doi: 10.1111/isj.12062

Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus

Flavius Kehr,* Tobias Kowatsch,* Daniel Wentzel† & Elgar Fleisch*,‡

*Institute of Technology Management, University of St. Gallen, St. Gallen, Switzerland, e-mail: flavius.kehr@unisg.ch; tobias.kowatsch@unisg.ch; wentzel@time.rwth-aachen.de; elgar.fleisch@unisg.ch, †Chair of Marketing, TIME Research Area, RWTH Aachen University, Aachen, Germany, and ‡Department of Management, Technology and Economics, ETH Zurich, Zurich, Switzerland

Abstract. *Existing research on information privacy has mostly relied on the privacy calculus model, which views privacy-related decision-making as a rational process where individuals weigh the anticipated risks of disclosing personal data against the potential benefits. In this research, we develop an extension to the privacy calculus model, arguing that the situation-specific assessment of risks and benefits is bounded by (1) pre-existing attitudes or dispositions, such as general privacy concerns or general institutional trust, and (2) limited cognitive resources and heuristic thinking. An experimental study, employing two samples from the USA and Switzerland, examined consumer responses to a new smartphone application that collects driving behavior data and provided converging support for these predictions. Specifically, the results revealed that a situation-specific assessment of risks and benefits fully mediates the effect of dispositional factors on information disclosure. In addition, the results showed that privacy assessment is influenced by momentary affective states, indicating that consumers underestimate the risks of information disclosure when confronted with a user interface that elicits positive affect.*

Keywords: privacy/information privacy, privacy calculus, privacy paradox, affect heuristic, rational/irrational behavior

INTRODUCTION

Rooted in an understanding of privacy as a commodity, i.e. an economic good that can be traded for other goods or services (Smith *et al*., 2011), prior research has predominantly regarded privacy-related decision-making as a rational process guided by an internal cognitive assessment of (1) the anticipated costs (or risks) and (2) the perceived benefits connected to the provision of personal data (Culnan & Armstrong, 1999; Dinev & Hart, 2006). That is, users are supposed to undertake an anticipatory, rational weighting of risks and benefits when

© 2015 Wiley Publishing Ltd

confronted with the decision to disclose personal information (Malhotra *et al*., 2004; Xu *et al*., 2009) or conduct transactions (Pavlou and Gefen 2004). Entitled the *privacy calculus* (Culnan & Armstrong, 1999), this privacy trade-off has been extensively researched in several contexts, such as e-commerce (Dinev & Hart, 2006), the Internet (Malhotra *et al*., 2004; Dinev *et al*., 2012) or mobile applications (Xu *et al*., 2009). Furthermore, numerous factors increasing or mitigating risk and benefit perceptions have been identified, e.g. financial rewards (Xu *et al*., 2011b), personalization (Xu *et al*., 2011b) or sensitivity of information to disclose (Li *et al*., 2011; Malhotra *et al*., 2004). However, researchers have recently challenged two basic propositions of the privacy calculus model.

First, current research has proposed a distinction between pre-existing attitudes, or dispositional tendencies, and situation-specific privacy constructs, arguing that (1) privacy concerns have been mostly measured on a global level, and (2) that situation-specific considerations may override general attitudes and tendencies (Li *et al*., 2011; Wilson & Valacich, 2012; Keith *et al*., 2013). That is, an individual who generally doubts the proper use of personal data by information systems may be persuaded to overcome his or her skepticism in a concrete situation and may provide personal data in exchange for saving of time and money, self-enhancements or pleasure (Hui *et al*., 2006).

Second, a growing body of literature argues that rational considerations concerning the privacy calculus may be bounded by psychological limitations, such as the inability to process all information relevant to the cost-benefit-ratio (Acquisti & Grossklags, 2005; Acquisti *et al*., 2009), intertemporal choice (Keith *et al*., 2012) or the attempt for immediate gratification (Acquisti, 2004; Wilson & Valacich, 2012). Embracing both propositions as valid extensions to the basic model, we define the privacy calculus as a *situation-specific* trade-off of privacy-related risk and benefit perceptions, *bounded* by dispositional factors and irrational behavior. In the current work, we will address these constraints by (1) conceptualizing privacy concerns and institutional trust as dispositional factors impacting a situational privacy calculus, and (2) assessing the impact of irrational thinking in situation-specific privacy assessment. More precisely, we will adopt an established approach from consumer behavior research, namely the affect heuristic (Finucane *et al*., 2000; Slovic *et al*., 2007), and will analyze its importance in the context of information privacy. As such, our work offers a first attempt to clarify the interplay of irrational, situation-specific behavior and dispositional factors in privacy-related decision-making.

In the following, we will review pertinent research streams and develop our research model. Then, we will describe the experimental approach and context chosen to empirically test our model, and report our findings. The paper concludes with a discussion on the results, implications and limitations of our study.

CONCEPTUAL MODEL AND HYPOTHESES

Depicted in Figure 1, our conceptual model proposes (1) the intention to disclose personal information to result from a conjoint assessment of perceived risks and benefits, (2) perceived privacy to conceptually reflect this cumulated assessment, (3) assessment in a concrete

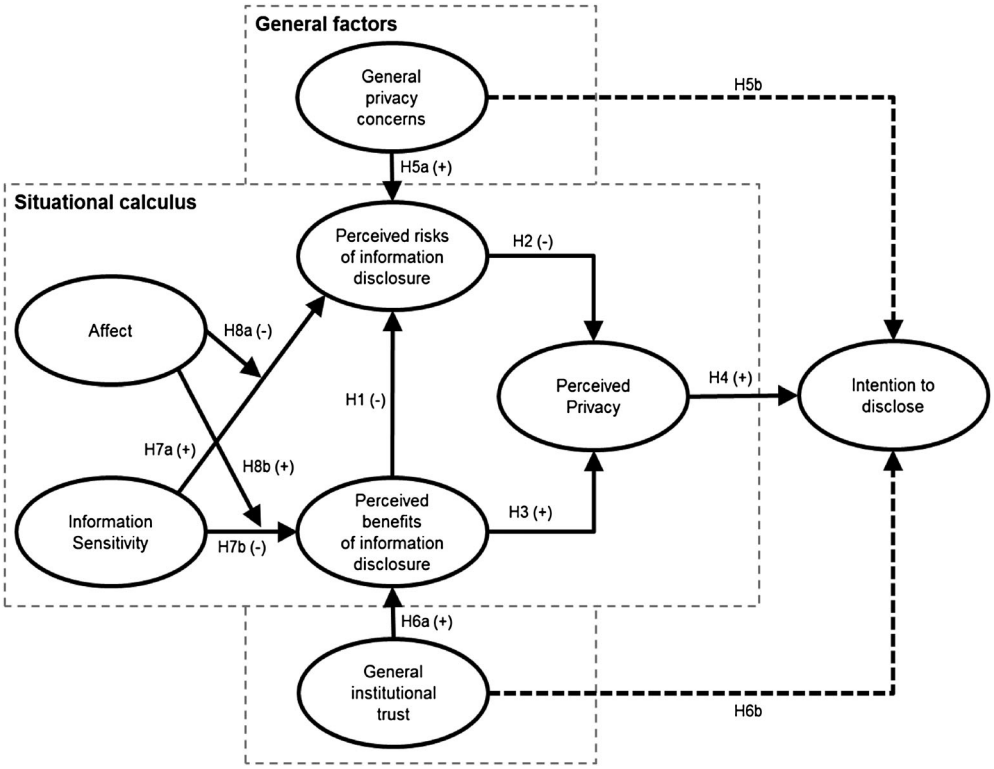

Figure 1. Conceptual model.

situation to potentially override dispositional factors, such as general privacy concerns and general institutional trust, and (4) positive affect to constitute a source of biased risk and benefit valuation in a situational privacy calculus. Rationales for these assumptions are provided in the succeeding sections.

A situational privacy calculus

According to the privacy calculus literature (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Anderson & Agarwal, 2011), individuals' disclosing intentions and behaviors result from an anticipatory, joint assessment of perceived risks and perceived benefits connected to the disclosure of private information. While many previous studies regarded perceived risks and benefits as independent (e.g. Dinev & Hart, 2006; Xu *et al*., 2009; Li *et al*., 2011), recent research suggests that risk and benefit perceptions are interdependent, with perceived risks mediating the relationship between privacy calculus antecedents and privacy calculus outcomes (Dinev *et al*., 2012; Knijnenburg *et al*., 2013). This view is in line with findings from consumer behavior research, repeatedly reporting that individuals tend to think that risks and benefits correlate negatively even though they often correlate positively in reality (Alhakami & Slovic, 1994; Siegrist *et al*., 2000; Fischhoff *et al*., 1978). For instance, nuclear power may be

both highly risky and highly beneficial in reality. Individuals, however, tend to think of nuclear power as highly risky and, *thus*, allocate only *few* benefits. Consequently, we conceptualize perceived risks and benefits to be interdependent, and hypothesize:

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

While many previous studies assumed risk and benefit perceptions to cumulate in an overall assessment of the data-requesting situation (Culnan & Bies, 2003; Dinev & Hart, 2006; Anderson & Agarwal, 2011), most studies have modeled risk and benefit perceptions to directly impact disclosing behaviors, and few attempts have been made to explicitly address the implicit assumption of a joint mental outcome of the risk-benefit ratio. As one of the few exceptions, Dinev *et al*. (2012) proposed privacy-related cognitive considerations to cumulate in an overall *state* of privacy, or *perceived privacy*. That is, individuals are expected to value their level of secrecy and protection at a specific point in time by developing an overall impression of their own privacy in this exact situation. Given our definition of the privacy calculus as a *situation-specific* risk-benefit trade-off, it becomes feasible to assume that the cumulated assessment of situational risk and benefit perceptions results in such a situation-specific state of overall privacy. In line with Dinev *et al*. (2012), we hence predict perceived privacy to be associated with perceived risks and perceived benefits, and hypothesize perceived privacy to antecede individuals' intention to disclose information:

H2: Perceived risks of information disclosure will be negatively associated with perceived privacy.

H3: Perceived benefits of information disclosure will be positively associated with perceived privacy.

H4: Perceived privacy will be positively associated with the intention to disclose information.

