Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus

Running Title: Privacy Calculus: Dispositions and Affect

Flavius Kehr
Institute of Technology Management
University of St. Gallen
St. Gallen, Switzerland

Tobias Kowatsch
Institute of Technology Management
University of St. Gallen
St. Gallen, Switzerland

Daniel Wentzel
Chair of Marketing
RWTH Aachen University
Aachen, Germany

Elgar Fleisch
Institute of Technology Management
University of St. Gallen
St. Gallen, Switzerland
and
Department of Management, Technology, and Economics
ETH Zurich
Zurich, Switzerland

to appear in:

Information Systems Journal Special Issue on:
Privacy in a Networked World (2015).

Number of Words: 7957

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 U.S. and Switzerland, examined consumer responses to a new smartphone application collecting 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 also 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 confronted with the decision to disclose personal information (Malhotra *et al.*, 2004; Xu *et al.*, 2009) or conduct transactions (Pavlou & 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 (Dinev *et al.*, 2012; Malhotra *et al.*, 2004), 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). 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 savings 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 affected by psychological limitations such as the inability to process all information relevant to the cost-benefit-ratio (Acquisti & Grossklags, 2005; Acquisti *et al.*, 2009), bounded rationality (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 tendencies 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

In the privacy calculus literature, perceived risks generally refer to the "potential for loss associated with the release of personal information" (Smith *et al.*, 2011, p. 1001), while perceived benefits are regarded as perceptions of the "derived value from the disclosure of personal information" (Wilson & Valacich, 2012, p. 6). Information systems (IS) researchers have typically regarded perceived risks and benefits as independent constructs (e.g. Dinev and Hart, 2006; Li *et al.*, 2011; Xu *et al.*, 2009). Recent research, however 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). This view is in line with findings in behavioral economics: Fischhoff *et al.* (1978), for example, noted that individuals tend to think that risk and benefits correlate negatively even though they often correlate positively in reality. For instance, nuclear power may be both highly risky and highly beneficial. Individuals, however, tend to think of nuclear power as highly risky and, *thus*, allocate only *few* benefits. Hence, 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.

According to the privacy calculus literature, individuals are expected to perform a joint valuation of perceived risks and perceived benefits when requested to disclose private information, resulting in an overall assessment of potential losses and gains connected to data provision. Intentions to disclose information, in turn, are seen as a result of this valuation process (Xu *et al.*, 2011b). In conceptualizing a construct that reflects the overall assessment of perceived risks and perceived benefits, some scholars focused on its utility dimension only (Xu *et al.*, 2011b, p. 44). Others, in turn, denoted a much broader impact of privacy valuation processes on one's current mind states by emphasizing the impact of risk and benefit valuations on "an individual's self-

assessed state in which external agents have limiting access to information about him or her" (Dinev *et al.* 2012, p. 5). Aiming to systematically distinguish dispositional factors from situational variables, we adopt this definition of privacy as a state, and define the outcome of the valuation of perceived risks and perceived benefits as the (state of) perceived privacy an individual feels in a concrete data-requesting situation. Stated differently, we predict perceived privacy to constitute an outcome of both perceived risks (Dinev *et al.*, 2012; Xu *et al.*, 2011b) and perceived benefits (Xu *et al.*, 2011b), and hypothesize the current state of perceived privacy to antecede individuals' intentions 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 intentions 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). We account for this distinction by modeling general privacy concerns as an antecedent to a situation-specific risk assessment. Due to 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 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 (Anderson & Agarwal, 2011; Bansal *et al.*, 2010; Dinev & Hart, 2006) 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 since 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 (Anderson & Agarwal, 2011; Dinev & Hart, 2006).

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). For example, Anderson and Agarwal (2011) conceptualized trust in the data-collecting electronic medium as a pre-existing cognitive factor that may be affected by situational variables such as the intended purpose of the disclosed information. 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.

Since prior research suggests that trust is a protective factor that mitigates risk beliefs and privacy concerns (Bansal *et al.*, 2010; Kim *et al.*, 2008; Malhotra *et al.*, 2004), we assume that 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 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.

H5b: The effect of general institutional trust on intention to disclose will be fully mediated by perceived benefits and perceived privacy.

Situational Factors: 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 (Li *et al.*, 2011; Malhotra *et al.*, 2004; 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 to disclose will positively impact perceived risks of information disclosure.

H7b: A higher perceived sensitivity of information to disclose 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). Recent studies by Tsai *et al.* (2011) and Brandimarte *et al.* (2012), for example, 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.

Yet, emotions and affect 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 (1) the interplay of emotional states with risk-enhancing or risk-mitigating factors such as sensitivity of information and (2) design guidelines accounting for users' affect-based valuation of privacy-related stimuli (Wakefield, 2013). This research gap has also been noted by Wakefield (2013): "Experiments that manipulate the extent or depth of information disclosure as well as the level of 'entertainment' or positive affect would clarify the effort websites should take to design and implement positive user experiences".

