RETHINKING PRIVACY DECISIONS: PRE-EXISTING ATTITUDES, PRE-EXISTING EMOTIONAL STATES, AND A SITUATIONAL PRIVACY CALCULUS

Complete Research

Flavius Kehr, Institute of Technology Management, University of St. Gallen, St. Gallen, Switzerland, flavius.kehr@unisg.ch

Daniel Wentzel, Chair of Marketing, RWTH Aachen University, Aachen, Germany, wentzel@time.rwth-aachen.de

Tobias Kowatsch, Institute of Technology Management, University of St. Gallen, Switzerland, tobias.kowatsch@unisg.ch

Elgar Fleisch, Institute of Technology Management, University of St. Gallen, St, Gallen, Switzerland, elgar.fleisch@unisg.ch

Abstract

As a potential explanation to measured inconsistencies between stated privacy concerns and actual disclosing behavior, denoted as the „privacy paradox", scholars have proposed a systematic distinction between situational privacy considerations and pre-existing, superordinate factors that shape the decisive situation without being directly connected to the situation itself. Deploying an experimental approach, we explored the dynamics of two types of such pre-existing factors, namely (1) pre-existing attitudes (such as general privacy concerns and general institutional trust) and (2) pre-existing emotional states (such as an individual's current mood) in shaping situation-specific risk and benefit considerations (i.e., a situational privacy calculus). Compared to a negative emotional state, individuals in a positive emotional state were found to perceive lowered situation-specific privacy risks, even if the sources of this state were unrelated to the decisive situation at hand. Moreover, results indicated that pre-existing attitudes may be partially or even fully overridden by situational risk and benefit considerations. Adopting a differentiated view on privacy decision-making, these findings imply that the privacy paradox could be driven by a gap between pre-existing cognitive and affective factors on the one side, and situation-specific considerations and decisions on the other. Implications for researchers and practitioners are discussed.

Keywords: Privacy Paradox, Privacy Calculus, Pre-Existing Attitudes, Emotion, Mood, General Privacy Concerns, General Institutional Trust

1 Introduction

More than ever, individuals are required to disclose private information in order to conduct e-commerce transactions (Pavlou and Gefen, 2004), register with online services (Li et al., 2013), or use smartphone applications (Keith et al., 2013). In this regard, notions of information privacy have raised increased attention by both researchers and practitioners (Belanger and Crossler, 2011; Smith et al., 2011). In particular, understanding the cognitive processes that underlie individual privacy decisions has developed as a field of fruitful research, yielding manifold factors that may shape individuals' privacy decisions, such as financial rewards (Xu et al., 2009), personalization (Sutanto et al., 2013), or the presence/absence of privacy seals (Hui et al., 2007).

Simultaneously, however, studies have pointed to inconsistencies between reported privacy concerns and disclosing behaviors, denoted as the *privacy paradox* (Awad and Krishnan, 2006; Li et al., 2011; Norberg et al., 2007; Spiekermann et al., 2001; Xu et al., 2011). That is, individuals tend to disclose their data "as if they didn't care" (Dinev and Hart, 2006), even if they report to be highly worried about potential data misuse (Norberg et al., 2007). As a potential explanation, scholars have recently started to distinguish pre-existing factors from a situation-specific privacy assessment, arguing that situation-specific considerations may have the potential to override general attitudes and tendencies (Kehr et al., 2013; Li et al., 2011; Wilson and Valacich, 2012). Stated differently, individuals may highly rely on factors that are genuine to the current situation when evaluating a privacy decision at hand, rather than considering superordinate, more time-consistent perceptions or attitudes (Kehr et al., in press). Embracing these assumptions, the current study seeks to explore cognitive and affective factors that may shape privacy-related decisions in a concrete situation without being directly connected to the situation itself. More precisely, we introduce and empirically test a model that rigorously distinguishes between pre-existing, superordinate factors, and situation-specific privacy considerations. Using an experimental setup, we attempt to demonstrate how two types of pre-existing factors, namely (1) pre-existing *attitudes* (such as general privacy concerns and general institutional trust) and (2) pre-existing *emotional states* (such as an individual's current mood), may shape situation-specific privacy cognitions and decision behavior. By doing so, we aim to answer the following research questions:

RQ1: How do pre-existing attitudes shape a situational privacy calculus?

RQ2: How do pre-existing mood states shape a situational privacy calculus?

In the following, we will first review pertinent research streams and introduce our conceptual model. Next, we will overview the methodology applied, and present the results of an empirical study aiming to test the model's predictions. Then, we will discuss theoretical and practical implications of the findings, and provide a summarizing conclusion.

2 Conceptual Model and Hypotheses

In information privacy literature, privacy-related decisions are typically regarded as an outcome of a rational, cognitive assessment of perceived risks and perceived benefits connected to the disclosure of private information, denoted as the privacy calculus (Anderson and Agarwal, 2011; Culnan and Armstrong, 1999; Dinev and Hart, 2006). That is, individuals are expected to independently weigh the "potential for loss associated with the release of private information" (Smith et al., 2011) against the "value from the disclosure of private information" (Wilson and Valacich, 2012) before deciding on whether or not they would like to disclose private information to a product or service. Our conceptual model, as depicted in Figure 1, embraces these assumptions by modelling the willingness to disclose private information as a conjoint outcome of (1) privacy-related risk perceptions and (2) privacy-related benefit perceptions. In contrast to many prior studies, however, we conceptualize the privacy calculus as a situation-specific risk-benefit trade-off, subject to interference by pre-existing factors. More precisely, we propose that (1) pre-existing *attitudes*, such as general privacy concerns and general institutional trust, and (2) pre-existing *emotional states*, such as positive and negative moods, may affect situation-specific risk and benefit considerations, even without being directly associated with the decision at hand. Rationales for these assumptions are provided in the following.

