Steudner, Tobias

Conference Paper

Consumer Groups and their Risk Perception in a Data Sharing Cooperation between Two Firms

ITS Online Event, 14-17 June 2020

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Steudner, Tobias (2021) : Consumer Groups and their Risk Perception in a Data Sharing Cooperation between Two Firms, ITS Online Event, 14-17 June 2020, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/235909

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 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 statements about what cause those different standpoints and about 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.[1] 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[2], 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

[1] It was verified that the obtained observations during the two collections are not significantly different.

[2] 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[3], 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 α 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.

	Construct Mean (Construct Standard Deviation)										
Consumer Group	**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.

[3] 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 (Δ_{Gr1-3} = .90, p = .04; Δ_{Gr2-3} = .80, p = .06) and dealt least intensively with privacy related issues in this situation (Δ_{Gr1-3} = .89, p = .008; Δ_{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 (Δ_{Gr1-3} = .77, p = .001; Δ_{Gr2-3} = .78, p = .002). Consumers in the "unreflected"-group have lower privacy concerns (GIPC: Δ_{Gr1-3} = .68, p < .001; Δ_{Gr2-3} = .66, p = .002; IPC: Δ_{Gr1-3} = .74, p = .015; Δ_{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 $Effect_{3-1}$) describes the effect for the "unreflective"-group compared to the "risks increase"-group, and the second regression coefficient (Group $Effect_{3-2}$) 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).[4]

We accept hypothesis H4, as consumers in the "unreflected"-group perceive the lowest privacy risks (Table 2: Δ_{Gr1-3} = 1.51, p < .001; Δ_{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: β_{Gr3-1} = 1.202, p < .001; β_{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

[4] 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.

		Regression 1		Regression 2		Regression 3	
Model: F-statistic, p-Value, R^2		RISK regressed on GIPC and Group-Effect: F(3, 178) = 18.51, p<.001; $.R^2$ = .238		WTD regressed on BENE, GIPC and Group-Effect: F(4, 177) = 50.5, p<.001; R^2 = .533		WTD regressed on RISK and Group-Effect: F(3, 178) = 51.93, p<.001; R^2 = .467	
Variable		**β (std. error)**	**t-Value (p-Value)**	**β (std. error)**	**t-Value (p-Value)**	**β (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 (β) 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: Δ_{Gr1-3} = -1.49, p < .001; Δ_{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: β_{Gr3-1} = -.468, p = .099; β_{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: β_{Gr3-1} = -.217, p = .483; β_{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 α. Item loadings in parentheses; correctness of statements in square brackets; * signalizes a reversive coded item.*

Global Information Privacy Concerns (GIPC)	
Abbreviated from Malhotra et al. (2004), Smith et al. (1996); Cronbach's α: .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.
Internet Privacy Concerns (IPC)	
Adapted from Dinev & Hart (2006), Culnan & Armstrong (1999), Smith et al. (1996); Cronbach's α: .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.
Mental Effort (ME)	
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?
Need for Cognition (NfC)	
Abbreviated from Cacioppo et al. (1984); Cronbach's α: .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.
Intensity of Dealing with Privacy Relevant and Situational Aspects (DEAL)	
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]
Privacy Intrusion Victim (VICT)	
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?

Question on Consumers' Data Sharing Cooperation Privacy Risk Consequences	
Question and answers, which are single response options, based on a pre-study (Steudner 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.
Perceived Benefits (BENE)	
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
Perceived Privacy Risks (RISK)	
Adapted from Dinev, Xu, Smith, & Hart (2013), Dinev & Hart (2006), Featherman & Pavlou (2003); Cronbach's α: .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.
Willingness to Disclose (WTD)	
Adapted from Anderson & Agarwal (2011); Cronbach's α: .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 (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/ (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).
Steudner, 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.