In contrast, the influence of affect on risk and benefit valuation has been extensively researched in other fields. In consumer behavior research, for example, affect is defined as "a faint whisper of emotion" resulting from an automatically occurring, rough classification of a stimulus into a feeling of either "good" or "bad" (Slovic *et al.*, 2004). Rooted in the work of Zajonc (1980), affect is seen as very first, inevitable evaluation of a stimulus: "We do not see just 'a house': We see a *handsome* house, an *ugly* house, or a *pretentious house*" (Zajonc, 1980, p. 154). This early, automatic emotional assessment is seen as an irreplaceable antecedent of human motivation (Epstein, 1994) and decision-making (Damasio, 1994), especially when deciding under uncertainty or pressure (Finucane *et al.*, 2000).

Furthermore, dual-process models of thinking (e.g. Epstein, 1994; Loewenstein *et al.*, 2001; Reyna, 2004) assume affect-based and rational, rule-based modes of thinking to co-exist, and to interact (Finucane & Holup, 2006). For example, Hsee and Rottenstreich (2004, study 3) asked consumers 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 influences behavioral reactions, yet contextual cues can determine whether consumers rely on affect-based or rule-based modes of thinking.

Prior research in consumer behavior has also shown that valuations of risk and benefits depend on affect. Finucane *et al.* (2000), for example, showed affect to mediate the spurious correlation between risk and benefit perception: 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). Called the *affect heuristic* (Finucane *et al.*, 2000; Slovic *et al.*, 2007), this effect highlights the potential of affect to influence individuals' decision-making and behavior.

In line with this research, we postulate that positive affect will result in a benefit overestimation and a risk underestimation (Slovic *et al.*, 2007), and that users' risks and benefit perceptions will be independent from information sensitivity when relying on affective thinking (Hsee & Rottenstreich, 2004, study 3):

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

<Figure 1 about here>

Building on the foundations described above, Figure 1 depicts our conceptual model. In line with previous research, the intention to disclose personal information is modeled as an outcome of the conjoint assessment of perceived risks and benefits, and assessment in a concrete situation may override dispositional factors like privacy concerns (Dinev & Hart, 2006; Li *et al.*, 2011; Xu *et al.*, 2009). However, we introduce

(1) general institutional trust as an additional dispositional factor and (2) hypothesize positive affect to be capable to override rational assessments of risks and benefits in the situational privacy calculus, implying a biased and irrational risk-benefit valuation. Neutral affect, in contrast, will lead to a differential cognitive evaluation of risks and benefits, only depending on information sensitivity.

METHODOLOGY

Given that several authors (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). More precisely, the application 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 insurance firm receives all data collected by the app. Within this context, the study was conducted as a 2x2 cross-sectional online experiment. Manipulating information sensitivity and affect using product presentation scenarios, we aimed to measure privacy-related constructs adopting scales from prior research.

Development of stimulus material

Since 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. Participants 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 as well as 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 and

Rottenstreich, 2004, study 3). Given the definition of affect as an automatic response towards a stimulus (Slovic *et al.* 2007), we expected cute and appealing screenshots to be equally effective. This is in line with prior research in ergonomics that showed that aesthetically appealing screenshots have the potential to raise positive feelings in users (Sonderegger & Sauer, 2010; Sonderegger *et al.*, 2012). 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-points 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 ($t(101) = 6.00$, $p < .01$, mean difference: 1.47), and the screenshot with the lowest deviation from baseline as neutral-affect manipulation ($t(101) = 1.47$, $p = .14$, mean difference = -0.10). The derived stimulus material for raising positive and neutral affect is depicted in Figure 2.

<Figure 2 about here>

Information Sensitivity

To assess which kinds of personal information are considered more or less sensible 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, 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 ($M = 4.94$, $SD = 2.00$), 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.

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 and Agarwal (2011). Furthermore, we adopted three items from Kim *et al.* (1996) and one item used by Xie *et al.* (2006) for manipulation checks of affect and information sensitivity.

Participants and Procedure

Being aware of cultural differences previously identified by information privacy researchers (Dinev *et al.*, 2006; 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 U.S. 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, study participants were requested to complete a short questionnaire focusing on dispositional factors and relevant control variables, such as general privacy concerns. 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 participants were influenced 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. Finally, participants were asked to fill out another short questionnaire containing situation-specific privacy scales, such as perceived risks of information disclosure or the intention to disclose personal information.