2.1 A Situational Privacy Calculus

In the privacy calculus literature, the willingness to disclose private information has been typically modeled as a conjoint outcome of a cognitive assessment of privacy-related risk perceptions and privacy-related benefit perceptions connected to information disclosure (Anderson and Agarwal, 2011;

Dinev and Hart, 2006). Importantly, however, the privacy calculus perspective also assumes that individuals carefully anticipate and weigh privacy-related risks and benefits of information disclosure *every time* they are confronted with a situation that requires the provision of private information (Culnan and Armstrong 1999; Dinev and Hart 2006; Malhotra et al. 2004). Consequently, one could expect risk and benefit assessments to significantly vary across situations and to entail different behaviors, respectively. Stated differently, situational factors may serve as important cues that signal whether a data-requesting situation is more or less risky, or more or less beneficial (Li et al. 2011; Malhotra et al. 2004). In line with this notion, studies have identified numerous factors that enhance or mitigate risk and benefit perceptions. For example, individuals may perceive increased risks in situations that require more sensitive information (Bansal et al. 2010; Malhotra et al. 2004; Mothersbaugh et al. 2012), but lowered risks in situations in which a privacy policy is present and designed thoroughly (Wu et al. 2012). Similarly, situations that signal a non-profit (as opposed to a commercial) purpose of data provision or a non-commercial stakeholder may increase a person's willingness to provide personal information (Anderson and Agarwal 2011; Li and Unger 2012). This "contextual nature of privacy" has also been noted by Smith et al. (2011, p. 1002), who called for an increased effort in investigating privacy as a situation-specific phenomenon that is driven by contextual cues.

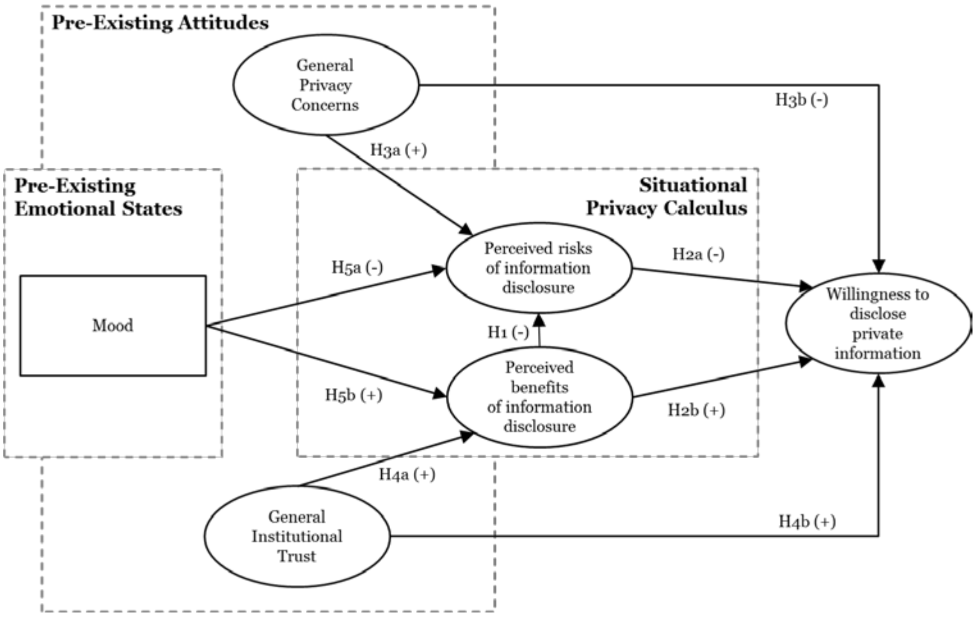
Pre-Existing Attitudes
General Privacy Concerns
H3b (-)
H3a (+)
Pre-Existing Emotional States
Situational Privacy Calculus
Mood
H5a (-)
Perceived risks of information disclosure
H2a (-)
Willingness to disclose private information
H1 (-)
H5b (+)
Perceived benefits of information disclosure
H2b (+)
H4a (+)
General Institutional Trust
H4b (+)

Figure 1. Conceptual Model.

Against this background, we argue the privacy calculus to constitute a *situational* trade-off of privacy-related risks and benefits, subject to variation across situations. Importantly, moreover, recent findings suggest that individuals may be incapable to assess both sides of the calculus separately, assuming that individuals tend to perceive lower risks if anticipated benefits of information disclosure are high (Dinev et al., 2012; Kehr et al., 2013). Following these insights, we predict situation-specific risk and benefit perceptions to antecede privacy-related behaviors and decisions, while risk and benefit perceptions constitute interdependent factors. Thus, we hypothesize:

H1: Perceived benefits of information disclosure will be negatively associated with perceived risks of information disclosure.

H2a: Perceived risks of information disclosure will be negatively associated with the willingness to disclose private information.

H2b: Perceived benefits of information disclosure will be positively associated with the willingness to disclose private information.

2.2 Pre-Existing Attitudes: Privacy Concerns and Institutional Trust

While scholars have argued that privacy constitutes a situation-specific, contextual phenomenon (see above), scholars have often conceptualized privacy concerns on a global, unspecific level, e.g. as an "individual's *general* tendency to worry about information privacy" (Li et al., 2011, p. 5). As such, scholars have argued that (1) privacy concerns may remain stable over time and in different situations (Kehr et al., in press), while (2) privacy-related cognitions of an individual in a certain situation may highly vary due to specific characteristics of the given context, such as attributes of a certain product (John et al., 2011; Li et al., 2011; Wilson and Valacich, 2012), or specific anticipated benefits (Xu et al., 2011). As such, it becomes likely to assume that an "individual who generally doubts the proper use of private data by information systems may be persuaded to overcome his or her skepticism in a concrete situation and may provide private data" (Kehr et al., 2013, p. 2), resulting in an observed discrepancy between stated privacy concerns and actual behavior.

Adopting this view, we model general privacy concerns as an antecedent to a situation-specific privacy calculus. More precisely, we rely on prior research that has typically associated privacy concerns with the risk side of a privacy trade-off (e.g. Anderson and Agarwal, 2011), and predict pre-existing, general privacy concerns to shape privacy-related risk cognitions in a given situation. In line with prior research (Kehr et al., 2013; Li et al., 2011; Wilson and Valacich, 2012), we also assume that general privacy concerns may be reconsidered by individuals when expressing their willingness to disclose private information. Thus, we hypothesize that (1) general privacy concerns may be associated with the willingness to disclose private information directly, and (2) that a situation-specific risk assessment may partially mediate the negative association between general privacy concerns and the willingness to disclose private information:

H3a: General privacy concerns will be positively associated with perceived risks of information disclosure.