Dispositional factors: privacy concerns and institutional trust

As discussed earlier, most prior studies have focused on *general* privacy concerns – an 'individual's general tendency to worry about information privacy' (Li *et al*., 2011, p. 5). However, situation-specific factors may override dispositional factors and persuade individuals to disclose their information despite general worries (Li *et al*., 2011; Wilson & Valacich, 2012; Keith *et al*., 2013). We account for this distinction by modeling general privacy concerns as an antecedent to a situation-specific risk assessment. Because of the large deviations of stated privacy concerns and measured (intentions) to disclose private information (Norberg *et al*., 2007; Xu *et al*., 2011b), we assume that situation-specific risk assessment will fully mediate the negative association between general privacy concerns and the intention to disclose information.

H5a: General privacy concerns will be positively associated with perceived risks of information disclosure.

H5b: The effect of general privacy concerns on intention to disclose will be fully mediated by perceived risks of information disclosure and perceived privacy.

Based on this conceptual distinction, one may further postulate that there are additional dispositional factors that shape privacy assessments in a similar vein as general privacy concerns. Institutional trust, for example, refers to an individual's confidence that the data-requesting medium will not misuse his or her data (Dinev & Hart, 2006; Bansal *et al*., 2010; Anderson & Agarwal, 2011) and has been found to be related to privacy concerns (Bansal *et al*., 2010), risk beliefs (Malhotra *et al*., 2004) and intentions to disclose information (Dinev & Hart, 2006). However, the exact role of trust in information privacy is still unclear because the relationship between these constructs has not been modeled consistently in the literature (Smith *et al*., 2011). While some authors have conceptualized trust as an antecedent (Wakefield, 2013) or as an outcome of privacy concerns (Bansal *et al*., 2010), others have argued that trust and privacy concerns are independent factors that may exert separate influences on intentions to disclose information (Dinev & Hart, 2006; Anderson & Agarwal, 2011).

Yet, most studies have measured institutional trust in *general* terms, referring to the degree of general confidence in the Internet (Dinev & Hart, 2006) or the data-collecting website or service (Krasnova *et al*., 2012). Similar to general privacy concerns, institutional trust may thus constitute a *general* tendency to have confidence in the data-collecting medium (or institution), subject to interference by a situation-specific privacy calculus.

Because prior research suggests that trust is a protective factor that mitigates risk beliefs and privacy concerns (Malhotra *et al*., 2004; Kim *et al*., 2008; Bansal *et al*., 2010), we assume that institutional trust affects the benefit side of the situation-specific privacy calculus. In accordance with the previous hypothesis, we assume perceived benefits of information disclosure and perceived privacy to fully mediate the relationship between institutional trust and intentions to disclose.

H6a: General institutional trust will be positively associated with perceived benefits of information disclosure.

H6b: The effect of general institutional trust on intention to disclose will be fully mediated by perceived benefits of information disclosure and perceived privacy.

Situational factors and irrationality: information sensitivity and affect

As outlined earlier, prior research has identified numerous factors that may determine the joint assessment of perceived risks and perceived benefits of information disclosure. Sensitive information, for example, deserves more protection, and potential for loss increases as information becomes more delicate (Smith *et al*., 2011, p. 1003). Perceived information sensitivity has been repeatedly identified as a crucial aspect of information disclosure, shaping beliefs of risk, trust and benefits (Malhotra *et al*., 2004; Li *et al*., 2011; Mothersbaugh *et al*., 2012). In line with this research, we conceptualize perceived sensitivity of information as an antecedent of risk and benefit

valuation that impacts cognitive assessment processes in a primarily *rational* way, i.e. higher information sensitivity will increase risk perceptions and decrease perceptions of benefits.

H7a: A higher perceived sensitivity of information will positively impact perceived risks of information disclosure.

H7b: A higher perceived sensitivity of information will negatively impact perceived benefits of information disclosure.

However, prior research has also argued that rational considerations in the context of privacy-related decision-making may be affected by psychological limitations and irrational behavior (Acquisti & Grossklags, 2005; Acquisti *et al*., 2009). Studies by Johnson *et al*. (2002) as well as Knijnenburg *et al*. (2013), for example, used default framing to provoke differential privacy decisions. Furthermore, Tsai *et al*. (2011), as well as Brandimarte *et al*. (2012), showed that the salience and immediacy of privacy-related constructs may affect decision-making, suggesting that 'gut' feelings may determine privacy decisions if salience is low and risks are distant in time or space.

As a possible explanation for these findings, several scholars (e.g. Acquisti, 2009; Smith *et al*., 2011; Wilson & Valacich, 2012) have discussed notions of *bounded rationality*: While rational decision-making implies comprehensive consideration and weighing of all possible choice alternatives and their potential consequences in the future, individuals' access to this information is often limited in reality (Simon, 1955; 1979). As a consequence, human decision-making processes are often guided by mental 'rules of thumb', or cognitive heuristics (Gigerenzer & Gaissmaier, 2011). For example, individuals rely on the most salient and available information rather than actively seeking for completeness (Pachur *et al*., 2012), or discontinue considering further choice alternatives as soon as an option is valued 'good enough' (Simon, 1955; Agosto, 2002). Building on these principles, research in consumer behavior has identified numerous principles that can be used to systematically guide human information processing and valuation and, thus, cause biased and irrational decisions (Decoster & Claypool, 2004).

In this regard, consumer behavior research has also noted that emotions and affective reactions[1] constitute an 'aid to bounded rationality' (Hanoch, 2002, p. 7). More precisely, affective reactions occur as a first, automatic and inevitable assessment of a stimulus (Zajonc, 1980), and may thus signalize its 'good' or 'bad' quality: 'We do not see just "a house": We see a *handsome* house, an *ugly* house, or a *pretentious house*' (Zajonc, 1980, p. 154). As a consequence, affect represents an important source of information for subsequent cognitive processes (Damasio, 1994; Epstein, 1994; Schwarz, 2011). Finucane *et al*. (2000), for example, showed affective reactions to mediate the spurious correlation between risk and benefit perceptions: High benefit perceptions increase positive feelings and lead to a lowered perception of risk, while high risk perceptions raise negative feelings, resulting in a lowered attribution of benefits. Stated differently, positive affect may cause individuals to overestimate benefits and underestimate risks (Finucane & Holup, 2006).

[1]Behavioral science differentiates between several states of affect and emotion (Fox, 2008). In this research, however, we refer to affect as 'a faint whisper of emotion' (Slovic *et al*., 2004, p. 312), and use the terms affect and emotion interchangeably.

Called the *affect heuristic* (Finucane *et al*., 2000; Slovic *et al*., 2007), the influential role of affective reactions on decision-making has been attributed to two co-existing and interacting processes of thinking: An affect-based mode and a rule-based mode. In affect-based mode, individuals tend to rapidly and subconsciously decide based on earlier experiences and related emotions. In contrast, individuals' decision-making relies on rationality, logical connections and conscious cognitive processing when in rule-based mode (e.g. Epstein, 1994; Loewenstein *et al*., 2001; Reyna, 2004; Finucane & Holup, 2006). As a consequence, affect-based thinking may result in biased and potentially irrational decisions. In a study by Hsee and Rottenstreich (2004, study 3), for example, consumers were asked to donate money for the salvation of either one or four panda bears. The pandas were represented either as cute pictures or sober black dots. When confronted with the affect-raising cute picture, consumers were willing to spend a medium amount of money, regardless of the count of pandas to save. In contrast, when representation of the pandas was more clinical, consumers' decisions depended on rational considerations – they decided to donate more if more pandas could be saved. Thus, affect may constrain rational decision-making, and contextual cues can determine whether individuals rely on affect-based or rule-based modes of thinking.

Despite these findings, emotions and affective reactions have played minor roles in research on information privacy (Nyshadham & Castano, 2012). Only recently, scholars have started to measure pre-existing emotional states and correlate them with constructs like intention to disclose information (Anderson & Agarwal, 2011), risk beliefs (Li *et al*., 2011), or trust (Pengnate & Antonenko, 2013; Wakefield, 2013). Although these studies generally support the idea that emotional states impact privacy-related decision making, there has been no attempt to experimentally manipulate affect in the context of privacy calculus research. As a result, there is a lack of knowledge on the interplay of emotional states with risk-enhancing or risk-mitigating factors such as information sensitivity (Wakefield, 2013). Addressing this gap, we postulate positive affect to result in a benefit overestimation and a risk underestimation (Slovic *et al*., 2007), and predict individuals' risks and benefit perceptions to be largely independent from rational considerations, such as the valuation of information sensitivity, when relying on affective thinking (Hsee & Rottenstreich, 2004, study 3):

H8a: The positive impact of a higher perceived sensitivity of information on perceived risks of information disclosure will be stronger if individuals feel neutral affect compared to positive affect.

H8b: The negative impact of a higher perceived sensitivity of information to disclose on perceived benefits of information disclosure will be stronger if individuals feel neutral affect compared to positive affect.

METHODOLOGY

Given that scholars (e.g. Anderson & Agarwal, 2011) revealed evidence on the influence of the data-requesting stakeholders on consumers' privacy concerns and the consequential privacy-

related decisions, we aimed to investigate the interplay of affective and rational thinking in a highly sensitive privacy context. Hence, we conducted our research as part of a requirements analysis for a smartphone application developed by an insurance firm, a stakeholder known to raise high concerns in consumers (Rohm & Milne, 2004).

We decided to focus on a mobile context for two reasons. First, developments in mobile technology increasingly allow firms to gather highly sensitive consumer information in an automated fashion, implying particularly high risks of data misuse (Mylonas *et al.*, 2013). Hence, examining individuals' privacy decisions in this context is of high relevance to theory and practice. Second, individuals may be particularly susceptible to manipulations of affect in the context of mobile applications. Deciding on whether to use a mobile application that collects personal data, for example, potential users typically need to rely on a verbal description, screenshots or user ratings only (Franko & Tirrell, 2012). Given this little opportunity to actually try the application before installing it on a personal device, the effects we were interested in seemed to be particularly likely to occur in a mobile context.

The application used in the study was designed to record and track driving behavior and to provide customized feedback on the own driving style in order to promote better and safer driving. For tracking purposes, the app may consider several types of data, including geolocation, velocity, travel date, time and distance as well as acceleration behavior, car type and driver characteristics. The study was conducted as a 2×2 cross-sectional online experiment. Manipulating information sensitivity and affect using product presentation scenarios, we aimed to measure privacy-related constructs by adopting scales from prior research.