RESULTS

In total, 480 participants completed the study. In both subsamples, we eliminated cases that showed response patterns or implausible short handling times (< 5 minutes), resulting in a total sample size of 442 participants (186 from the U.S. and 228 from Switzerland). Mean age was 31.24 (SD = 10.19) for U.S. and 34.32 (SD = 14.23) for Swiss participants ($t(405.52) = -2.56$, $p < .05$), with a larger proportion of males in the U.S. sample (60% compared to 40% among Swiss participants, $\chi^2(1, N = 414) = 7.62$,

$p < .01$). With regard to the used privacy-related scales, the averaged means of American and Swiss participants did not differ in four of six cases. However, U.S. participants indicated to have a higher general institutional trust ($t(412) = 3.43$, $p < .01$) and perceived higher benefits connected to data provision ($t(412) = 2.77$, $p < .01$). Table 1 shows the mean scores and standard deviations of the deployed scales.

<Table 1 about here>

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 ($t(412) = -2.78$, $p < .01$) and highly significant overall differences of affect ratings between participants in the neutral and positive affect condition ($t(412) = -3.12$, $p < .01$).

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 zero and latent variances to one. Following the two-step methodology suggested by Segars and Grover (1993), we first conducted confirmatory factor analyses (CFA) to analyze 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

Due to the cross-national nature of the overall sample, we started with measurement invariance[1] testing in order to ensure comparability of the samples from different populations. As suggested by many scholars (MacKenzie *et al.*, 2011; Steenkamp & Baumgartner, 1998; Teo *et al.*, 2009; van de Schoot *et al.*, 2012; Vandenberg & Lance, 2000), 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/df as an indicator of overall model fit as the χ^2-test is known to

[1] 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.

become more conservative as sample sizes increase. According to Carmines and 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 from 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)[2] to compare model 1 to the baseline model. Since 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 the 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 U.S. sample and $\lambda = 0.47$ for the Swiss sample). As a SBS-χ^2 between this new model (model 1a) and model1 was insignificant, we concluded that partial metric invariance could be established.

<Table 2 about here>

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 due to 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. Since, 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

[2] 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

invariance analysis. That is, we used Model1a as the most appropriate measurement model for further investigation.

Reliability, Validity and Common Method Variance

In a next step, we inspected reliability and validity coefficients of the measurement model. Results for the Swiss and U.S. sample can be obtained from 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 .69, all scales exceeded the recommended thresholds of .70 for Cronbach's α and composite reliability (Gefen *et al.*, 2000). Apart from the mentioned scale, all composite reliability coefficients were even above .80, indicating strong internal consistency (Koufteros, 1999). 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.

<Table 3 about here>

Convergent validity of the measurement model was tested by two approaches: First, we analyzed the factor loadings and t-values of all indicators. As illustrated in Table 3, all indicators exceeded factor loadings of .70 and showed highly significant t-values. Second, we calculated the average variances extracted (AVEs) for each scale. Except for the general privacy concerns scale in the Swiss sample, AVEs were above the recommended threshold of .50 (Fornell & Larcker, 1981) for all constructs, indicating that convergent validity was largely supported by the data. Discriminant validity was assessed by analyzing 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.

<Table 4 about here>

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* = .97, *TLI* = .97, *RMSEA* = .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 $\lambda_{TRUST1} = .00$, $p = .92$ in the U.S. sample and $\lambda_{TRUST1} = .16$, $p = .43$ in the Swiss sample).

Structural Model and Hypothesis Testing

In order to retain the final structural model, we included experimental condition variables. Although applied rarely, dichotomous variables such as experimental conditions may be included in SEM the same way they can be included in regression analysis, allowing for simultaneous modeling of variable relationships and group differences (Muller *et al.*, 2005). 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 model fit to the data ($\chi^2 = 585.50$, $df = 408$, $\chi^2/df=1.44$, *CFI* = .97, *TLI* = .96, *RMSEA* = .046), with mostly significant and highly comparable path coefficients and large coefficients of explained variance in both samples (see Table 5).

<Table 5 about here>

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 U.S. sample, indicating that predominant antecedents of the intention to disclose information have been covered.

Dispositional Factors: Privacy Concerns and Institutional Trust

With regard to hypotheses H5b and H6b, 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 to 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. Dinev & Hart, 2006). Although model estimation yielded significant impacts of concerns and trust on the intention to disclose in both samples (U.S. sample: $\gamma_{concerns} = -.34$, $p < .01$, $\gamma_{trust} = .27$, $p < .01$; Swiss sample: $\gamma_{concerns} = -.31$, $p < .01$, $\gamma_{trust} = 22$, $p < .01$), all path

coefficients were lower than the path 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* = .97, *TLI* = .97, *RMSEA* = .067), and the explained variance of intention to disclose was low with 19% of explained variance in the U.S. sample and 15% of explained variance in the Swiss sample.

<Table 6 about here>

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, only one of four direct effects was marginally significant, while total and specific indirect paths yielded significant outcomes in all 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 U.S. sample. Therefore, we concluded that H5b and H6b were mainly supported by the data.

Situational Factors: Information Sensitivity and Affect

In hypotheses H7a, H7b, H8a and H8b, 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 due to risk underestimation and benefit overestimation.