H3b: General privacy concerns will be negatively associated with the willingness to disclose private information.

H3c: The negative association between general privacy concerns and the willingness to disclose private information will be partially mediated by perceived risks of information disclosure.

Besides, a small stream of literature has argued that institutional trust, often conceptualized as "an individual's confidence that the data-requesting stakeholder or medium will not misuse his or her data" (Kehr et al., 2013), may shape situation-specific privacy considerations in a similar manner as general privacy concerns. In line with this assumption, Anderson and Agarwal (2011), for example, found trust in the data-collecting electronic medium to constitute a pre-existing cognitive factor subject to interference by situational variables, such as beliefs about the stakeholder requesting a particular piece of information. As such, it becomes likely to assume that a conceptualization of institutional trust as a pre-existing attitude may help to deepen insights on privacy-related cognitions and decision-making. Since prior research suggests that trust is a protective factor that mitigates risk beliefs and privacy concerns (Bansal et al., 2010; Kim et al., 2008; Malhotra et al., 2004), we assume that general institutional trust may primarily affect the benefit side of a situation-specific privacy calculus. However, we also believe that users will rely on pre-existing *and* situation-specific factors when assessing their willingness to disclose private information. Thus, we hypothesize perceived benefits of information disclosure to partially mediate the relationship between general institutional trust and the willingness to disclose information.

H4a: General institutional trust will be positively associated with perceived benefits of information disclosure.

H4b: General institutional trust will be positively associated with the willingness to disclose private information.
H4c: The positive association between general institutional trust and the willingness to disclose private information will be partially mediated by perceived benefits of information disclosure.

2.3 Pre-Existing Emotional States: Mood

While research on privacy-related decision-making has predominantly regarded the willingness to disclose private information as an outcome of a *rational* assessment of both anticipated risks and benefits connected to data provision, a growing body of literature considers privacy valuation processes to be influenced by bounded rationality, emotional states, or intuitive thinking (Brandimarte et al., 2013; Kehr et al., 2013; Li et al., 2011; Wakefield, 2013). Li et al. (2011) as well as Wakefield (2013), for example, found positive (and negative) emotional states evoked by the interface or interaction with an information system (IS) to positively (or negatively) impact privacy-related constructs such as trust or risk beliefs. Similarly, (Kehr et al., in press) showed individuals to underestimate privacy-related risks if confronted with a screenshot that evoked positive feelings. Typically, however, these studies attempted to investigate emotional states that were directly induced by characteristics of a given IS, such as its user interface. As such, prior studies have largely neglected the potential of emotional states in shaping situational decisions, even if the source of these feelings is not directly associated with the decisive situation itself.

In this regard, research in psychology and behavioral economics suggests that an individual's current mood, defined as a weak, yet enduring emotional state (George, 1989), is capable to guide human behavior and decision-making without being connected to a certain situation directly. That is, positive moods (e.g. happiness) typically entail a more superficial cognitive elaboration of arguments, resulting in more positive judgments than negative moods (e.g. sadness, Schwarz and Clore, 1983; Schwarz et al., 1987). Importantly, however, this "how do I feel about it" heuristic (Schwarz and Clore, 1988) does not necessarily depend on conscious cognitive attribution, i.e. individuals don't have to consciously connect their feelings to characteristics of the decision at hand (Schwarz, 2011). Rather, current moods may serve as global cues that shape information perception, processing and validation in multiple future situations (ibid.). In a seminal study by Schwarz and Clore (1983), for example, happy or sad mood was induced by asking participants to recall either positive or negative life events, resulting in a mood-congruent rating of their own life satisfaction, i.e. individuals in a happy mood reporting higher life satisfaction than individuals in a negative mood. Similarly, Hirshleifer and Shumway (2003) showed positive mood to mediate the relationship between sunny weather and increasing stock market investments, indicating financial decisions may be heavily impacted by an individual's current mood, even if the source of one's mood does not connect to the decision at hand (stock market investments), but originates from other sources (sunny weather). Also, a large stream of research engaged in mood-congruency effects in social judgments, such as school admission interviews (Redelmeier and Baxter, 2009) or partner choice (Forgas, 1991). With regard to the judgment of risks and benefits, moreover, prior work has repeatedly reported mood-congruency effects, showing that individuals in a positive mood tend to process information more superficially, resulting in higher reported risk-taking attitudes and riskier choices. Individuals in negative mood states, in contrast, tend to judge more conservatively due to deeper and more elaborated information processing (Forgas, 1995; Johnson and Tversky, 1983; Kim and Kanfer, 2009; Yuen and Lee, 2003).

Regarding the privacy calculus model as a situation-specific trade-off between perceived risks and perceived benefits, we expect mood-congruency effects to be transferable to the field of information privacy. That is, we assume individuals to value risks as high and benefits as low when in a positive mood, even if the reason for their good mood is unlikely connected to the subject of valuation (Schwarz, 2011). In line with this assumption, we postulate that a positive mood, in contrast to a negative mood, will result in higher benefit and a lower risk perceptions when taking a privacy-related decision (Forgas, 1995; Johnson and Tversky, 1983):

H5a: In contrast to a negative mood, a positive mood will negatively impact perceived risks of information disclosure.
H5b: In contrast to negative mood, a positive mood will positively impact perceived benefits of information disclosure.

3 Methodology

In order to test our model, we designed and conducted a cross-sectional online experiment, manipulating users' mood while simultaneously requesting for privacy-related constructs such as general privacy concerns, risk and benefit perceptions and the willingness to disclose information. The experiment was presented as a very early market research on the potential of an upcoming smartphone application intended to improve driving skills.

3.1 Sample and Procedure

Participants were recruited via university-related communication channels, such as mailing lists and Facebook groups. We did not disburse any incentive for participation.

After clicking on the link to the study, participants were randomly assigned to one of two experimental conditions, and watched a short video clip with an either funny or sad content. For the sad movie condition, we used an extract from 1979's film "The Champ", in which a little boy cries after his father has died in a boxing match. In contrast, a scene from the movie "When Harry met Sally" (1989) served as manipulation in the positive mood condition, featuring a fake orgasm of the female protagonist in a restaurant. Both movie clips have been extensively tested for validity with respect to their ability to induce positive and negative moods (Gross and Levenson, 1995; Hewig et al., 2005). Importantly, the mood-inducing experimental material was chosen to be unrelated to the decision at hand. That is, the content of the deployed movie clips did not relate to topics of privacy, driving behavior, or technology (i.e., smartphone applications, computers etc.).

