A	Internet Security Positive Affect Negative Affect	Mediators: Website Trust Website Privacy	Intention to Disclose	Cognitive Consistency Theory	Survey participants (N=301, N/A)/Q/PLS
Walker (2016)/ Journal of Public Policy and Marketing/ B	Trust Transparency	-	Consumer Information Exchange	Sharing-- Surrendering Information Matrix	Literature review
Wirtz, J., and Lwin, M.O. (2009)/ Journal of Service Research/ A	Consumer Perceptions of Organizational Practices (Justice Dimensions)	Privacy Concern Trust	Promotion-focused Behaviors Prevention-focused Behaviors	Regulatory Focus Theory	Students (N=271, N/A)/ Q/ ANOVA, CFA

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Xu, H. (2007)/ International Conference on Information Systems/A	Technology Self-Regulation Legislation	Perceived Control	Privacy Concerns	Control agency Theory Self-Constual Theory	Lab-experiment participants (N=141, Singapore)/Q/ANOVA/ PLS
Xu, H., Dinev, T., Smith, H., and Hart, P. (2008)/ International Conference on Information Systems/A	Antecedents to Disposition to Privacy: Privacy Awareness Privacy Social Norm Institutional Privacy Assurance: Perceived Effectiveness of Privacy Policy Perceived Effectiveness of Industry Self-regulation	Mediators: Privacy Risk Disposition to Value Privacy Privacy Control Perception of Intrusion	Privacy Concerns	Information Boundary Theory	Students (N=823, USA)/Q/PLS
Xu, H., Luo, X., Carroll, J.M., and Rosson, M.B. (2011)/ Decision Support Systems/B	Personalization Interpersonal Differences: Previous Privacy Experience Personal Innovativeness Coupon Proneness	Mediators: Perceived Benefits Perceived Risks Perceived Value Willingness to have personal Information Used Moderator: Covert vs. Overt	Purchase Intention	Privacy Calculus Social Exchange Theory Economic Utility Theory	Students (N=545, N/A)/Q/PLS
Xu, Y., Tan, B., and Hui, K. (2003)/ International Conference on Information Systems/A	Reward Preference Privacy Concern Trust	Moderator: Consumer Trust	Disclosure Intention	Social Exchange Theory	Students (N=331, N/A)/Q/CFA/R
Xu, H., Teo, H.H., and Tan, B. (2005)/ International Conference on Information Systems/A	Third Party Privacy Seals Platform for Privacy Preferences (P3P) Project Compliance Device-Based Privacy Enhancing Features	Mediators: Trust Beliefs Perceived Privacy Risks	Behavioral Intention	Social Contract Theory	Mobile phone users (N=176, Singapore)/Q/ANOVA/PLS
Xu, H., Teo, H.H., Tan, B., and Agarwal, R. (2012)/ Information Systems Research/A+	Individual Self-Protection Industry Self-regulation Government Legislation	Moderator: Individual Self-Protection Mediator: Perceived Control	Context-specific Privacy Concerns	Control Agency Theory	Survey participants (N=178, Singapore)/Q/SEM/ANOVA
Yang S., and Wang, K. (2009)/ ACM SIGMIS Database/B	Information Sensitivity Compensation	Mediator: Privacy Concern	Information Disclosure Protection Intention Transaction Intention	Social Exchange Theory	Students (N=458, China)/Q/R /ANOVA/ GLM/CFA/SEM

Authors(Year)/ Journal/VHB-Rank	Independent Variable(s)	Mediator/ Moderator	Dependent Variable(s)	Conceptual Basis	Sample/ Survey design/ Analysis method
Yu, Hu, Cheng (2015)/ Journal of Management Information Systems/A	Affect Toward Self-disclosures Affect Toward Social Network Website	Mediators: Self-presentation Expression Social Acceptance Reciprocity Social Rejection Privacy Risk	Self-Disclosures on Social Network Websites	Direct Causation Theory Affect Heuristic Theory	Students (N=517, Taiwan)/Q/CFA
Zhao, L., Lu, Y., and Gupta, S. (2012)/ International Journal of Electronic Commerce/B	Incentives Provision Interaction Promotion Privacy Control Privacy Policy Awareness of Legislation Previous Privacy Invasions Personal Innovativeness	Mediators: Extrinsic Benefits (Personalization) Intrinsic Benefits (Connectedness) Privacy Concerns	Intention to Disclose location- based Information	Justice Theory	Survey participants (N=368, China)/Q/CFA/SEM
Zimmer, J.C., Aisal, R.E., Al- Marzouq, M., and Grover, V. (2010)/ Information and Management/B	Trust Relevance	Mediators: Risk Attitude Moderator: Usefulness	Intention to Disclose	Transaction Cost Economics Theory of Reasoned Action	Students (N=264, USA)/Q/MANOVA/ SEM
Zimmer, Aisal, Al-Marzouq, Moore, Grover (2010)/Decision Support Systems/B	Trust Privacy Benefits	Mediator: Intention to Disclose Moderator: (Un)reasoned Dyadic Condition	Disclosure	Theory of Reasoned Action Social Response Theory	Students (N=236, USA)/Q/R

ANCOVA = Analysis of Covariance; ANOVA = Analysis of Variance; CATA = Correlation Analysis; CFA = Confirmatory Factor Analysis; CJ = Conjoint Analysis; DA = Discriminant Analysis; EFA = Exploratory Factor Analysis; FG = Focus Group; GLM = General Linear Modelling; L = longitudinal study; LISREL = Linear Structural Relations; MANOVA = Multivariate Analysis of Variance; N/A = Not Available; PCA = Principal Component Analysis; PLS = Partial Least Squares; Q = cross-sectional study; R = Regression Analysis; SEM = Structural Equation Modeling