<Figure 3 about here>

With regard to risk perception, we found a significant main effect of information sensitivity in the U.S. sample and a significant interaction effect of information sensitivity and affect (see Table 5): Participants in the high sensitivity condition generally tended to rate risks higher by 0.20 standard deviations ($p < .05$). For participants in the positive affect and high information sensitivity condition, however, the expectation value decreased by -0.24 standard deviations ($p < .05$), approximating the expectation value of 0.07 standard deviations 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 standard deviations in the Swiss sample between low and high sensitivity conditions ($p < .06$), indicating a

general increase in risk perception for participants in the high information sensitivity condition. As reflected by a significant interaction effect ($p < .05$), the expectation value for participants in the positive affect and high information sensitivity condition (0.15 standard deviations) was comparable to the expectation value for participants in the positive affect and low information sensitivity condition (0.20 standard deviations), 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 to 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 standard deviations ($p < .01$). 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 U.S. sample. Compared to the low sensitivity condition, participants in the high sensitivity condition showed lower ratings of perceived benefits (expectation value of -0.24 standard deviations across conditions, $p < .01$). However, further effects could not be identified. As a result, we concluded that hypotheses H7a and H8a were supported by the data, while we only found partial support for hypothesis H7b, and no support for hypothesis H8b.

DISCUSSION

In our study, we embraced two extensions to the basic privacy calculus model by designing and conducting an experiment that systematically manipulated affective thinking in a privacy-related situation, while simultaneously distinguishing dispositional tendencies from situational constructs. In data acquisition and analysis, we relied on two samples from the U.S. and Switzerland in order to emphasize the cross-cultural validity of the deployed methodology and revealed findings.

Results indicated differences between the U.S. and the Swiss sample with regard to demographics, privacy-related constructs, and psychometric properties of the underlying measurement model. Despite these inconsistencies, however, the data largely supported the hypothesized relationships and group differences in *both* samples, supporting the generalizability of our findings.

Concerning the distinction between dispositional factors and situation-specific privacy valuations, we found the relationship of dispositional tendencies and intentions to disclose to be fully mediated by situational calculus variables in three of four cases. In accordance with expectations, these results indicate that a situation-specific privacy calculus has the potential to override dispositional tendencies in privacy-related

decision-making, implying situation-specific considerations to dominate pre-existing attitudes.

Moreover, our experimental approach revealed affective thinking to constitute a factor that guides irrational valuation of perceived risks: In both samples, we found a significant interaction effect of experimental conditions on perceived risks of information disclosure, indicating that individuals underestimate risks when confronted with a cue that designates positive affect. In contrast, participants under neutral affect conditions were found to value perceived risks in a rational way.

Apart from these findings, our study confirmed the validity of the privacy calculus as a theoretical framework for investigations of privacy-related decision-making. As indicated by highly significant, negative relationships between risks and benefits in both samples, our data strongly supported the assumption of risks and benefits to constitute interdependent factors, a relationship rarely accounted for in prior research (Dinev *et al.*, 2012). Furthermore, we conceptualized perceived privacy as the main outcome variable of the joint assessment of perceived risks and perceived benefits, and as a construct anteceding intentions to disclose. Strong relationships between correspondent variables as well as high ratios of explained variances of perceived privacy in both samples confirmed these hypothesized relationships. Overall, our model fitted the data well and accounted for 58% of explained variance of the main outcome variable in the U.S., respectively 50% in the Swiss sample. Theoretical and practical implications of these findings are discussed below.

Theoretical Implications

Defining the privacy calculus as a *situation-specific* trade-off of privacy-related risk and benefit perceptions, *bounded* by dispositional tendencies and irrational behavior, we uniquely add to existing literature in at least three ways:

First, our experimental approach yielded evidence on the impact of affective thinking on privacy-related decision-making. Although prior research has recently started to measure pre-existing affects and emotion and analyze their impact in the context of information privacy (Anderson & Agarwal, 2011; Pengnate & Antonenko, 2013), there has been no attempt to demonstrate their overriding effects using a strong, experimental approach (Wakefield, 2013). By showing that affective thinking, as induced by affect-raising screenshots, impacts individuals' risk perceptions, we contribute to the understanding of contextual preconditions that determine privacy-related reasoning and decision-making (Bélanger & Crossler, 2011; Smith *et al.*, 2011).