After a short manipulation check, the basic idea of the driving behavior application was introduced. To this extent, participants read a short text, telling them the application provided tips for safer or greener driving based on individual driving behavior, and that the app had to collect several types of data to achieve this goal, including GPS coordinates and position, velocity and speeding, travel date, time and distance as well as acceleration behavior and demographic data (e.g. age, gender, driving experience). Furthermore, the text emphasized that all of the collected data would be shared with insurance companies, universities and public institutions to improve traffic safety and establish programs on ecological driving. Finally, participants were asked to fill out a questionnaire containing privacy-related scales and constructs as well as questions on both private (e.g. age, gender) and driving-related (e.g. driving experience) demographics. They also answered questions on the familiarity with the watched movie scene and smartphone possession. In order to decouple questions on general privacy concerns and general institutional trust from the given situation, items were presented on a separate questionnaire page and introduced using an adequate instruction ("Now we would like to receive your opinion on data disclosure *in general*").

3.2 Used measures

Wherever possible, measures were adapted from previous studies. In order to check for successful mood induction, we used the sadness and joviality subscales of the expanded form of the Positive and Negative Affect Schedule (PANAS-X, (Röcke and Grühn, 2003; Watson et al., 1988), a well-established instrument to capture moods and emotion. Items were measured on a 5-point Likert scale ranging from 1 (not at all) to 5 (extremely). Scales for perceived privacy risks and perceived benefits were adapted from Dinev et al. (2012) and assessed with four and three items, respectively (e.g. "Private data could be used inappropriately by the provider of this smartphone application"). The willingness to disclose information was captured by three items adopted from Anderson and Agarwal

(2011). General privacy concerns and general institutional trust were measured with two respectively four items adapted from Dinev and Hart (2006) (e.g. General Institutional Trust: “Normally, providers of smartphone applications are honest when dealing with private data”, General Privacy Concerns: “In general, I am worried about the misuse of my private data”). In order to ensure semantic equivalence and validity, items were first translated to German by the authors, and then translated back to English and compared to the original wording by an English native speaker. All privacy-related items were measured on a 6-point Likert scale ranging from 0 (totally disagree) to 5 (totally agree).

4 Results

In total, 148 persons participated in the study. In a first step, we excluded (1) participants with incomplete questionnaires or unreasonable completion times (< 8 minutes), and (2) participants who declared to be familiar with the correspondent movie clip in order to prevent biased responses due to memory effects (Kim et al., 2009). The mean age of the remaining 94 participants was 25.28 years (*SD* = 6.59), and 73% of them were female. More than two thirds (69%) of the respondents possessed a smartphone, and 89% had access to a car on a regularly base (own car, car of family members, corporate car etc.). After this initial screening, we proceeded by (1) testing the manipulation’s effectiveness and (2) fitting a structure equation model that represented our conceptual framework.

4.1 Manipulation Check

After watching the movie clip, participants were asked to rate their current mood on the sadness and joviality subscales of the PANAS-X (Röcke and Grühn, 2003). As internal consistency of the two scales was sufficient (Sadness: 5 items, $\alpha = .83$; Joviality: 8 Items, $\alpha = .96$), we conducted independent sample t-tests for the averaged values of both scales to test for manipulation effectiveness. Results indicated mood induction was successful, with participants who watched the sad movie being significantly sadder ($t(92) = 6.38$, $p < .01$) and participants who watched the funny movie being significantly happier ($t(92) = -7.87$, $p < .01$) than the respective other group. Experimental conditions did not differ in other control variables, such as age ($t(92) = -.01$, $p = .99$), driving experience ($t(85) = .70$, $p = .49$) or gender ($\chi^2(1, N = 94) = .11$, $p = .74$).

4.2 Measurement Model

Following the two step methodology suggested by Segars and Grover (1993), we first conducted a confirmatory factor analysis (CFA) to analyze the psychometric properties of the privacy-related scales. Applying guidelines by Gefen et al. (2000), the CFA was carried out with all items simultaneously, and factor loadings were estimated by Maximum likelihood algorithm in MPlus 6.12 (Muthén and Muthén, 2011). The overall model fit was good ($\chi^2 = 103.98$, $p = .23$; $RMSEA = .03$; $CFI = .99$). Thus, we proceeded by testing reliability, convergent and discriminant validity of the measurement model.

With regard to reliability, we inspected Cronbach’s Alpha and the Composite Reliability of the de ployed scales. As depicted in Table 1, all indices exceeded the recommended thresholds of .70 (Gefen et al., 2000), indicating good reliability of the measurement items. In a second step, we examined convergent validity by (1) analyzing the factor loadings and t-values for every single item used, and (2) calculating the average variance extracted (AVE) for every scale. Given that (1) t-values indicated every item to significantly load on the corresponding factor, and (2) AVEs met or exceeded the recommended threshold of .50 for every deployed scale (Fornell and Larcker, 1981), we concluded convergent validity to be largely supported by the data. With regard to discriminant validity, we proceeded by comparing AVEs to bivariate correlations between latent factors, analyzing whether the square roots of AVEs exceeded correlations between constructs and other constructs in the model (Fornell and Larcker, 1981). As illustrated in Table 2, this was the case for every single scale, indicating good discriminant validity. Thus, we concluded psychometric properties of the measurement model to suffice for further analysis, and retained all items for further steps in order to preserve content validity and theoretical consistency with prior research.