Development of stimulus material

Because we focused on a new kind of application (i.e. driving behavior apps) in a particular context (i.e. insurance firms), we conducted a pre-study in order to develop stimulus materials for the affect and information sensitivity manipulations. For this purpose, we collected data from 61 English-speaking and 41 German-speaking individuals. In order to ensure accordance with the samples used in the main study, the vast majority of participants in the pre-study were US (56 out of 61) or Swiss (29 out of 41) citizens. Individuals were requested to rate a sequence of screenshots representing design alternatives of the upcoming application and a set of context-specific data types with regard to affective response and information sensitivity, respectively. In order to prevent sequence or priming effects, screenshots and data types were presented in random order.

Affect

As reported by prior research, affect-based thinking and decision-making can be induced by affect-rich cues such as pictures of cute panda bears (Hsee & Rottenstreich, 2004; study 3). Given prior research in ergonomics showing that aesthetically appealing screenshots have the potential to raise positive feelings in users (Sonderegger & Sauer, 2010; Sonderegger *et al*., 2012), we expected cute and appealing screenshots to be equally effective in our context. Therefore, we tested a set of potentially affect-raising screenshots by asking participants in the pre-study to rate their spontaneous affective reaction towards a respective screenshot on a 10-

point semantic differential consisting of three items adopted from Kim *et al*. (1996). Then, we compared the average ratings of every screenshot with a baseline measurement conducted at the beginning of the pre-study, and extracted the screenshot with the highest positive deviation as positive-affect ($t(101) = 6.00$, $p < 0.01$, mean difference: 1.47), and the screenshot with the lowest deviation from the baseline as the neutral-affect manipulation ($t(101) = 1.47$, $p = 0.14$, mean difference = -0.10). The derived stimulus material for raising positive and neutral affect is depicted in Figure 2.

Information sensitivity

To assess which kinds of personal information are considered more or less sensitive in the given context, we assessed information sensitivity for a set of context-specific data types (e.g. year of car construction, use of indicator light and violations of speed limit) on a 7-point Likert scale using one item adopted from Xie *et al*. (2006). Participants indicated to perceive information on their location ($M = 4.94$, standard deviation (SD) = 2.00), potential speed violations ($M = 4.84$, $SD = 2.14$) and the time of a trip ($M = 3.97$, $SD = 2.11$) as most sensitive. Hence, these three types served as the manipulation of high information sensitivity. In contrast, the pre-study indicated that information about the year of construction of the car ($M = 2.71$, $SD = 1.68$), the car type ($M = 3.11$, $SD = 1.71$) and the distance travelled ($M = 3.21$, $SD = 1.92$) were not considered as particularly sensitive pieces of information, and thus served as the manipulation of low information sensitivity. Significant differences were found between the averaged values of the three high sensitivity items ($M = 4.59$, $SD = 1.60$) and the averaged values of the three low sensitivity items ($M = 3.01$, $SD = 1.52$, $t(101) = 12.22$, $p < 0.01$).

Note: The original screenshots were colored.

Figure 2. Screenshots inducing (a) neutral affect and (b) positive affect.

Measures

To ensure construct validity, scales from previous studies were adapted wherever possible. Institutional trust and general privacy concerns were measured by three items each, adapted from Malhotra *et al*. (2004). Perceived risks were measured by four items, perceived benefits and perceived privacy by three items adapted from Dinev *et al*. (2012). These constructs were assessed on a 7-point Likert scale ranging from *totally disagree* (1) to *totally agree* (7). Intention to disclose was measured on a 7-point semantic differential using three items derived from Anderson & Agarwal (2011). Furthermore, we adopted three items from Kim *et al*. (1996) and one item used by Xie *et al*. (2006) for manipulation checks.

Participants and procedure

Being aware of cultural differences previously identified by information systems researchers (Dinev *et al*. 2006; Dinev *et al*. 2009; Krasnova *et al*. 2012), we strived to ensure cross-cultural validity of our findings by drawing on two samples with different cultural background. Hence, we recruited citizens from the USA via Amazon Mechanical Turk and cooperated with a market research company to recruit German-speaking participants from Switzerland. All participants received monetary compensation for their time and effort. In order to ensure equal comprehension of the study materials and instruments among all subjects, all materials were translated from English to German, and then re-translated and validated by an English native speaker.

After clicking on an invitation link, participants were requested to complete a short questionnaire focusing on dispositional factors and relevant control variables. General privacy concerns and general institutional trust were presented prior to the experimental manipulations in order to (1) emphasize their theoretical conceptualization as dispositional factors and (2) prevent priming effects that could have biased ratings if situational cues were presented first (Decoster & Claypool, 2004). Following this, participants were randomly assigned to one of four product presentation pages that introduced the context and basic idea of the driver behavior application. Depending on the experimental condition, participants were told that an optimal functionality of the application could only be achieved by gathering either lowly or highly sensitive information, while the product presentation was accompanied by an either neutral-affect or positive-affect screenshot. After viewing the application, participants responded to the dependent measures.

RESULTS

In total, 480 participants completed the study. In both subsamples, we eliminated cases that showed response patterns or implausible short handling times ($<$5 min), resulting in a total sample size of 414 participants (186 US citizens and 228 Swiss citizens). Mean age was 31.24 years (SD = 10.19) for US participants and 34.32 years (SD = 14.23) for Swiss participants ($t(405.52) = -2.56$, $p < 0.05$), with a larger proportion of males in the US sample (60% compared with 40% among Swiss participants, $\chi^2(1, N = 414) = 7.62$, $p < 0.01$). With regard to the privacy-related scales, the averaged means of American and Swiss participants did not differ in four of six cases. However, US participants indicated to have a higher general

Table 1. Descriptive statistics of the constructs

Construct	US sample (n = 186)		Swiss sample (n = 228)		Overall (n = 414)		t-value
	M	*SD*	*M*	*SD*	*M*	*SD*	
General Privacy Concerns	4.34	1.50	4.28	1.28	4.31	1.38	0.46
General Institutional Trust	3.68	1.23	3.26	1.23	3.45	1.25	3.43**
Perceived Risks	4.41	1.58	4.43	1.55	4.42	1.56	−0.13
Perceived Benefits	4.28	1.45	3.89	1.41	4.06	1.43	2.77**
Perceived Privacy	3.87	1.53	3.66	1.40	3.76	1.46	1.49
Intention to Disclose	3.74	1.90	3.83	1.65	3.79	1.76	−0.51

**$p < 0.01$

institutional trust ($t(412) = 3.43$, $p < 0.01$) and perceived higher benefits connected to data provision ($t(412) = 2.77$, $p < 0.01$). Table 1 shows the mean scores and *SD* of the deployed scales.

With regard to the manipulations, mean differences between experimental conditions showed that the manipulations were effective in both samples, with highly significant overall differences of sensitivity ratings between participants in the low and high sensitivity condition ($t(412) = -2.78$, $p < 0.01$) and highly significant overall differences of affect ratings between participants in the neutral and positive affect condition ($t(412) = -3.12$, $p < 0.01$).

Measurement model

For the main analysis, we used MPlus 6.12 (Muthén & Muthén, 2011), a covariance-based structure equation modeling tool. All model estimations were conducted using maximum likelihood estimation with robust standard errors to adjust the estimation for non-normality in the data. For identification purposes, we furthermore fixed latent means to 0 and latent variances to 1. Following the two-step methodology suggested by Segars & Grover (1993), we first conducted confirmatory factor analyses to analyse the psychometric properties of the privacy-related scales. We adhered to guidelines by Gefen *et al*. (2000) and Gefen *et al*. (2011) in all steps of data analysis and reporting.

Measurement invariance and overall model fit

Because of the cross-national nature of the overall sample, we started with measurement invariance[2] testing in order to ensure comparability of the samples from different populations. As suggested by many scholars (Steenkamp & Baumgartner, 1998; Vandenberg & Lance, 2000; Mackenzie *et al*., 2011), we investigated measurement invariance by comparing a set of increasingly restricted measurement models. Apart from the Root Mean Square Error of Approximation (RMSEA), the Comparative Fit Index (CFI) and the Tucker–Lewis Index (TLI), we used χ^2/degrees of freedom (df) as an indicator of overall model fit as the χ^2-test is known

[2]Generally, measurement invariance describes the equivalence of psychometric properties across groups, or over time. Obtained measurement invariance indicates that the same construct is measured the same way across groups and thus constitutes a necessary condition when aiming for group comparisons.

Table 2. Measurement invariance testing and model comparisons

	χ^2	*df*	χ^2/*df*	*CFI*	*TLI*	*RMSEA*	Comparison	SBS-χ^2 *(df)*	Decision
Model0	397.74	274	1.45	0.97	0.97	0.047	–	–	Accept
Model1	437.09	293	1.49	0.97	0.96	0.049	Model1 vs. Model0	43.26 (18) $p < 0.01$	Decline
Model1a	414.98	292	1.42	0.97	0.97	0.045	Model1a vs. Model0	15.16 (18) $p = 0.65$	Accept
Model2	509.54	311	1.64	0.96	0.95	0.056	Model2 vs. Model1a	55.89 (16) $p < 0.01$	Decline

df, degrees of freedom; CFI, Comparative Fit Index; TLI, Tucker–Lewis Index; RMSEA, Root Mean Square Error of Approximation; SBS-χ^2, Satorra–Bentler Scaled Chi-squared test.

to become more conservative as sample sizes increase. According to Carmines & McIver (1981), a value of χ^2/df of less than 3.0 indicates acceptable model fit. Model fit indices and comparative statistics for all models described in the following can be obtained in Table 2.

First, we conducted a multi-group comparison of the unconstrained measurement model (baseline model) in order to obtain insights on configural invariance. The tested model indicated a good fit of the model to the data, indicating that the hypothesized model structure fits the data well in both samples, and configural invariance could be established. Next, we tested for metric invariance by constraining factor loadings in the baseline model to be equal across groups (model1). In addition to the fit indices, we calculated a Satorra–Bentler scaled χ^2-test (SBS-χ^2, Satorra & Bentler, 2001)[3] to compare model 1 with the baseline model. Because the test was significant, full metric invariance could not be established. Therefore, we proceeded by investigating partial metric invariance. Prior research suggests that partial metric invariance is given if at least two factor loadings of every latent construct are constrained equal across groups (Byrne *et al*., 1989; Van De Schoot *et al*., 2012). As proposed by literature (Van De Schoot *et al*., 2012), partial metric invariance can be tested by freeing the unstandardized factor loadings of the indicator that shows the highest deviation across groups, which was the third indicator of general privacy concerns in our case ($\lambda = 0.90$ for the US sample and $\lambda = 0.47$ for the Swiss sample). As the SBS-χ^2 between this new model (model 1a) and model1 was insignificant, we concluded that partial metric invariance could be established.