Second, our findings extend the proposition of a possible distinction between dispositional tendencies and situational privacy-related constructs (Li *et al.*, 2011) in at

least two important ways: First, we found evidence that other dispositional tendencies, such as general institutional trust, may provoke similar effects with regard to the intention to disclose, implying individuals' trust beliefs may be dominated by situational variables in a similar vein as individuals' privacy concerns. Second, our findings indicate the relationship between dispositional tendencies and the intention to disclose information to be *fully* mediated by a situational calculus. These findings contradict earlier work that proposed *partial* mediation between general privacy concerns and disclosing intentions (Li *et al.*, 2011; Wilson & Valacich, 2012). We suppose these inconsistencies to result from the methodological approach chosen: While earlier studies usually measured dispositional tendencies *after* introducing the context or product of investigation (Anderson & Agarwal, 2011; Dinev & Hart, 2006; Hu *et al.*, 2010; Li *et al.*, 2011; Xu *et al.*, 2011a), we systematically distinguished dispositional tendencies from situational variables by assessing them *before* experimental manipulation. Relying on studies on cognitive priming (DeCoster & Claypool, 2004), we propose our methodological approach to more thoroughly emphasize the dispositional nature of general privacy concerns and general institutional trust. Given that earlier studies have inconsistently modeled disclosure behavior in the privacy calculus framework, e.g. as an outcome of privacy concerns and institutional trust (Dinev & Hart, 2006), privacy control and privacy risks (Xu *et al.*, 2011a), or perceived risks and perceived relevance (Knijnenburg *et al.*, 2013), the conceptual and methodological separation of dispositions and situational factors may help scholars to better understand and investigate the exact interplay of privacy-related constructs.

Third, our research adds to the understanding of discrepancies between reported privacy concerns and behavioral intentions, denoted as the *privacy paradox* (Norberg *et al.*, 2007; Xu *et al.*, 2011b). 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). Others, in contrast, have made attempts to explain these inconsistencies by proposing extensions or modifications to the predominant research models, arguing that discrepancies may be determined by "affective and cognitive factors and their relationships at a specific level over and above that of general privacy concern" (Li et al. 2011, p . 9). In line with the latter argumentation, our research 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 to 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). Given that behaviors generally follow intentions (Ajzen, 1985), 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 & Krishnan, 2006; Van Slyke *et al.*, 2006).

Practical Implications

The results of this research also have important managerial and public policy implications. In this regard, 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 regarding the role of affect are also of relevance to public policy decisions. In this regard, our results show that consumers experiencing positive affect may agree to disclose information that they may not agree to disclose in a more balanced affective state. This finding may help to explain why consumers frequently disclose very personal information on Web 2.0 and social media applications such as Facebook or Google+. Since these applications are mostly focused on recreational purposes, consumers may frequently experience positive affect while using these applications and may thus fail to fully understand how and to what extent their personal information is used for targeted advertising. Against this background, policy makers may attempt 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, 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. 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), or more realistic stimuli (such as an ongoing interaction with a product, Wakefield, 2013) may result in more theory-accordant reactions.

Second, our research focused on positive affect, considering the elicitation of positive affect to be a more common goal in product design (Zhang, 2007). However, future research may investigate whether induced negative affect provokes similar effects. Anxiety, for example, is known to inhibit rational considerations of risks, resulting in risk overestimation (Nesse & Klaas, 1994).

Third, our study focused on one particular decision heuristic, namely the affect heuristic. However, knowledge on the role of other cognitive heuristics capable to guide privacy-related decisions is scarce, despite an increasing number of studies that emphasize the impact of irrationality in the context of information privacy (Acquisti & Grossklags, 2008; Brandimarte *et al.*, 2012; Tsai *et al.*, 2011). Hence, our work may encourage other researchers to more intensively explore heuristic thinking and decision-making in the context of information privacy (for a review on heuristic decision-making, see Gigerenzer and Gaissmaier, 2011).

Fourth, we have discussed the significance of the privacy paradox as an attitude-intention rather than an intention-behavior gap. Similar to most of the research in information privacy (Smith *et al.*, 2011), however, our research relied on intentions as main outcome. As such, research incorporating pre-existing attitudes, intentions and actual disclosure behavior is needed in order to further investigate the nature of the privacy paradox.

Fifth, our study was planned and conducted as a cross-sectional experiment. An understanding of general privacy concerns and general institutional trust as dispositional tendencies, however, raises the question on their stability, or instability, over time and situations. Stated differently, an individual's dispositional tendencies should administer similar influence in different situations and remain relatively stable over time in order to be considered truly "dispositional". Yet, longitudinal studies that analyze the dynamics of privacy-related constructs over time are scarce in information privacy research (see Milne and Culnan, 2002, for one of the few exceptions). Relying on our work, future research may therefore intensify efforts to explore the nature of privacy-related decisions from a longitudinal perspective, too.

Considering these aspects, the contributions of our study lay a fruitful ground for further work that strives to investigate the dynamics of privacy-related decision-making and thus deepen our theoretical and practical understanding of when and why individuals disclose (or not disclose) personal information.

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., & Grossklags, J. (2005) Privacy and Rationality in Individual Decision-Making. *IEEE Security & Privacy,* **3**, 26-33.