	RISK	**BEN**	**WILL**	**TRUST**	**CONC**	**t-value**	**R^2**	**CR**	**AVE**
Item	α = .89	α = .73	α = .87	α = .95	α = .88				
RISK1	.90					33.83	.81	.89	.68
RISK2	.86					26.69	.75		
RISK3	.85					24.23	.72		
RISK4	.66					10.29	.43		
BEN1		.79				11.93	.63	.74	.50
BEN2		.77				11.32	.59		
BEN3		.51				5.70	.26		
WILL1			.92			34.43	.85	.87	.73
WILL2			.87			27.05	.76		
WILL3			.69			11.73	.48		
TRUST1				.94		56.72	.88	.95	.84
TRUST2				.94		60.87	.89		
TRUST3				.89		37.06	.80		
TRUST4				.88		32.53	.77		
CONC1					.95	22.54	.91	.88	.80
CONC2					.82	16.77	.67		

Table 1. *Statistics of Confirmatory Factor Analysis. RISK = Perceived risks of information disclosure; BEN = Perceived benefits of information disclosure; WILL = Willingness to disclose private information; TRUST = General Institutional Trust; CONC = General Privacy Concerns; CR = Composite Reliability; AVE = Average Variance Extracted; α = Cronbach's Alpha. All t-values were significant with p < .01.*

	M	**SD**	**RISK**	**BEN**	**WILL**	**TRUST**	**CONC**
RISK	3.46	1.30	.82				
BEN	2.52	1.25	-.36	.70			
WILL	1.74	1.36	-.70	.50	.85		
TRUST	1.63	1.21	-.63	.47	.56	.91	
CONC	3.13	1.46	.60	-.29	-.58	-.49	.89

Table 2. *Descriptive Statistics, Bivariate Correlations and square roots of AVEs (Average Variances Extracted) of Latent Constructs. The diagonal terms indicate the square roots of AVEs, non-diagonal terms indicate correlations. M = Mean; SD = Standard Deviation; RISK = Perceived risks of information disclosure; BEN = Perceived benefits of information disclosure; WILL = Willingness to disclose private information; TRUST = General Institutional Trust; CONC = General Privacy Concerns. All bivariate correlations were significant with p < .01.*

4.3 Structural Equation Model

We proceeded by fitting the hypothesized structure model to the data. We included the experimental factor as an exogenous, categorical variable with the values zero representing the sad mood condition and one representing the joyful mood condition. Although applied rarely, dichotomous variables such as experimental conditions may be included in SEM the same way they can be included to regression analysis as so called dummy variables, allowing for simultaneous modeling of variable relationships and group differences (Muller et al., 2005). The overall model fit of the complete model covering mood effects and dispositional tendencies was good ($\chi^2 = 125.98$, $p = .14$; $RMSEA = .04$; $CFI = .99$). Furthermore, a large proportion of explained variance in the total model ($R^2 = .77$) suggested that (1) study design had covered some of the main predictors in privacy-related decision-making, and (2) empirical data mainly confirmed theoretical predictions on variable relationships.

As depicted in figure 2, there was empirical evidence for most of the hypothesized effects: The negative relationship found between perceived benefits and perceived risks (H1) resembled findings of earlier studies, although it had been found to be slightly higher in previous investigations (e.g. Dinev et al. (2012). Also, the conjoint valuation of perceived risks and perceived benefits in determining one's willingness to disclose private information (H2a and H2b) could be confirmed.With regard to H3a and H3b, (1) a positive relationship between general privacy concerns and perceived risks as well as (2) a negative relationship between privacy concerns and the willingness to disclose private information was found. As predicted, these effects indicated general privacy concerns may affect privacy decisions by both impacting risk considerations as well as intention forming in a decisive situation. In order to test the mediation effect predicted in H3c, we applied the delta method (MacKinnon et al., 2007), a more generalized approach than the Sobel test (Sobel, 1982). Results yielded a significant direct ($d_{direct} = -.21$, $p < .05$) as well as a highly significant indirect ($d_{indirect} = -.19$, $p < .01$) effect for the impact of general privacy concerns on the willingness to disclose information, resulting in a significant total effect ($d_{total} = -.40$, $p < .01$). As such, it could be assumed that situation-specific risk considerations partially mediated the relationship between general privacy concerns and the willingness to disclose private information, supporting hypothesis H3c.

On the benefit side of the situational privacy calculus, however, our data did only partially support the hypothesized relationships. Specifically, we found a significant relationship between general institutional trust and perceived benefits of information disclosure, supporting H4a, but not between general institutional trust and the willingness to disclose private information (H4b). Moreover, mediation analysis revealed a full mediation of the relationship between general institutional trust and the willingness to disclose private information through situation-specific benefit perceptions. That is, the delta method yielded a significant indirect ($d_{indirect} = .24$, $p < .01$) and total ($d_{total} = .24$, $p < .01$), but no significant direct effect ($d_{direct} = .00$, $p = .97$). Interestingly, variance proportions of institutional trust were not only carried through perceived benefits ($d_{indirect1} = .18$, $p < .01$), but also double-mediated through the path from institutional trust over perceived benefits *and* perceived risks to willingness to disclose information ($d_{indirect2} = .06$, $p < .05$). As such, our results imply that situational benefit perceptions may not only have the potential to partially, but even *fully* override general institutional trust in a decisive situation.

Finally, mood was found to significantly influence perceived risks (H5a), but not perceived benefits (H5c) in the situational privacy calculus. That is, while no direct relationship between an individual's current mood and situation-specific benefit perceptions were found, risk perceptions of participants in the happy mood condition were significantly lower than perceived risks of participants in the sad mood condition, implying joyful feelings lead to lowered risk perceptions. An exploratory mediation analysis also revealed risk perception to potentially mediate the effect between moods and the willingness to disclose private information, indicating that initial feelings may sustain in cognitive valuation processes without being overridden by other factors, such as privacy concerns. However, this effect was only found to be marginally significant in the current study ($d_{indirect} = .17$, $p = .08$). Also, we tested an alternative model with the mood variable excluded. Underlining the importance of an individual's current mood in shaping privacy perceptions, this alternative model showed substantially worse overall fit than the initial model (χ^2 = 117.49, *p* = .06; *RMSEA* = .05; *CFI* = .98).