Proceeding with a model constraining item intercepts to be the same across groups, we tested for scalar invariance (model2). Scalar invariance ensures the equivalence of latent mean scores, i.e. latent mean scores can be directly compared across groups when scalar invariance is given (Steenkamp & Baumgartner, 1998). In our case, however, scalar invariance could not be established because of a significant change in χ^2 between model1a and model2 as indicated by a significant SBS-χ^2. This corresponds to the results reported in Table 1, yielding differences in the ratings of two constructs across nations. Because, however, partial metric invariance suffices to 'compare the strength of relationships between constructs from one group to another' (Teo *et al*., 2009, p. 1002), we proceeded with multi-group comparisons, building on a measurement model with parameters fixed to the results of the measurement invariance analysis. That is, we used model1a as the most appropriate measurement model for further investigation.

[3]This test is used for model comparison testing of nested models using scaled χ^2s and is necessary when using estimation procedures with robust standard errors.
For more information, see http://www.statmodel.com/chidiff.shtml

Reliability, validity and common method variance

In the next step, we inspected reliability and validity coefficients of the measurement model. Results for the Swiss and US sample can be obtained in Table 3. With regard to reliability, we examined coefficients of composite reliability and Cronbach's α. Except for the general privacy concerns scale in the Swiss sample, yielding a Cronbach's α of 0.69, all scales exceeded the recommended thresholds of 0.70 for Cronbach's α and composite reliability (Gefen *et al*., 2000). Given that composite reliability constitutes a more rigorous approximation of internal consistency (Chin &` Gopal, 1995), results indicated a very good reliability of the measurement model in both samples.

Convergent validity of the measurement model was tested by two approaches: First, we analysed the factor loadings and *t*-values of all indicators. As illustrated in Table 3, all indicators showed highly significant *t*-values, and all indicators except for the third indicator of the general privacy concerns scale in the Swiss sample (λ = 0.47) exceeded factor loadings of 0.70. Second, we calculated the average variances extracted (AVEs) for each scale. Except for the general privacy concerns scale in the Swiss sample, yielding an AVE of 0.46, AVEs were above the recommended threshold of 0.50 (Fornell & Larcker, 1981) for all constructs, indicating that convergent validity was largely supported by the data. Because deviation from threshold values was low, we decided to proceed with an unmodified version of the general privacy concerns scale in the Swiss sample in order to keep measurement models consistent across samples.

Discriminant validity was assessed by analysing whether the square root of AVEs exceeded correlations between the corresponding construct and other constructs in the model in every single case (Fornell & Larcker, 1981). As illustrated in Table 4, this was the case for every single pair of latent constructs in both samples, indicating sufficient discriminant validity of the measurement model.

Moreover, we tested whether common method variance (CMV) would significantly impact the yielded measurement criteria. For this purpose, we estimated a model with an additional, unrelated latent common methods variance factor as proposed by Podsakoff *et al*. (2003). For model identification, we constrained the factor loadings on the common method factor to be equal inside each group. Comparing the two models, we concluded that CMV did not significantly impact our original model as (1) the CMV model did not show different overall fit to the data (χ^2 = 413.93, *df* = 290, χ^2/df=1.43, *CFI* = 0.97, *TLI* = 0.97, *RMSEA* = 0.045), (2) overall patterns of significant relationships between latent constructs for both samples remained stable in the CMV model, and (3) all item loadings of manifest indicators on the latent common method factor were small and non-significant (highest factor loadings were λ_{TRUST1} = 0.00, p = 0.92 in the US sample and λ_{TRUST1} = 0.16, p = 0.43 in the Swiss sample).

Structural model and hypothesis testing

In order to retain the final structural model, we included experimental condition variables. Furthermore, we included the direct effects of the dispositional factors on intention to disclose in order to prepare for mediation analysis. Estimation of the structural model yielded good

Table 3. Confirmatory factor analysis statistics

		US Sample									
Latent variable	Item	CONC α = 0.84	TRUST α = 0.82	RISK α = 0.91	BEN α = 0.84	PRIV α = 0.93	WILL α = 0.98	*t-value*	R^2	Composite reliability	AVE
CONC	CONC1	0.77						23.61	0.63	0.83	0.62
	CONC2	0.73						21.16	0.63		
	CONC3	0.88						25.39	0.60		
TRUST	TRUST1		0.79					19.76	0.60	0.84	0.64
	TRUST2		0.80					20.57	0.54		
	TRUST3		0.78					25.10	0.77		
RISK	RISK1			0.87				41.32	0.76	0.88	0.71
	RISK2			0.93				44.91	0.86		
	RISK3			0.77				26.32	0.59		
	RISK4			0.83				34.06	0.69		
BEN	BEN1				0.78			20.70	0.61	0.84	0.63
	BEN2				0.80			19.17	0.63		
	BEN3				0.81			17.47	0.65		
PRIV	PRIV1					0.89		38.41	0.79	0.92	0.80
	PRIV2					0.92		47.05	0.84		
	PRIV3					0.87		28.62	0.76		
INT	INT1						0.96	99.12	0.91	0.97	0.93
	INT2						0.97	108.41	0.94		
	INT3						0.97	102.07	0.94		

		Swiss Sample									
Latent variable	Item	CONC α = 0.69	TRUST α = 0.88	RISK α = 0.92	BEN α = 0.82	PRIV α = 0.90	WILL α = 0.96	*t-value*	R^2	Composite reliability	AVE
CONC	CONC1	0.76						19.19	0.58	0.71	0.46
	CONC2	0.76						18.79	0.58		
	CONC3	0.47						5.83	0.22		
TRUST	TRUST1		0.83					27.37	0.69	0.88	0.71
	TRUST2		0.82					18.75	0.67		
	TRUST3		0.88					37.77	0.77		
RISK	RISK1			0.88				40.81	0.77	0.88	0.72
	RISK2			0.90				47.11	0.82		
	RISK3			0.81				27.38	0.65		
	RISK4			0.82	–			32.98	0.68		
BEN	BEN1				0.80			24.71	0.63	0.82	0.61
	BEN2				0.78			21.55	0.61		
	BEN3				0.76			17.57	0.58		
PRIV	PRIV1					0.84		26.83	71	0.91	0.77
	PRIV2					0.92		54.42	0.84		
	PRIV3					0.88		32.41	0.77		
INT	INT1						0.95	59.93	90	0.97	0.91
	INT2						0.94	93.71	0.89		
	INT3						0.97	95.04	0.94		

TRUST, general institutional trust; CONC, general privacy concerns; RISKS, perceived risks of information disclosure; BEN, perceived benefits of information disclosure; PRIV, perceived privacy; INT, intention to disclose; α, Cronbach's alpha; AVE, Average variance extracted.

Table 4. Bivariate correlations of latent constructs and average variance extracted for each construct

			US sample			
	CONC	TRUST	RISK	BEN	PRIV	INT
CONC	0.64					
TRUST	−0.32** (0.09)	0.62				
RISK	0.47** (0.07)	−0.22* (0.09)	0.71			
BEN	−0.13 (0.10)	0.28** (0.10)	–0.50** (0.07)	0.63		
PRIV	−0.33** (0.07)	0.33** (0.08)	−0.75** (0.04)	0.68** (0.07)	0.80	
INT	−0.36** (0.06)	0.31** (0.07)	−0.65** (0.05)	0.62** (0.06)	0.71** (0.04)	0.93
			Swiss sample			
CONC	0.46					
TRUST	−0.07 (0.10)	0.71				
RISK	0.62** (0.07)	–0.31** (0.07)	0.72			
BEN	−0.38** (0.09)	0.45** (0.07)	−0.58** (0.07)	0.61		
PRIV	−0.45** (0.08)	0.51** (0.06)	−0.78** (0.03)	0.77** (0.05)	0.77	
INT	−0.36** (0.08)	0.27** (0.07)	−0.67** (0.05)	0.69** (0.06)	0.71** (0.05)	0.91

[†]The diagonal terms indicate the average variance extracted, non-diagonal terms indicate correlations and standard errors reported in parentheses.
TRUST, general institutional trust; CONC, general privacy concerns; RISKS, perceived risks of information disclosure; BEN, perceived benefits of information disclosure; PRIV, perceived privacy; INT: intention to disclose,
*$p < 0.05$ **$p < 0.01$.

model fit to the data (χ^2 = 585.50, *df* = 408, χ^2/df=1.44, *CFI* = 0.97, *TLI* = 0.96, *RMSEA* = 0.046), with mostly significant and highly comparable path coefficients and large coefficients of explained variance in both samples (Table 5).

Consistently across samples and as hypothesized, significant relationships were found between perceived risks and perceived benefits of information disclosure (H1), perceived risks and perceived privacy (H2), perceived benefits and perceived privacy (H3), perceived privacy and intention to disclose (H4), as well as general privacy concerns and perceived risks (H5a) and general institutional trust and perceived benefits (H6a). Furthermore, the model explained 50% of the variance of intention to disclose in the Swiss sample and even 58% in the US sample, indicating that predominant antecedents of the intention to disclose information had been covered.