Acquisti, A., & Grossklags, J. (2008). What Can Behavioral Economics Teach Us About Privacy? In: *Ditigal Privacy - Theory, Technologies, and Practices,* Acquisti, A., Gritzalis, S., Lambrinoudakis, C. & de Capitani di Vimercati, S. (Eds.). Auerbach Publications, Boca Raton, USA.

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.

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.

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.

Culnan, M. J., & Armstrong, P. K. (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science,* **10**, 104-115.

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

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., 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.

Finucane, M. L., & Holup, J. L. (2006) Risk as Value: Combining Affect and Analysis in Risk Judgments. *Journal of Risk Research,* **9**, 141-164.

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*, 39-50.

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*.

Gefen, D., Straub, D. W., & Rigdon, E. E. (2011) An Update and Extension to Sem Guidelines for Admnistrative and Social Science Research. *MIS Quarterly,* **35**, iii-xiv.

Gigerenzer, G., & Gaissmaier, W. (2011) Heuristic Decision Making. *Annual Review of Psychology,* **62**, 451-482.

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.

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, Orlando*.

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.

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.

Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013) Counteracting the Negative Effect of Form Auto-Completion on the Privacy Calculus. *Proceedings of the 34rd International Conference on Information Systems*.

Koufteros, X. A. (1999) Testing a Model of Pull Production: A Paradigm for Manufacturing Research Using Structural Equation Modeling. *Journal of Operations Management,* **17**, 467-488.

Krasnova, H., Veltri, N. F., & Gunther, O. (2012) Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture Intercultural Dynamics of Privacy Calculus. *Business & Information Systems Engineering,* **4**, 127-135.

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.

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.

Muller, D., Judd, C. M., & Yzerbyt, V. Y. (2005) When Moderation Is Mediated and Mediation Is Moderated. *Journal of Personality and Social Psychology,* **89**, 852.

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

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*.

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.

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

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.

Steenkamp, J.-B. E. M., & Baumgartner, H. (1998) Assessing Measurement Invariance in Cross-National Consumer Research. *Journal of Consumer Research,* **25**, 78-107.

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.

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, 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., 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.

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.

Zajonc, R. B. (1980) Feeling and Thinking - Preferences Need No Inferences. *American psychologist,* **35**, 151-175.

Zhang, P. (2007). Toward a Positive Design Theory: Principles for Designing Motivating Information and Communication Technology. 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. Emerald Group Publishing Limited.

FIGURES AND TABLES

Figure 1. Conceptual Model.

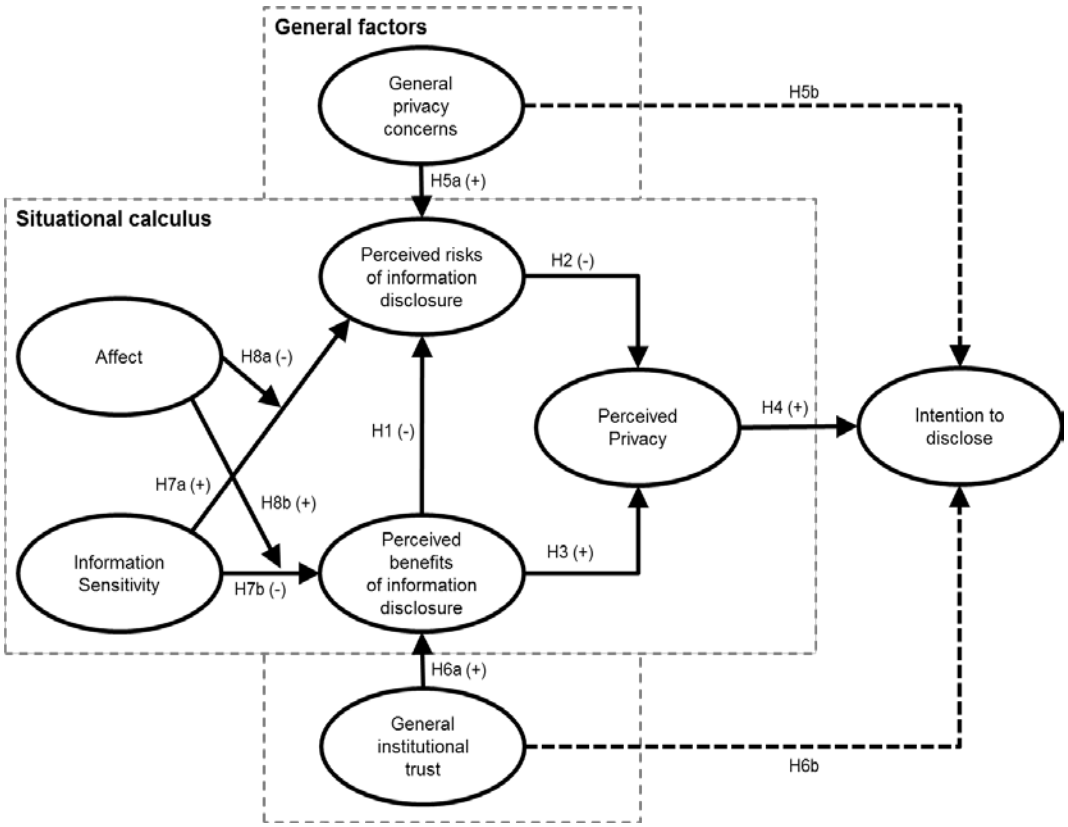
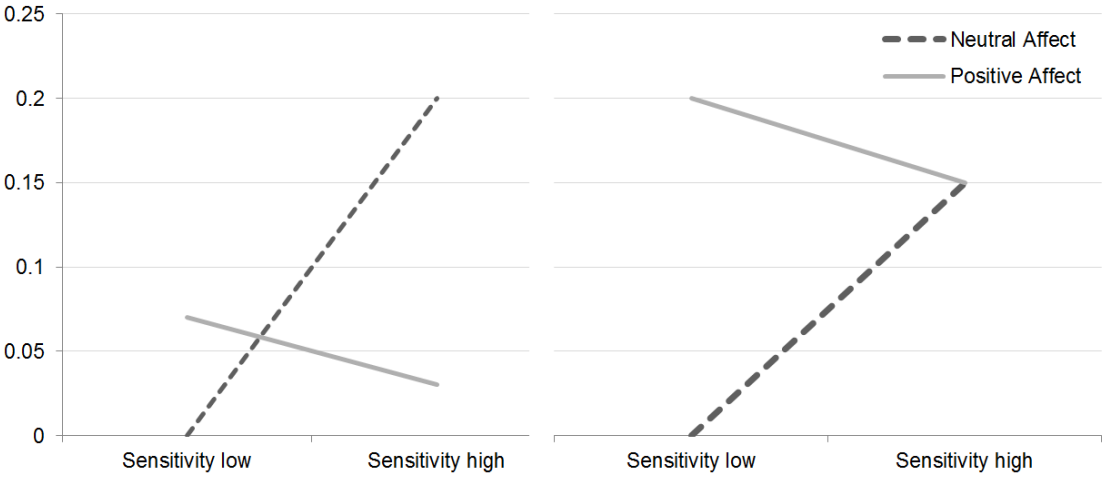