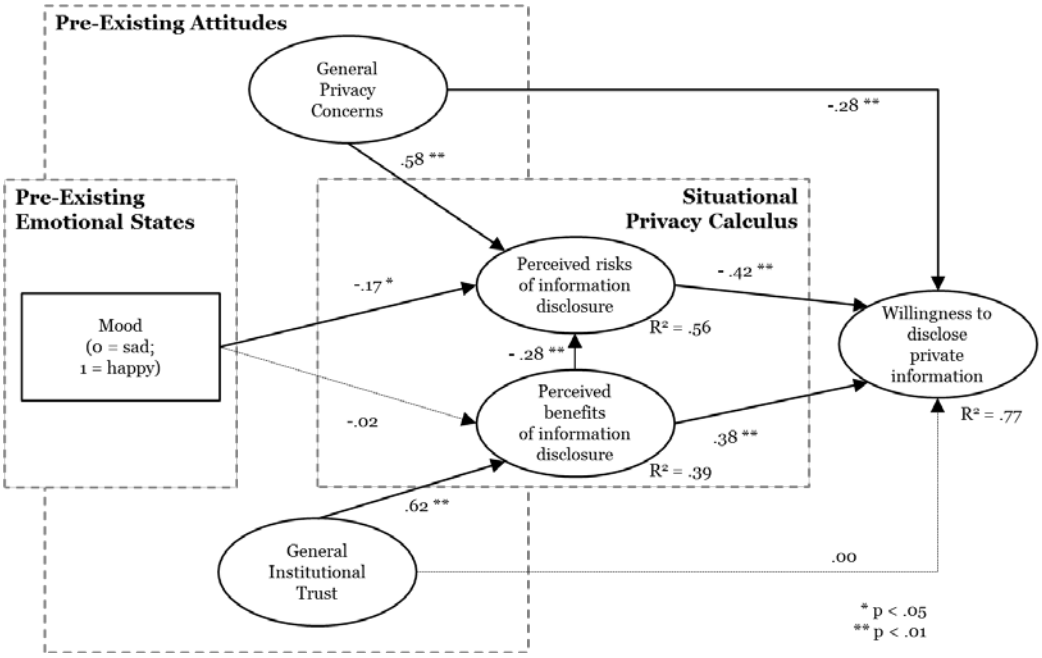
Pre-Existing Attitudes
General Privacy Concerns
-.28 **
.58 **
Pre-Existing Emotional States
Situational Privacy Calculus
-.17 *
Perceived risks of information disclosure
- .42 **
Willingness to disclose private information
Mood (0 = sad; 1 = happy)
R² = .56
- .28 **
Perceived benefits of information disclosure
-.02
R² = .77
.38 **
R² = .39
.62 **
General Institutional Trust
.00
* p < .05
** p < .01

Figure 2. Structural equation model with standardized path coefficients.

5 Discussion

Aiming to address a systematic distinction between pre-existing and situational factors in privacy-related decision-making, the current study introduced a model that rigorously distinguished between (1) pre-existing attitudes, namely general privacy concerns and general institutional trust, (2) pre-existing emotional states, namely an individual’s current mood, and (3) situation-specific privacy considerations. The results of an experimental study largely supported the hypothesized relationships, yielding evidence on the validity of a distinction between situation-specific privacy considerations and pre-existing factors. In particular, we found the impact of pre-existing attitudes on the willingness to disclose private information to be partially or even fully mediated by situational variables, indicating situation-specific privacy considerations may be capable to override superordinate variables. Moreover, we found privacy-related risk perceptions in a given situation to be biased by an individual’s current mood, with positive mood leading to lower risk perceptions than negative mood.

5.1 Theoretical and Practical Implications

Although several studies have proposed and discussed a systematic distinction between pre-existing factors and a situational privacy calculus (Kehr et al., 2013; Li et al., 2011; Wilson and Valacich, 2012), few attempts have been made to empirically validate these assumptions. In particular and to the knowledge of the authors, only three prior studies (Kehr et al., in press; Keith et al., 2013; Li et al., 2011) used a distinct framework to explore the role of general privacy concerns in shaping situation-specific decisions, yielding concordant results on the potential of situational variables to partially (Keith et al., 2013; Li et al., 2011) or even fully (Kehr et al., in press) override pre-existing worries. In this regard, our work constitutes an important addition to these findings by supporting the general notion of a distinct privacy decision framework, in which privacy concerns constitute an important antecedent, but not necessarily a key driver to privacy decisions in a certain situation. This view, essentially, expands prior work which typically investigated privacy concerns as a situation-specific construct (Anderson and Agarwal, 2011; Dinev and Hart, 2006), while simultaneously emphasizing the contextual and situated nature of privacy decisions (Smith et al., 2011). In this regard, moreover, our work has made two important additions that could help scholars to explore privacy-related decisions from a more differentiated angle:

First, we have explored the role of general institutional trust as a second pre-existing attitude, and showed its potential to drive situation-specific privacy considerations likewise general privacy concerns. Although a small stream of literature has proposed such a conceptualization of trust beliefs (Kehr et al., in press; Kehr et al., 2013), trust has been mostly conceptualized inconsistently in prior literature (Kehr et al., in press; Kehr et al., 2013; Smith et al., 2011), e.g. as an antecedent (Wakefield, 2013) or outcome of privacy concerns (Bansal et al., 2010). As such, our work essentially adds to the understanding of the dynamic relationships among constructs in driving privacy decisions in a certain situation. Specifically, we found situation-specific risk and benefit perceptions to be capable to even fully override prior trust beliefs, emphasizing the conceptual and empirical distinction between general institutional trust and situation-specific privacy decisions.

Second, we have introduced pre-existing emotional states, in particular an individual's current mood, to information privacy research. Although the notion of feelings and emotions as drivers to privacy decisions is not new per se (Kehr et al., 2013; Li et al., 2011; Wakefield, 2013), our work differs from prior studies in two important ways: First, we explored the role of emotions as pre-existing factors, i.e. as states that were induced before the actual decisive situation occurred. Second, we demonstrated that such emotional states may impact situation-specific privacy considerations even if the sources of these states are completely independent from privacy or technology-related topics. That is, we showed that a mood induction procedure using unrelated film material was effective in driving individuals to perceive lowered risk if in a happy mood, and potentially biasing their privacy decisions towards disclosure. Referring to (1) the large number of studies showing such mood-congruency effects in different contexts (e.g. Forgas, 1991; Johnson and Tversky, 1983; Redelmeier and Baxter, 2009), and (2) the definition of moods as weak, yet enduring emotional states (George, 1989), it becomes likely to assume that individuals (1) may be impacted by their current mood when taking privacy decisions in their everyday life, and that (2) the influence of mood states may persist over a set of consecutive privacy-related decisions. As such, our results may contribute to the emerging stream of literature that highlights cognitive restrictions and boundaries to rational decision-making in a privacy context (Acquisti, 2009; Acquisti et al., 2012; Kehr et al., 2013).