Dispositional factors: privacy concerns and institutional trust

With regard to Hypotheses 5b and 6b, we have postulated full mediation of the relationship between dispositional factors and the intention to disclose by situational calculus constructs. In order to test these hypotheses, we employed two approaches:

First, we compared the complete structural model with a model without situational calculus variables. That is, we estimated an alternative model where general privacy concerns and general institutional trust directly impact the intention to disclose private information, while other variables were excluded. Such models have been proposed by several researchers in the privacy calculus literature (e.g. Anderson & Agarwal, 2011; Dinev & Hart, 2006; Li *et al.*, 2013). Although model estimation yielded significant impacts of concerns and trust on the intention to disclose in both samples (US sample: $\gamma_{concerns} = -0.34$, $p < 0.01$, $\gamma_{trust} = 0.27$, $p < 0.01$; Swiss sample: $\gamma_{concerns} = -0.31$, $p < 0.01$, $\gamma_{trust} = 0.22$, $p < 0.01$), all path coefficients were lower than the path

Table 5. Path coefficients and coefficients of explained variance for the structural model

		US sample		Swiss sample	
		Path coefficient	R^2	Path coefficient	R^2
H1	BEN ➜ RISK	−0.50*** (0.07)	–	−0.44*** (0.08)	–
H2	RISK ➜ PRIV	−0.56*** (0.08)	–	−0.50*** (0.06)	–
H3	BEN ➜ PRIV	0.46*** (0.09)	–	0.51*** (0.06)	–
H4	PRIV ➜ INT	0.70*** (0.05)	–	0.72*** (0.05)	–
H5a	CONC➜ RISK	0.44*** (0.07)	–	0.50*** (0.07)	–
H5b	CONC➜ INT	−0.13* (0.07)	–	−0.04 (0.07)	–
H6a	TRUST➜ BEN	0.34*** (0.09)	–	0.47*** (0.06)	–
H6b	TRUST ➜ INT	0.07 (0.07)	–	−0.08 (0.07)	–
H7a	SENS ➜ RISK	0.20** (0.10)	–	0.15* (0.08)	–
	AFF ➜ RISK	0.07 (0.10)	–	0.20*** (0.08)	–
H8a	AFFxSENS ➜ RISK	−0.24** (0.11)	–	−0.20** (0.10)	–
H7b	SENS ➜ BEN	−0.24** (0.11)	–	−0.05 (0.09)	–
	AFF ➜ BEN	−0.19 (0.11)	–	−0.03 (0.09)	–
H8b	AFFxSENS ➜ BEN	0.02 (0.15)	–	0.02 (0.11)	–
	RISK	–	0.48*** (0.06)	–	0.47*** (0.06)
	BEN	–	0.19*** (0.07)	–	0.22*** (0.05)
	PRIV	–	0.77*** (0.04)	–	0.74*** (0.04)
	INT	–	0.58*** (0.04)	–	0.50*** (0.05)

Standard errors reported in parentheses.
SE, standard error; TRUST, general institutional trust; CONC, general privacy concerns; RISKS, perceived risks of information disclosure; BEN, perceived benefits of information disclosure; PRIV, perceived privacy; INT, intention to disclose; AFF, main effect of affect; SENS, main effect of information sensitivity; AFF×SENS, interaction effect affect and information sensitivity
*$p < 0.06$ **$p < 0.05$ ***$p < 0.01$.

coefficients output by the complete structural model. Furthermore, model fit indices indicated worse fit to the underlying data structure (χ^2 = 111.88, *df* = 58, χ^2/df =1.93, *CFI* = 0.97, *TLI* = 0.97, *RMSEA* = 0.067), and the explained variance of intention to disclose was lower with 19% of explained variance in the US sample and 15% of explained variance in the Swiss sample.

Second, we tested for significant mediation effects in the complete structural model. In Mplus, mediation analysis is conducted using the delta method, a more generalized and reliable approach than the Sobel test (MacKinnon *et al*., 2002). As illustrated in Table 5, one of four direct effects was marginally significant, while total and specific indirect paths yielded significant outcomes in all other cases. As such, full mediation hypotheses could be supported in three of four cases, while the relationship between general privacy concerns and intention to disclose was partially mediated by situational calculus variables in the US sample. Therefore, we concluded that Hypotheses 5b and 6b were mainly supported by the data.

Situational factors: information sensitivity and affect

In Hypotheses 7a, 7b, 8a and 8b, we proposed that (1) a higher level of information sensitivity would cause an increase in perceived risks and a decrease in perceived benefits, and that (2) this effect could be overridden by positive affect because of risk underestimation and benefit overestimation.

Table 6. Tests of total, direct and indirect effects

	US sample				Swiss sample			
	Total	Indirect	Direct	Decision	Total	Indirect	Direct	Decision
CONC➔ INT	−.30**	−.17**	−.13*	PM	−.23**	−.18**	−.04	FM
TRUST➔ INT	.25**	.17**	.08	FM	.16**	.25**	−.08	FM

CONC, general privacy concerns; INT, intention to disclose; TRUST, general institutional trust; PM, partial mediation; FM, full mediation.
**$p < 0.01$. *$p = 0.045$.

With regard to risk perception, we found a significant main effect of information sensitivity in the US sample and a significant interaction effect of information sensitivity and affect (Table 5): Participants in the high sensitivity condition generally tended to rate risks higher by 0.20 *SD* ($p < 0.05$). For participants in the positive affect and high information sensitivity condition, however, the expectation value decreased by −0.24 *SD* ($p < 0.05$), approximating the expectation value of 0.07 *SD* for participants in the positive affect, but low sensitivity condition. This indicates that participants in the positive affect but low sensitivity condition did not noticeably differ from participants in the positive affect but high sensitivity condition. Stated differently, the risk perceptions of participants in the positive affect condition were not substantially influenced by information sensitivity, while risk perceptions of participants in the neutral affect condition were highly dependent on information sensitivity.

Similarly, ratings of information sensitivity increased by 0.15 *SD* in the Swiss sample between low and high sensitivity conditions, indicating a general increase in risk perception for participants in the high information sensitivity condition. In contrast to the US sample, however, this effect was only marginally significant ($p < 0.06$) among Swiss participants. As reflected by a significant interaction effect ($p < 0.05$), the expectation value for participants in the positive affect and high information sensitivity condition (0.15 *SD*) was comparable with the expectation value for participants in the positive affect and low information sensitivity condition (0.20 *SD*), implying that the risk perception of participants in the positive affect condition did not substantially differ across information sensitivity conditions. Surprisingly, however, participants in the positive affect condition tended to generally rate perceived risks higher as compared with participants in the neutral affect condition. In our model, this is reflected by a significant main effect of affect in the Swiss sample with an expectation value of 0.20 *SD* ($p < 0.01$). For illustration purposes, expectation values of perceived risks for both samples are depicted in Figure 3.

With regard to perceived benefits, a significant main effect of information sensitivity could be identified in the US sample. Compared with the low sensitivity condition, participants in the high sensitivity condition showed lower ratings of perceived benefits (expectation value of −0.24 *SD* across conditions, $p < 0.01$). However, further effects could not be identified. As a result, we concluded that Hypotheses 7a and 8a were supported by the data, while we only found partial support for Hypothesis 7b, and no support for Hypothesis 8b.

DISCUSSION

In our study, we designed and conducted an experiment that systematically manipulated affective thinking in a situational privacy calculus while simultaneously distinguishing dispositional from situational factors.

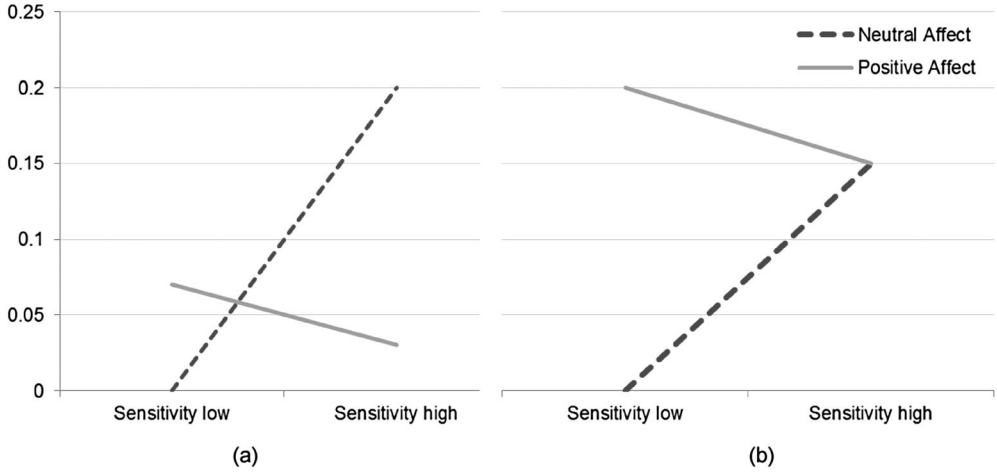

Figure 3. Effects of experimental manipulation on perceived risks in (a) the US sample and (b) the Swiss sample.

Our results largely supported the hypothesized relationships and differences in both samples. As reflected by strong relationships between correspondent constructs, the study confirmed the suitability of a situational privacy calculus as a theoretical framework to study privacy-related decision-making, and strong support for the assumption of interdependence of risk and benefit perceptions was revealed. Furthermore, we conceptualized the conjoint assessment of perceived risks and perceived benefits as a state of privacy, or perceived privacy, and yielded strong relationships between correspondent variables.

Also, we found the relationship of dispositional factors and intentions to disclose to be fully mediated by situational privacy calculus variables in three of four cases. In line with our expectations, these results imply situation-specific considerations to be capable to dominate pre-existing attitudes. Moreover, our approach revealed affective thinking to constitute a factor that guides irrational valuation of perceived risks, supporting the hypothesis that rationality in privacy-related decision-making is bounded by psychological limitations.

Theoretical implications

This research presented a model that integrates two streams of literature in the domain of privacy-related decision-making: First, several authors (Li *et al*., 2011; Wilson & Valacich, 2012; Keith *et al*., 2013) have proposed a systematic distinction between dispositional tendencies and situational factors that shape privacy-related decisions. Second, an increasing number of studies (e.g. Grossklags & Acquisti, 2007; Acquisti, 2009; Brandimarte *et al*., 2012) attempts to explore the boundaries of rationality in this context. Embracing both aspects, our study uniquely contributes to current research in information privacy in several ways:

First, the study has shown that perceived privacy may constitute a valuable construct to reflect the conjoint assessment of situation-specific risk and benefit perceptions. Similar to Dinev *et al*. (2012), we defined perceived privacy as an individual state, subsuming all privacy-related

considerations at a specific point in time. While many prior studies have used privacy concerns as a 'proxy to privacy' (Smith *et al*., 2011), a conceptualization of privacy as a state emphasizes the contextual and situational nature of privacy beliefs. As such, researchers may find the construct helpful when further exploring the contextual nature of privacy-related phenomena (Bélanger & Crossler, 2011; Smith *et al*., 2011).

Also, we found evidence on the *interdependence* of risk and benefit perceptions, implying individuals to use perceptions of benefits as a cue for risk valuation. Given that risks and benefits often correlate positively in reality, founding risk valuations on benefit perceptions is likely to result in biased appraisals. For example, the application that offers the most beneficial functionality may also heavily misuse sensitive information provided by the user. Relying on own benefit perceptions when valuing risks, therefore, could lead to biased decisions. In this regard, this finding challenges some of the basic notions of the privacy calculus model, which expects individuals to fully and independently weigh risks and benefits in order to take decisions (Dinev & Hart, 2006; Anderson & Agarwal, 2011).