Figure 2. Screenshots inducing (a) neutral affect and (b) positive affect.

(a) (b)

Note: The original screenshots were colored.

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



(a) (b)

Table 1. Descriptive Statistics of the constructs

Construct	U.S. 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

** $p < .01$

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	.97	.97	.047	-	-	Accept
Model1	437.09	293	1.49	.97	.96	.049	Model1 vs. Model0	43.26 (18) $p < .01$	Decline
Model1a	414.98	292	1.42	.97	.97	.045	Model1a vs. Model0	15.16 (18) $p = .65$	Accept
Model2	509.54	311	1.64	.96	.95	.056	Model2 vs. Model1a	55.89 (16) $p < .01$	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^2-Test.

Table 3. Confirmatory Factor Analysis Statistics.

U.S. Sample

Latent Variable	Item	CONC α = .84	TRUST α = .82	RISK α = .91	BEN α = .84	PRIV α = .93	WILL α = .98	*t-value*	R^2	Composite Reliability	AVE
CONC	CONC1	.77						23.61	.63	.83	.62
	CONC2	.73						21.16	.63		
	CONC3	.88						25.39	.60		
TRUST	TRUST1		.79					19.76	.60	.84	.64
	TRUST2		.80					20.57	.54		
	TRUST3		.78					25.10	.77		
RISK	RISK1			.87				41.32	.76	.88	.71
	RISK2			.93				44.91	.86		
	RISK3			.77				26.32	.59		
	RISK4			.83				34.06	.69		
BEN	BEN1				.78			20.70	.61	.84	.63
	BEN2				.80			19.17	.63		
	BEN3				.81			17.47	.65		
PRIV	PRIV1					.89		38.41	.79	.92	.80
	PRIV2					.92		47.05	.84		
	PRIV3					.87		28.62	.76		
INT	INT1						.96	99.12	.91	.97	.93
	INT2						.97	108.41	.94		
	INT3						.97	102.07	.94		

Swiss Sample

Latent Variable	Item	CONC α = .69	TRUST α = .88	RISK α = .92	BEN α = .82	PRIV α = .90	WILL α = .96	*t-value*	R^2	Composite Reliability	AVE
CONC	CONC1	.76						19.19	.58	.71	.46
	CONC2	.76						18.79	.58		
	CONC3	.47						5.83	.22		
TRUST	TRUST1		.83					27.37	.69	.88	.71
	TRUST2		.82					18.75	.67		
	TRUST3		.88					37.77	.77		
RISK	RISK1			.88				40.81	.77	.88	.72
	RISK2			.90				47.11	.82		
	RISK3			.81				27.38	.65		
	RISK4			.82				32.98	.68		
BEN	BEN1				.80			24.71	.63	.82	.61
	BEN2				.78			21.55	.61		
	BEN3				.76			17.57	.58		
PRIV	PRIV1					.84		26.83	.71	.91	.77
	PRIV2					.92		54.42	.84		
	PRIV3					.88		32.41	.77		
INT	INT1						.95	59.93	.90	.97	.91
	INT2						.94	93.71	.89		
	INT3						.97	95.04	.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 (AVE) for each construct.