As a whole, our research has argued for a more differentiated view on privacy decision-making as a cognitive process situated in a certain context, yet impacted by several pre-existing, superordinate variables. As such, our results may substantially contribute to the understanding of the privacy paradox as a gap between pre-existing factors and situation-specific considerations (Kehr et al., 2013; Li et al., 2011). More precisely, our work has outlined two potential dynamics that could promote its emergence when individuals are confronted with a privacy decision: First, situation-specific considerations may partially or even fully override pre-existing attitudes, leading individuals to neglect their preferences and principles if aspects of the current situation seem, for any reason, attractive and worthwhile. Second, the valuation of a situation, in particular the anticipation of privacy-related risks, may depend on prior emotional experiences that are unrelated to the decision at hand, such as a happy or sad mood.

For managers and policymakers, our insights may have important implications, too. Specifically, the results of our study may help firms to deepen their understanding on when and why individuals disclose their private information, and which preconditions seem essential in this process. In contrast to many other studies that highlighted the importance of procedures that help to mitigate privacy concerns, such as privacy seals or notices (e.g. Hui et al., 2007; Kim et al., 2008; Larose and Rifon, 2007), our approach emphasizes the role of right-in-time actions that may help individuals to classify privacy-related risks and privacy-related benefits just as data is requested in a particular moment. Stated differently, ensuring privacy protection for a whole website or service may be helpful to increase trust and mitigate privacy concerns on a general level. However, it may not ensure individuals behave accordingly when requested to disclose private information while browsing the website or using the service. In these situations, in contrast, other pre-existing states, such as one's current mood, may be of higher importance. Given that information systems also have the potential to manipulate individual emotions (Kehr et al., in press; Kramer et al., 2014), however, our results also indicate that policymakers should carefully consider the role of emotional states when designing actions that aim to protect consumers' privacy.

5.2 Limitations

Although our conceptual model was largely supported by the empirical data and analysis, several limitations in this study apply, opening an avenue for future research endeavors.

First, we relied on a student sample in data acquisition and examination, with a high percentage of female participants. Although such sample compounds are widely accepted in behavioral science, resorting on students may raise methodological limitations with regard to the generalization of the obtained results. In particular, the comparably young age of the participants in the current study may restrict generalizability to a whole population, given that younger individuals are known to hold specific attitudes on privacy-related topics (Youn, 2009), but also show specific behavioral patterns in contact with information technology (Vodanovich et al., 2010). Apart from sample structure, the size of the sample was relatively small, and residing at the lower end of minimal sample sizes recommended for structure equation modeling (Gefen et al., 2000). As such, our results should be interpreted as a preliminary investigation of the dynamics of pre-existing factors and situational privacy decisions, and more research is needed to validate and extend these findings.

Second, despite the fact that all recommended thresholds for reliability and validity examination were met or exceeded, the measurement model showed inconsistencies worth further investigation. In particular, some items showed comparably small loadings on their correspondent factors (RISK4 and BEN3), which indicates that items did not properly reflect underlying latent variables. A possible explanation to this validity-restricting issue concerns the translation procedure: While we attempted to assure semantic equivalence between languages by validating item translations by an English native speaker, validated and standardized multilingual measurement instruments are still scarce in information privacy research. As such, the psychometric properties of some of the deployed items may have been flawed by improper translation. Besides, bivariate correlations between scales were notably high, especially between situational privacy calculus variables. Apart from methodological implications, such as lowered discriminant validity between constructs, this result may also reflect individuals' restricted capabilities to properly distinguish between privacy-related risks, benefits, and disclosure intentions. This view is in line with recent findings (including our own) on the negative correlation between privacy-related risks and benefits (e.g. Dinev et al., 2012), but also with recent findings that emphasize the tendency of certain individuals to skip or overleap a privacy calculus when taking privacy decisions (Kehr et al., in press).

Third, likewise many other studies in the field (Smith et al., 2011), we relied on disclosing intentions rather than actual disclosure as a main outcome variable. Given that intention-behavior gaps occur in many fields of behavior (Ajzen, 1985), therefore, reinvestigating the obtained results in a more realistic scenario while measuring actual disclosing behavior of individuals may substantially enhance our understanding on when, why and how individuals disclose private information.

6 Conclusion

Introducing a systematic distinction between pre-existing factors and a situational privacy calculus, our studies revealed evidence on the dynamics of (1) pre-existing attitudes and (2) pre-existing emotional states in determining privacy-related decisions in a concrete situation. As such, our study may substantially add to the ongoing debate on the sources of the privacy paradox by highlighting the situated and contextual nature of privacy decisions, and provides a suitable framework for future privacy investigations.

References

Acquisti, A. (2009). "Nudging Privacy the Behavioral Economics of Personal Information." *Ieee Security & Privacy*, 7 (6), 82-85.

Acquisti, A., L.K. John and G. Loewenstein (2012). "The Impact of Relative Standards on the Propensity to Disclose." *Journal of Marketing Research*, 49 (2), 160-174.

Ajzen, I. (1985). *From Intentions to Actions: A Theory of Planned Behavior*. Berlin: Springer.

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.

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.

Bansal, G., F.M. 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.

Belanger, F. and R.E. Crossler (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly*, 35 (4), 1017-1041.

Brandimarte, L., A. Acquisti and G. Loewenstein (2013). "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science*, 4 (3), 340-347.

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.

Dinev, T. and P. Hart (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research*, 17 (1), 61-80.

Dinev, T., H. Xu, J.H. Smith and P. Hart (2012). "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts." *European Journal of Information Systems*, 22 (3), 61-80.

Forgas, J.P. (1991). "Mood Effects on Partner Choice: Role of Affect in Social Decisions." *Journal of Personality and Social Psychology*, 61, 708-720.

Forgas, J.P. (1995). "Mood and Judgment: The Affect Infusion Model (Aim)." *Psychological Bulletin*, 117 (1), 39-66.

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.

Gefen, D., D.W. Straub and M.C. Boudreau (2000). "Structural Equation Modeling and Regression: Guidelines for Research Practice." *Communications of the Association for Information Systems* (4).