Furthermore, our study uniquely adds to the increasing stream of literature that analyses the role of bounded rationality in privacy-related decision-making. While prior studies in this field mainly focused on cognitive phenomena that modulate rational thinking (such as salience shifting; Johnson *et al*., 2002), we have emphasized the role of affective thinking as a second parallel mode of cognitive processing. That is, we have demonstrated that feelings and emotion subconsciously shape privacy-related risk perceptions. Our results are in line with prior research that linked positive emotions to lowered perceptions of risk (Li *et al*., 2011), higher intention to disclose information (Anderson & Agarwal, 2011) or increased trust (Wakefield, 2013). In contrast to these studies, however, we used an experimental approach to induce affect, and demonstrated affect-based thinking to be capable to not only shape but even override rational factors. Given that information privacy research has predominantly assumed privacy-related decision-making to constitute a rational process, our study opens a new avenue for the investigation of irrationality and emotion in information privacy research.

We further proposed a conceptual distinction between dispositional and situational factors. This differentiation is not new per se – Li *et al*. (2011) as well as Keith *et al*. (2013) used a similar approach to analyse disclosing behaviors. In this regard, however, our findings make two relevant additions: First, we have extended the basic idea to a second factor, general institutional trust, and found that privacy assessment is shaped by institutional trust in a similar vein as general privacy concerns. Second, empirical results indicate the relationship between dispositional tendencies and the intention to disclose information to be *fully* mediated by a situational calculus. This finding contradicts earlier works that proposed *partial* mediation between general privacy concerns and disclosing intentions (Li *et al*., 2011; Wilson & Valacich, 2012). One explanation might concern the methodological approach chosen: While earlier studies usually measured dispositional tendencies *after* introducing the context or product of investigation (Dinev & Hart, 2006; Hu *et al*., 2010; Anderson & Agarwal, 2011; Li *et al*., 2011; Xu *et al*., 2011a), we systematically distinguished dispositional tendencies from situational variables by assessing them *before* experimental manipulation. Thus, our approach might have emphasized the dispositional nature of general privacy concerns and general institutional trust more thoroughly, and prevented the deployed scales to be biased from priming effects rooted in the

situation at hand (Decoster & Claypool, 2004). Given that earlier studies have inconsistently modeled disclosure behavior in the privacy calculus framework, the conceptual and methodological separation of dispositional and situational factors as suggested by our findings makes an important addition to the knowledge on the relationship and interplay of privacy-related constructs.

On the whole, our research offers a new perspective on the widespread observation of discrepancies between reported privacy concerns and disclosing behaviors, often referred to as the *privacy paradox* (Norberg *et al*., 2007; Xu *et al*., 2011b). While some researchers (Smith *et al*., 2011) have attributed this phenomenon to the scarce number of studies involving actual data disclosure as opposed to behavioral intentions, arguing that intention-behavior gaps occur in numerous areas of behavior (Ajzen, 1985; Ajzen *et al*., 2004), our results imply the privacy paradox to result from biased intention forming. That is, our study suggests that small relationships between privacy concerns and disclosing behavior may be caused by (1) biased cognitive valuation processes due to misleading situational cues, such as affective thinking, and (2) the relative valence of situation-specific considerations as compared with rather generic attitudes. Based on these propositions, the privacy paradox could be described as an attitude-intention rather than an intention-behavior gap: While privacy-related, dispositional attitudes determine initial cognitions in a privacy decision-making situation, the intention to disclose, or not disclose, private information is primarily determined by situational cues (Li *et al*., 2011). This view is supported by prior studies that did not only identify small or non-significant relationships between privacy concerns and *actual* disclosing behavior (e.g. Hui *et al*., 2007) but also between privacy concerns and behavioral *intentions* (Awad &d Krishnan, 2006; Van Slyke *et al*., 2006). Also, Keith *et al*. (2013) found similar effects when studying attitudes, intentions *and* actual disclosing behavior simultaneously. Yet, more research that tracks the full path from attitudes to behaviors is needed in order to foster our understanding on the sources of the privacy paradox. In this regard, our model may serve as a useful framework for further empirical investigation and theory-building.

Practical implications

The results of this research also have important managerial and public policy implications. First, our results may help firms in understanding when and to what extent consumers are willing to disclose personal information. Although our results indicate that dispositional factors may affect disclosure intentions, they also show that these dispositions operate through a situation-specific privacy assessment. Hence, a firm aiming to collect personal information needs to understand how consumers weigh risks and benefits at the particular moment it is asking for access to that information. In this respect, our results indicate that a firm may be more likely to gain access to personal information when it manages to elicit positive affect through the specific design of their information systems. In our research, we elicited positive affect through a modification of the user interface. While this modification was simple to implement, it was strong enough to affect consumers' perceptions of risks connected to information disclosure. However, positive affect may not only be elicited through an interface's design but may also be momentarily induced through factors that are external to the actual decision environment (Coan & Allen, 2007).

At the same time, our findings may have important implications for public policy decisions. As such, while researchers have argued that consumers are increasingly concerned about protecting personal information from commercial firms (Pavlou & Fygenson, 2006; Pavlou, 2011), our findings suggest that a simple manipulation of affective context may be sufficient to override these concerns and may lead consumers to disclose personal information that they would not agree to disclose in a more balanced affective state. Affect-eliciting newsfeeds on social media websites, for example, could lead individuals to frequently experience positive affect (Kramer *et al*., 2014) and result in biased beliefs and behaviors concerning the use of personal information, e.g. for targeted advertising.

Given that, on the other hand, the elicitation of positive affect is a common goal in user experience design (Zhang, 2008), our results may also have implications for the broader literature on information privacy policies and the ethical behavior of firms (e.g. Walsham, 1996; Culnan & Williams, 2009; Smith *et al*., 2011; Stahl, 2012). Most of this research has focused on the problems that may arise after firms have collected information, including the reuse of personal information without the explicit consent from the consumer, or selling private data to third parties (Culnan and& Williams, 2009; Pavlou, 2011; Conger *et al*., 2013). Apart from identifying these problems, prior research has also developed recommendations on how firms can integrate ethical considerations into their privacy policies and how consumers can be protected against misuse of their information (e.g. Culnan & Williams, 2009). Our research may provide a different perspective on this discussion. That is, while existing studies have mostly examined how to protect consumers *after* information has been collected, our research indicates that policy makers may also need to think about how to protect consumers *before* or *while* their personal information is being collected.

Hence, our findings may not only raise the question if and to what extent affect-eliciting practices, such as the ones described in this research, are appropriate from a normative perspective but they may also indicate that policy makers may need to think about how to improve privacy-related decision-making in these environments. This may, for example, involve informing consumers about how positive affect may influence their privacy-related decisions and/or developing methods that will allow consumers to make balanced decisions regarding their personal data, even when influenced by affective thinking.

Limitations and future work

Although the data generally supported the proposed model, several limitations of our work need to be noted. In the following, we will discuss these constraints and expound their potential to encourage future work.

First, our study was planned as a cross-sectional experiment and used product scenarios in order to induce affect and information sensitivity. Although this approach seemed valuable with regard to the internal validity of our findings, it can be assumed that a more realistic scenario could deepen insights on the interplay of dispositional tendencies and situational factors. A study comprising actual disclosing behaviors of a real product over a certain amount of time, for example, would add to the literature by exploring the temporal stability of dispositional factors, as well as the relative importance of situational factors in different situations. Yet,

longitudinal studies that analyze the dynamics of privacy-related constructs over time are scarce in information privacy research (see Milne & Culnan, 2002, for one of the few exceptions).

Second, our results reveal general privacy concerns to be subject to overriding effects by a situational privacy calculus. In the Swiss sample, however, psychometric properties of the deployed privacy concerns scale yielded low convergent validity, indicating results in the Swiss sample might be flawed by validity issues. Because this outcome seems to result from a low factor loading of only one indicator, we assume the differences between samples to be likely caused by methodological artifacts, such as misleading translation. As such, this limitation highlights the need for validated multi-language instruments in the domain of information privacy.

Also, the results of the Swiss sample indicated perceived risks to generally increase if participants were confronted with a positive affect screenshot. Furthermore, our data did not reveal evidence on the influence of affective thinking on individuals' benefit perceptions, resulting in comparably low proportions of explained variance in this variable (Table 5). In this regard, our research constitutes a preliminary investigation of affective stimuli capable to guide privacy-related decision-making, and further research is needed to investigate the interplay of rational and affective thinking in this context. For instance, it could be hypothesized that stronger affective appeals (such as even cuter screenshots; Hsee & Rottenstreich, 2004) may result in more theory-accordant reactions. Also, investigating different emotions might be of interest, given that separate emotions seem to administer differential impact on risk assessment and decision-making (Lerner *et al.*, 2004). Anxiety, for example, is known to inhibit rational considerations of risks, resulting in risk overestimation (Nesse & Klaas, 1994).

Similarly, our research may encourage scholars to more intensively explore the boundaries of rationality in the context of privacy-related decision-making. While this study was designed to cover one specific cognitive heuristic, knowledge on the role of other heuristics could essentially deepen our understanding on how and why individuals disclose their data. In this regard, the framework developed in our study might also foster research on cognitive interventions that aim to strengthen individuals' capabilities to take decisions that are in line with their own dispositions. Techniques of cognitive dissonance reduction, for example, are known to bridge attitude-intention gaps in many other fields of behavior (Stone & Fernandez, 2008).

CONCLUSION

This research has provided insights into the psychological processes that are triggered when firms ask consumers for access to highly personal information. In particular, our study illustrates the complexity of privacy decisions by showing that these decisions are not only driven by a situation-specific privacy assessment but are also determined by general dispositions (i.e. general privacy concerns and institutional trust) and affect-based heuristics that consumers may not be fully aware of. While examining the joint influence of situational, dispositional and affective factors in a single research model necessarily increases the complexity of the conceptual and empirical analyses, we feel that this will allow us to gain a more accurate understanding of individuals' privacy decisions. As such, the results of our work lay a fruitful ground for further

work that strives to investigate the dynamics of privacy-related decision-making and enhance our understanding of when and why individuals disclose personal information.

CONFLICT OF INTEREST

No conflicts of interest have been declared.