	U.S. Sample					
	CONC	TRUST	RISK	BEN	PRIV	INT
CONC	.64					
TRUST	-.32** (0.09)	.62				
RISK	.47** (0.07)	-.22* (0.09)	.71			
BEN	-.13 (0.10)	.28** (0.10)	-.50** (0.07)	.63		
PRIV	-.33** (0.07)	.33** (0.08)	-.75** (0.04)	.68** (0.07)	.80	
INT	-.36** (0.06)	.31** (0.07)	-.65** (0.05)	.62** (0.06)	.71** (0.04)	.93
	Swiss Sample					
	CONC	TRUST	RISK	BEN	PRIV	INT
CONC	.46					
TRUST	-.07 (0.10)	.71				
RISK	.62** (0.07)	-.31** (0.07)	.72			
BEN	-.38** (0.09)	.45** (0.07)	-.58** (0.07)	.61		
PRIV	-.45** (0.08)	.51** (0.06)	-.78** (0.03)	.77** (0.05)	.77	
INT	-.36** (0.08)	.27** (0.07)	-.67** (0.05)	.69** (0.06)	.71** (0.05)	.91

Note: The diagonal terms indicate the average variance extracted (AVE), non-diagonal terms indicate correlations, 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,
* $p < .05$, ** $p < .01$.

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

		U.S. Sample		Swiss Sample	
		Path Coefficient (SE)	R^2	Path Coefficient (SE)	R^2
H1	BEN → RISK	-.50** (0.07)		-.44** (0.08)	
H2	RISK → PRIV	-.56** (0.08)		-.50** (0.06)	
H3	BEN → PRIV	.46** (0.09)		.51** (0.06)	
H4	PRIV → INT	.70** (0.05)		.72** (0.05)	
H5a	CONC → RISK	.44** (0.07)		.50** (0.07)	
H5b	CONC → INT	-.13^ (0.07)		-.04 (0.07)	
H6a	TRUST → BEN	.34** (0.09)		.47** (0.06)	
H6b	TRUST → INT	.07 (0.07)		-0.08 (0.07)	
H7a	SENS → RISK	.20* (0.10)		.15^ (0.08)	
	AFF → RISK	.07 (0.10)		.20** (0.08)	
H8a	AFFxSENS → RISK	-.24* (0.11)		-.20* (0.10)	
H7b	SENS → BEN	-.24* (0.11)		-.05 (0.09)	
	AFF → BEN	-.19 (0.11)		-.03 (0.09)	
H8b	AFFxSENS → BEN	.02 (0.15)		.02 (0.11)	
	RISK		.48** (0.06)		.47** (0.06)
	BEN		.19** (0.07)		.22** (0.05)
	PRIV		.77** (0.04)		.74** (0.04)
	INT		.58** (0.04)		.50** (0.05)

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; AFFxSENS: Interaction effect affect and information sensitivity

^ $p < .06$; * $p < .05$; ** $p < .01$.

Table 6. Tests of total, direct and indirect effects.

	U.S. 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. ** $p < .01$. ^ $p = .045$.

APPENDIX

Appendix 1: Questionnaire

Construct / Items	Scale	Origin
General Privacy Concerns	Likert 1-7	Malhotra *et al.* (2004)
Compared to others, I am more sensitive about the way smartphone apps handle my personal information.	(1 = totally disagree, 7 = totally agree)	
To me, it is the most important thing to keep my privacy intact from smartphone apps. (reverse coded)		
In general, I am very concerned abouth threats to my personal privacy.		
General Institutional Trust	Likert 1-7	Malhotra *et al.* (2004)
Smartphone apps are trustworthy in handling client data.	(1 = totally disagree, 7 = totally agree)	
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)
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	Dinev *et al.* (2012)
It would be risky to give personal information to the smartphone app.	(1 = totally disagree, 7 = totally agree)	
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 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.	Likert 1-7 (1 = totally disagree, 7 = totally agree)	Dinev *et al.* (2012)
Perceived Privacy 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.	Likert 1-7 (1 = totally disagree, 7 = totally agree)	Dinev *et al.* (2012)
Intention to disclose Please specify the extent to which you would reveal your personal information to use the smartphone app: willing/unwilling unlikely/likely not probable/probable	Semantic differential	Anderson and Agarwal (2011)

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, distance travelled) 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.

Conflict of Interest Statement

No conflicts of interest have been declared.

Source of Funding

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