George, J.M. (1989). "Mood and Absence." *Journal of Applied Psychology*, 74 (2), 317-324.

Gross, J.J. and R.W. Levenson (1995). "Emotion Elicitation Using Films." *Cognition & Emotion*, 9 (1), 87-108.

Hewig, J., D. Hagemann, J. Seifert, M. Gollwitzer, E. Naumann and D. Bartussek (2005). "A Revised Film Set for the Induction of Basic Emotions." *Cognition & Emotion*, 19 (7), 1095-1109.

Hirshleifer, D. and T. Shumway (2003). "Good Day Sunshine: Stock Returns and the Weather." *The Journal of Finance*, 58 (3), 1009-1032.

Hui, K.L., H.H. Teo and S.Y.T. Lee (2007). "The Value of Privacy Assurance: An Exploratory Field Experiment." *Mis Quarterly*, 31 (1), 19-33.

John, L.K., A. Acquisti and G. Loewenstein (2011). "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information." *The Journal of Consumer Research*, 37 (5), 858-873.

Johnson, E.J. and A. Tversky (1983). "Affect, Generalization, and the Perception of Risk." *Journal of personality and social psychology*, 45 (1), 20.

Kehr, F., T. Kowatsch, D. Wentzel and E. Fleisch (in press). "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus." *Information Systems Journal Special Issue on: Reframing Privacy in a Networked World*.

Kehr, F., D. Wentzel and P. Mayer Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect. Proceedings of the 34th International Conference on Information Systems (ICIS 2013), Milan, Italy, 2013.

Keith, M.J., S.C. Thompson, J. Hale, P.B. Lowry and C. Greer (2013). "Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior." *International Journal of Human-Computer Studies*, 71 (12), 1163-1173.

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.Y. and R. Kanfer (2009). "The Joint Influence of Mood and a Cognitively Demanding Task on Risk-Taking." *Motivation and Emotion*, 33 (4), 362-372.

Kim, Y.J., J. Park and R.S. Wyer (2009). "Effects of Temporal Distance and Memory on Consumer Judgments." *Journal of Consumer Research*, 36 (4), 634-645.

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*.

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

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, T., P.A. Pavlou and G.L. Dos Santos What Drives Users' Website Registration? A Randomized Field Experiment. 34th International Conference on Information Systems, Milan, 2013.

Mackinnon, D.P., A.J. Fairchild and M.S. Fritz (2007). "Mediation Analysis." *Annu Rev Psychol*, 58, 593-614.

Malhotra, N.K., S.S. Kim and J. Agarwal (2004). "Internet Users' Information Privacy Concerns (Iuipc): Tthe Construct, the Scale, and a Causal Model." *Information Systems Research*, 15 (4), 336-355.

Muller, D., C.M. Judd and V.Y. Yzerbyt (2005). "When Moderation Is Mediated and Mediation Is Moderated." *Journal of personality and social psychology*, 89 (6), 852.

Muthén, L.K. and B.O. Muthén (2011) Mplus. In Proceedings of the *Statistical analysis with latent variables. Version*.

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.

Pavlou, P.A. and D. Gefen (2004). "Building Effective Online Marketplaces with Institution-Based Trust." *Information Systems Research*, 15 (1), 37-59.

Redelmeier, D.A. and S.D. Baxter (2009). "Holiday Review. Rainy Weather and Medical School Admission Interviews." *CMAJ*, 181 (12), 933.

Röcke, C. and D. Grühn (2003). "German Translation of the Panas-X." *Unpublished manuscript, Free University Berlin*.

Schwarz, N. (2011). "Feelings-as-Information Theory." In: *Handbook of Theories of Social Psychology*, P. Van Lange, A.W. Kruglanski and E.T. Higgins (eds.), London: Sage Publications Ltd., 289-308.

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.

Schwarz, N. and G.L. Clore (1988). "How Do I Feel About It? The Informative Function of Affective States." *Affect, cognition, and social behavior*, 44-62.

Schwarz, N., F. Strack, D. Kommer and D. Wagner (1987). "Soccer, Rooms, and the Quality of Your Life: Mood Effects on Judgments of Satisfaction with Life in General and with Specific Domains." *European Journal of Social Psychology*, 17 (1), 69-79.

Segars, A.H. and V. Grover (1993). "Re-Examining Perceived Ease of Use and Usefulness." *MIS quarterly*, 17 (4), 517-525.

Smith, H.J., T. Dinev and H. Xu (2011). "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly*, 35 (4), 989-1015.

Sobel, M.E. (1982). "Asymptotic Confidence Intervals for Indirect Effects in Structural Equation Models." *Sociological methodology*, 13 (1982), 290-312.

Spiekermann, S., J. Grossklags and B. Berendt (2001). "Stated Privacy Preferences Versus Actual Behaviour in Ec Environments: A Reality Check." *Proceedings of Wirtschaftsinformatik*.

Sutanto, J., E. Palme, C.-H. Tan and C.W. Phang (2013). "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users." *MIS Quarterly*, 37 (4), 1141-1164.

Vodanovich, S., D. Sundaram and M. Myers (2010). "Digital Natives and Ubiquitous Information Systems." *Information Systems Research*, 21 (4), 711-723.

Wakefield, R. (2013). "The Influence of User Affect in Online Information Disclosure." *Journal of Strategic Information Systems*, 22 (2), 157-174.

Watson, D., L.A. Clark and A. Tellegen (1988). "Development and Validation of Brief Measures of Positive and Negative Affect - the Panas Scales." *Journal of Personality and Social Psychology*, 54 (6), 1063-1070.

Wilson, D. and J. Valacich (2012). "Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus." *Proceedings of the 33rd International Conference on Information Systems, Orlando.*

Xu, H., X. 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.

Xu, H., H.H. Teo, B.C.Y. Tan and R. Agarwal (2009). "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." *Journal of Management Information Systems*, 26 (3), 135-173.

Youn, S. (2009). "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents." *Journal of Consumer Affairs*, 43 (3), 389-418.

Yuen, K.S.L. and T.M.C. Lee (2003). "Could Mood State Affect Risk-Taking Decisions?" *Journal of Affective Disorders*, 75 (1), 11-18.