ACKNOWLEDGEMENTS

This research has been partially funded by a Swiss insurance company.

REFERENCES

Acquisti, A. (2004) Privacy in electronic commerce and the economics of immediate gratification. Paper presented at the 5th ACM conference on Electronic Commerce, New York, USA.

Acquisti, A. (2009) Nudging privacy: the behavioral economics of personal information. *IEEE Security and Privacy*, **7**, 82–85.

Acquisti, A., & Grossklags, J. (2005) Privacy and rationality in individual decision-making. *IEEE Security and Privacy*, **3**, 26–33.

Acquisti, A., John, L., & Loewenstein, G. (2009) What is privacy worth? Paper presented at the Twenty First Workshop on Information Systems and Economics (WISE), Phoenix, AZ.

Agosto, D.E. (2002) Bounded rationality and satisficing in young people's Web-based decision making. *Journal of the American Society for Information Science and Technology*, **53**, 16–27.

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

Ajzen, I., Brown, T.C. & Carvajal, F. (2004) Explaining the discrepancy between intentions and actions: the case of hypothetical bias in contingent valuation. *Personality and Social Psychology Bulletin*, **30**, 1108–1121.

Alhakami, A.S., & Slovic, P. (1994) A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis*, **14**, 1085–1096.

Anderson, C.L. & Agarwal, R. (2011) The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, **22**, 469–490.

Awad, N.F. & Krishnan, M.S. (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, **30**, 13–28.

Bansal, G., Zahedi, F.M. & Gefen, D. (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, **49**, 138–150.

Bélanger, F. & Crossler, R.E. (2011) Privacy in the digital Age: a review of information privacy research in information systems. *MIS Quarterly*, **35**, 1017–1042.

Brandimarte, L., Acquisti, A. & Loewenstein, G. (2012) Misplaced confidences: privacy and the control paradox. *Social Psychological and Personality Science*, **4**, 340–347.

Byrne, B.M., Shavelson, R.J. & Muthén, B. (1989) Testing for the equivalence of factor covariance and mean structures: the issue of partial measurement invariance. *Psychological Bulletin*, **105**, 456–466.

Carmines, E.G. & Mciver, J.P. (1981) Analyzing models with unobserved variables: analysis of covariance structures. In: *Social Measurement: Current Issues*, Bohmstedt, G.W. & Borgatta, E.F. (Eds.), pp. 65–115. Sage, Newberry Park, CA.

Chin, W.W., & Gopal, A. (1995) Adoption intention in GSS: relative importance of beliefs. *ACM SigMIS Database*, **26**, 42–64.

Coan, J.A. & Allen, J.J.B. (2007) *Handbook of Emotion Elicitation and Assessment*. Oxford University Press, Oxford.

Conger, S., Pratt, J.H. & Loch, K.D. (2013) Personal information privacy and emerging technologies. *Information Systems Journal*, **23**, 401–417.

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

Culnan, M.J. & Bies, R.J. (2003) Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues*, **59**, 323–342.

Culnan, M.J. & Williams, C.C. (2009) How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, **33**, 673–687.

Damasio, A.R. (1994) *Descartes' Error: Emotion, Rationality and the Human Brain*. Putnam, New York, NY.

Decoster, J. & Claypool, H.M. (2004) A meta-analysis of priming effects on impression formation supporting a general model of informational biases. *Personality and Social Psychology Review*, **8**, 2–27.

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

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. & Colautti, C. (2006) Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, **15**, 389–402.

Dinev, T., Goo, J., Hu, Q. & Nam, K. (2009) User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, **19**, 391–412.

Dinev, T., Xu, H., Smith, J.H. & Hart, P. (2012) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, **22**, 61–80.

Epstein, S. (1994) Integration of the cognitive and the psychodynamic unconscious. *American Psychologist*, **49**, 709–724.

Finucane, M.L. & Holup, J.L. (2006) Risk as value: combining affect and analysis in risk judgments. *Journal of Risk Research*, **9**, 141–164.

Finucane, M.L., Alhakami, A., Slovic, P. & Johnson, S.M. (2000) The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, **13**, 1–17.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. & Combs, B. (1978) How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, **9**, 127–152.

Fornell, C. & Larcker, D.F. (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, **18**, 39–50.

Fox, E. (2008) *Emotion Science: Cognitive and Neuroscientific Approaches to Understanding Human Emotions*. Palgrave, Basingstoke.

Franko, O.I. & Tirrell, T.F. (2012) Smartphone app use among medical providers in ACGME training programs. *Journal of Medical Systems*, **36**, 3135–3139.

Gefen, D., Straub, D.W. & Boudreau, M.C. (2000) Structural equation modeling and regression: guidelines for research practice. *Communications of the Association for Information Systems*, **4**, 2–76.

Gefen, D., Straub, D.W. & Rigdon, E.E. (2011) An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, **35**, iii–xiv.

Gigerenzer, G. & Gaissmaier, W. (2011) Heuristic decision making. *Annual Review of Psychology*, **62**, 451–482.

Grossklags, J. & Acquisti, A.C. (2007) When 25 cents is too much: an experiment on willingness-to-sell and willingness-to-protect personal information. Paper presented at the Workshop on the Economics of Information Security, New York, NY.

Hanoch, Y. (2002) "Neither an angel nor an ant": emotion as an aid to bounded rationality. *Journal of Economic Psychology*, **23**, 1–25.

Hsee, C.K. & Rottenstreich, Y. (2004) Music, pandas, and muggers: on the affective psychology of value. *Journal of Experimental Psychology: General*, **133**, 23–30.

Hu, X.R., Wu, G.H., Wu, Y.H. & Zhang, H. (2010) The effects of Web assurance seals on consumers' initial trust in an online vendor: a functional perspective. *Decision Support Systems*, **48**, 407–418.

Hui, K.L., Tan, B.C.Y. & Goh, C.Y. (2006) Online information disclosure: motivators and measurements. *ACM Transactions on Internet Technology (TOIT)*, **6**, 415–441.

Hui, K.L., Teo, H.H. & Lee, S.Y.T. (2007) The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, **31**, 19–33.

Johnson, E.J., Bellmann, S. & Lohse, G.L. (2002) Defaults, framing and privacy: Why opting in-opting Out. *Marketing Letters*, **13**, 5–15.

Keith, M., Thompson, S., Hale, J. & Greer, C. (2012) Examining the rationality of location data disclosure through mobile devices. *Proceedings of the 33rd International Conference on Information Systems* (*ICIS 2012*), *Orlando*.

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

Kim, J., Allen, C.T. & Kardes, F.R. (1996) An investigation of the mediational mechanisms underlying attitudinal conditioning. *Journal of Marketing Research*, **33**, 318–328.

Kim, D.J., Ferrin, D.L. & Rao, H.R. (2008) A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support Systems*, **44**, 544–564.

Knijnenburg, B.P., Kobsa, A. & Jin, H. (2013) Counteracting the negative effect of form auto-completion on the privacy calculus. *Proceedings of the 34th International Conference on Information Systems* (*ICIS 2013*), Milan, Italy.

Kramer, A.D.I., Guillory, J.E. & Hancock, J.T. (2014) Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 10.1073/pnas.1320040111.

Krasnova, H., Veltri, N.F. & Gunther, O. (2012) Self-disclosure and privacy calculus on social networking sites: the role of culture. *Business and Information Systems Engineering*, **4**, 127–135.

Lerner, J.S., Small, D.A. & Loewenstein, G. (2004) Heart strings and purse strings: carryover effects of emotions on economic decisions. *Psychological Science*, **15**, 337–341.

Li, H., Sarathy, R. & Xu, H. (2011) The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, **51**, 434–445.

Li, T., Pavlou, P.A. & Dos Santos, G.L. (2013) What drives users' website registration? A randomized field experiment. *Proceedings of the 34th International Conference on Information Systems* (*ICIS 2013*), Milan, Italy.

Loewenstein, G.F., Weber, E.U., Hsee, C.K. & Welch, N. (2001) Risk as feelings. *Psychological Bulletin*, **127**, 267–286.

Mackenzie, S.B., Podsakoff, P.M. & Podsakoff, N.P. (2011) Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. *MIS Quarterly*, **35**, 293–334.

MacKinnon, D.P., Lockwood, C.M., Hoffman, J.M., West, S. G. & Sheets, V. (2002) A comparison of methods to test mediation and other intervening variable effects. *Psychological Methods*, **7**, 83–104.

Malhotra, N.K., Kim, S.S. & Agarwal, J. (2004) Internet users' information privacy concerns (IUIPC): tthe construct, the scale, and a causal model. *Information Systems Research*, **15**, 336–355.

Milne, G.R. & Culnan, M.J. (2002) Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998–2001 US web surveys. *The Information Society*, **18**, 345–359.

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E. & Wang, S.J. (2012) Disclosure antecedents in an online service context: the role of sensitivity of information. *Journal of Service Research*, **15**, 76–98.

Muthén, L.K. & Muthén, B.O. (2011) MPlus (Version 6.12).

Mylonas, A., Meletiadis, V., Mitrou, L. & Gritzalis, D. (2013) Smartphone sensor data as digital evidence. *Computers and Security*, **38**, 51–75.

Nesse, R.M. & Klaas, R. (1994) Risk perception by patients with anxiety disorders. *The Journal of Nervous and Mental Disease*, **182**, 465–470.

Norberg, P.A., Horne, D.R. & Horne, D.A. (2007) The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, **41**, 100–126.

Nyshadham, E.A. & Castano, D. (2012) Affect and online privacy concerns. *SSRN Electronic Journal*. available from: http://ssrn.com/abstract=2051044.

Pachur, T., Hertwig, R. & Steinmann, F. (2012) How do people judge risks: availability heuristic, affect heuristic, or both? *Journal of Experimental Psychology: Applied*, **18**, 314–330.

Pavlou, P.A. (2011) State of the information privacy literature: where are we now and where should we go? *MIS Quarterly*, **35**, 977–988.

Pavlou, P.A. & Fygenson, M. (2006) Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. *MIS Quarterly*, **30**, 115–143.

Pavlou, P.A. & Gefen, D. (2004) Building effective online marketplaces with institution-based trust. *Information Systems Research*, **15**, 37–59.

Pengnate, S. & Antonenko, P. (2013) A multimethod evaluation of online trust and its interaction with metacognitive awareness: an emotional design perspective. *International Journal of Human-Computer Interaction*, **29**, 582–593.

Podsakoff, P.M., Mackenzie, S.B., Lee, J.Y. & Podsakoff, N. P. (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, **88**, 879–903.

Reyna, V.F. (2004) How people make decisions that involve risk – a dual-processes approach. *Current Directions in Psychological Science*, **13**, 60–66.

Rohm, A.J. & Milne, G.R. (2004) Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, **57**, 1000–1011.

Satorra, A. & Bentler, P.M. (2001) A scaled difference Chi-square test statistic for moment structure analysis. *Psychometrika*, **66**, 507–514.

Schwarz, N. (2011) Feelings-as-information theory. In: *Handbook of Theories of Social Psychology*, Van Lange, P., Kruglanski, A.W. & Higgins, E.T. (Eds.), pp. 289–308. Sage Publications Ltd., London.

Segars, A.H., & Grover, V. (1993) Re-examining perceived ease of use and usefulness. *MIS Quarterly*, **17**, 517–525.

Siegrist, M., Cvetkovich, G., & Roth, C. (2000) Salient value similarity, social trust, and risk/benefit perception. *Risk Analysis*, **20**, 353–362.

Simon, H.A. (1955) A behavioral model of rational choice. *The Quarterly Journal of Economics*, **69**, 99–118.

Simon, H.A. (1979) Rational decision making in business organizations. *The American Economic Review*, **69**, 493–513.

Slovic, P., Finucane, M.L., Peters, E. & Macgregor, D.G. (2004) Risk as analysis and risk as feelings: some thoughts about affect, reason, risk, and rationality. *Risk Analysis*, **24**, 311–322.

Slovic, P., Finucane, M.L., Peters, E. & Macgregor, D.G. (2007) The affect heuristic. *European Journal of Operational Research*, **177**, 1333–1352.

Smith, H.J., Dinev, T. & Xu, H. (2011) Information privacy research: an interdisciplinary review. *MIS Quarterly*, **35**, 989–1015.

Sonderegger, A. & Sauer, J. (2010) The influence of design aesthetics in usability testing: effects on user performance and perceived usability. *Applied Ergonomics*, **41**, 403–410.

Sonderegger, A., Zbinden, G., Uebelbacher, A. & Sauer, J. (2012) The influence of product aesthetics and usability over the course of time: a longitudinal field experiment. *Ergonomics*, **55**, 713–730.

Stahl, B.C. (2012) Morality, ethics, and reflection: a categorization of normative IS research. *Journal of the Association for Information Systems*, **13**, 636–656.

Steenkamp, J.-B.E. M., & Baumgartner, H. (1998) Assessing measurement invariance in cross-national consumer research. *Journal of Consumer Research*, **25**, 78–107.

Stone, J. & Fernandez, N.C. (2008) To practice what we preach: the use of hypocrisy and cognitive dissonance to motivate behavior change. *Social and Personality Psychology Compass*, **2**, 1024–1051.

Teo, T., Lee, C.B., Chai, C.S. & Wong, S.L. (2009) Assessing the intention to use technology among pre-service teachers in Singapore and Malaysia: a multigroup invariance analysis of the technology acceptance model (TAM). *Computers & Education*, **53**, 1000–1009.

Tsai, J.Y., Egelman, S., Cranor, L. & Acquisti, A. (2011) The effect of online privacy information on purchasing behavior: an experimental study. *Information Systems Research*, **22**, 254–268.

Van De Schoot, R., Lugtig, P. & Hox, J. (2012) A checklist for testing measurement invariance. *European Journal of Developmental Psychology*, **9**, 486–492.

Van Slyke, C., Shim, J.T., Johnson, R. & Jiang, J. (2006) Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, **7**, 415–444.

Vandenberg, R.J. & Lance, C.E. (2000) A review and synthesis of the measurement invariance literature: suggestions, practices, and recommendations for organizational research. *Organizational Research Methods*, **3**, 4–70.

Wakefield, R. (2013) The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, **22**, 157–174.

Walsham, G. (1996) Ethical theory, codes of ethics and IS practice. *Information Systems Journal*, **6**, 69–81.

Wilson, D. & Valacich, J. (2012) Unpacking the privacy paradox: irrational decision-making within the privacy calculus. *Proceedings of the 33rd International Conference on Information Systems* (*ICIS 2012*), *Orlando*.

Xie, E., Teo, H.-H. & Wan, W. (2006) Volunteering personal information on the Internet: effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters*, **17**, 61–74.

Xu, H., Teo, H.H., Tan, B.C.Y. & Agarwal, R. (2009) The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, **26**, 135–173.

Xu, H., Dinev, T., Smith, J.H. & Hart, P. (2011a) Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, **12**, 798–824.

Xu, H., Luo, X., Carroll, J.M. & Rosson, M.B. (2011b) The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, **51**, 42–52.

Zajonc, R.B. (1980) Feeling and thinking - preferences need no inferences. *American Psychologist*, **35**, 151–175.

Zhang, P. (2008). Toward a positive design theory: Principles for designing motivating information and communication technology. In: *Advances in Designing Information and Organizations with a Positive Lens (Advances in Appreciative Inquiry, Volume 2)*, Avital, M., Boland, R.J. & Cooperrider, D.L. (Eds.), pp. 45–74. JAI Press, Greenwich, CT.

Biographies

Flavius Kehr is a PhD candidate at the Institute of Technology Management (ITEM) of the University of St. Gallen in Switzerland. He holds a German diploma in psychology and has worked as a User Experience professional for stakeholders in Germany and Singapore. Focusing on the

impact of motivation and emotion on technology use, his scientific work has been published in national and international outlets, including ACM's Conference on Human Factors in Computing Systems (CHI) and the International Conference of Information Systems (ICIS). His research interests include information privacy, health information systems, user experience and technology-mediated behavior change.

Tobias Kowatsch leads the Health-IS Lab, a joint initiative of the University of St. Gallen and ETH Zurich in Switzerland. His research interests are the design and evaluation of health information systems that improve not only the outcomes of health interventions but also support health promotion and disease prevention strategies of organizations. In 2005, he received his diploma degree in media informatics from Hochschule Furtwangen University (HFU), Germany. After studying in Scotland and doing social volunteering in South Africa, he attended the Master's program in computer science in media at HFU and passed with distinction. Since 2012, he also holds a master's degree in business informatics from Saarland University, Germany. His research was published in journals such as *Computers and Human Behavior* and presented at various conferences such as the *European Conference on Information Systems*.

Daniel Wentzel is professor of marketing at RWTH Aachen University, Germany. He holds a PhD in business administration from the University of St. Gallen, Switzerland. His research has been published in journals such as *Journal of Marketing*, *Journal of the Academy of Marketing Science* and *Journal of Service Research* as well as the *Proceedings of the International Conference on Information Systems*. His current research interests include innovation marketing, product design and consumer behavior in digital environments. He is especially interested in understanding how consumers make sense of innovative products, services and technologies and how they incorporate new technologies into their existing consumption patterns.

Elgar Fleisch is a professor of Information and Technology Management at the Institute of Technology Management, University of St. Gallen (ITEM-HSG) and the Department of Management, Technology and Economics, ETH Zurich (D-MTEC). The research of Prof. Fleisch focuses on the intersection of technology and behavioral economics in several application domains, e.g. with regard to energy consumption, e-commerce, health or privacy. The interdisciplinary research of Prof. Fleisch and his team has been published in more than 200 scientific journals and books, including computer science outlets such as *ACM UbiComp*, IS outlets such as *MIS Quarterly*, as well as domain-specific journals such as *Obesity Reviews* or *Energy Policy*.

APPENDIX

Appendix 1. Questionnaire

Construct / Items	Scale	Origin
General Privacy Concerns	Likert 1–7 (1 = totally disagree, 7 = totally agree)	Malhotra *et al*. (2004)
Compared with others, I am more sensitive about the way smartphone apps handle my personal information.		
To me, it is the most important thing to keep my privacy intact from smartphone apps. (reverse coded)		
In general, I am very concerned about threats to my personal privacy		
General Institutional Trust	Likert 1–7 (1 = totally disagree, 7 = totally agree)	Malhotra *et al*. (2004)
Smartphone apps are trustworthy in handling client data.		
Smartphone apps would tell the truth and fulfill promises related to the information provided by me.		
Smartphone apps are always honest with customers when it comes to using the information that I would provide		
Information Sensitivity	Semantic differential	Xie *et al*. (2006)

(Continues)

Appendix 1. (Continued)

Construct / Items	Scale	Origin
How sensitive do you perceive the information requested by the app to be?		
Not sensitive at all/very sensitive		
Affect	Semantic differential	Kim *et al*. (1996)
Please rate the screenshot on the following dimensions:		
Unpleasant/pleasant		
Dislike very much/like very much		
Left me with a bad feeling/left me with a good feeling		
Perceived Risks of Information Disclosure	Likert 1–7 (1 = totally disagree, 7 = totally agree)	Dinev *et al*. (2012)
It would be risky to give personal information to the smartphone app.		
There would be high potential for privacy loss associated with giving personal information to the smartphone app.		
Personal information could be inappropriately used by using the smartphone app.		
Providing the smartphone app with my personal information could involve many unexpected problems.		
Perceived Benefits of Information Disclosure	Likert 1–7 (1 = totally disagree, 7 = totally agree)	Dinev et al. (2012)
Providing my personal information to the smartphone app will entail benefits.		
Revealing my personal information to the smartphone app will help me obtain the services I want.		
I believe that as a result of my personal information disclosure, I will benefit from a better, more customized service.		
Perceived Privacy	Likert 1–7 (1 = totally disagree, 7 = totally agree)	Dinev *et al*. (2012)
I feel I'll have enough privacy when using the smartphone app.		
I am comfortable with the amount of privacy I will have when using the smartphone app.		
I think my privacy is preserved when I use the smartphone app.		
Intention to disclose	Semantic differential	Anderson and Agarwal (2011)
Please specify the extent to which you would reveal your personal information to use the smartphone app:		
Willing/unwilling		
Unlikely/likely		
Not probable/probable		

Appendix 2. Stimulus Material

Note: The following screenshot depicts the stimulus material as used in the positive affect/low information sensitivity condition. In high information sensitivity condition, information types (year of construction, car type and distance traveled) were replaced by 'time of a trip', 'violation

of speed limits while driving car' and 'information about location while driving car'. For an illustration of the used screenshot in neutral affect condition, see Figure 2.