RETHINKING THE PRIVACY CALCULUS: ON THE ROLE OF DISPOSITIONAL FACTORS AND AFFECT

Research-in-Progress

Flavius Kehr
University of St. Gallen
Chair of Operations Management
Dufourstrasse 40A
9000 St. Gallen, Switzerland
flavius.kehr@unisg.ch

Daniel Wentzel
RWTH Aachen University
Chair of Marketing
Kackertstrasse 7
52072 Aachen, Germany
dw@lum.rwth-aachen.de

Peter Mayer
Business Engineering Institute St. Gallen AG
Holzstrasse 39
9001 St. Gallen, Switzerland
peter.mayer@bei-sg.ch

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. However, scholars have recently challenged two basic propositions of the privacy calculus model. First, some authors have distinguished between general and situational factors in the context of privacy calculus and have argued that perceived risks and perceived benefits are primarily related to a situation-specific privacy assessment. Second, a growing body of literature has argued that rational considerations in privacy assessment are bounded by limited resources or heuristic thinking. In this research, we address both of these issues and develop a conceptual model that suggests (1) that dispositional factors such as privacy concerns and institutional trust may affect situation-specific privacy calculus and (2) that privacy assessment may also be determined by momentary affective states.

Keywords: Privacy/information privacy, consumer behavior, consumer decision-making, 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 and Armstrong 1999; Dinev and 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 and Gefen 2004). Entitled the *privacy calculus* (Culnan and Armstrong 1999), this privacy trade-off has been extensively researched in several contexts, such as e-commerce (Dinev and Hart 2006), the Internet (Dinev et al. 2012; Malhotra et al. 2004), mobile applications (Xu et al. 2009), or Internet of Things Services (Kowatsch and Maass 2012). Also, numerous factors increasing or mitigating risk and benefit perceptions have been identified, e.g. financial rewards (Xu et al. 2011), personalization (Xu et al. 2011) or sensitivity of information to disclose (Li et al. 2011).

However, scholars have recently challenged two basic propositions of the privacy calculus model: First, some authors (Li et al. 2011; Wilson and Valacich 2012) have distinguished between general and situational factors in the context of privacy calculus and have argued that perceived risks and perceived benefits are primarily related to a situation-specific privacy assessment. Second, a growing body of literature doubts the proposition of rationality in the privacy calculus, stating that rational considerations are bounded by limited resources or heuristic thinking (Acquisti and Grossklags 2005; Brandimarte et al. 2013; Tsai et al. 2011). Embracing both aspects as valid extensions to the basic model, we propose the privacy calculus to be 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 general factors impacting the situation-specific 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, and will analyze its importance in the context of information privacy.

In the following, we will first review pertinent research streams and will develop our conceptual model and the accompanying hypotheses. Next, we will describe an experiment that is designed to test our model. Finally, we will briefly describe the implications that may follow from our work.

Theoretical Background

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 and Valacich 2012 p. 6). Intentions to disclose information, in turn, are seen as a result of a rational, independent assessment of perceived risks and perceived benefits (Culnan and Armstrong 1999).

However, prior research has also pointed to discrepancies between reported privacy concerns and behavioral intentions, denoted as the *privacy paradox* (Li et al. 2011; Norberg et al. 2007; Xu et al. 2011). That is, users tend to disclose their data "as if they didn't care" (Dinev and Hart 2006, p. 76), even if they report to be highly worried about potential data misuse (Norberg et al. 2007). As a possible explanation, recent research has distinguished general factors from a situation-specific privacy assessment, arguing that (1) privacy concerns have been mostly measured on a global level and (2) situation-specific considerations may override general attitudes and tendencies (Li et al. 2011; Wilson and 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).

Furthermore, research has also found that users may disclose their data in exchange for very small rewards or discounts (Acquisti 2004). From a fully rational viewpoint, however, an increase in disclosing intentions or behavior is expectable if, and only if, the sum of perceived benefits in a concrete situation outweighs the sum of all perceived risks. Thus, 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 and Grossklags 2005; Acquisti 2009), bounded rationality (Keith et al. 2012) or the attempt for immediate gratification (Acquisti 2004; Wilson and Valacich 2012).

Unifying both research streams, our work offers a first attempt to clarify the interplay of irrational, situation-specific behavior and dispositional tendencies in privacy-related decision making. Specifically, we will examine the role of privacy concerns and institutional trust as general dispositional factors, while also considering the role of affective states in situation-specific privacy assessment.

General Factors: Privacy Concerns and Institutional Trust

As discussed earlier, inconsistencies in the relationship between privacy concerns and behavior (denoted as the privacy paradox, Norberg et al. 2007) may be explained by a distinction between general and situational factors: While most studies have focused on *general* privacy concerns – an "individual's general tendency to worry about information privacy" (Li et al. 2011, p. 5) – situation-specific factors may override dispositional tendencies and persuade individuals to disclose their information despite general worries (Li et al. 2011; Wilson and Valacich 2012). Based on this conceptual distinction, one may postulate that there are further dispositional factors that shape privacy assessments in a similar vein as general privacy concerns.

As such, institutional trust refers to an individual's confidence that the data-requesting stakeholder or medium will not misuse his or her data (Anderson and Agarwal 2011; Bansal et al. 2010; Dinev and 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 and 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 and Agarwal 2011; Dinev and Hart 2006).

Yet, most studies have measured institutional trust in *general* terms, referring to the degree of general confidence in the internet (Dinev and 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 beliefs about the stakeholder requesting the information. Similar to general privacy concerns, institutional trust may thus be considered as a *general* tendency to have confidence in the data-collecting medium (or institution), subject to interference by a situation-specific privacy calculus. This conceptualization may help to clarify the role of trust in information privacy and may also deepen our understanding of the relationship between general and situational factors in the privacy calculus.

Affects and Privacy

A growing body of literature suggests that rational considerations in the context of privacy-related decision making may be affected by psychological limitations such as the inability to process all information relevant to the cost-benefit-ratio (Acquisti and Grossklags 2005; Acquisti 2009) or the attempt for immediate gratification (Acquisti 2004; Wilson and Valacich 2012). Recent studies by Tsai et al. (2011) and Brandimarte et al. (2013), 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.

However, emotions and affect have played minor roles in research on information privacy (Nyshadham and Castano 2012). Scholars have only recently started to measure pre-existing emotional states and correlate them with constructs like intention to disclose information (Anderson and Agarwal 2011), risk belief (Li et al. 2011), or trust (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 affects 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. 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 affective states on risk and benefit valuation has been extensively researched in other fields. In consumer behavior research, for example, affects are 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), affects are seen as very first, inevitable evaluations 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 and 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, affects influence behavioral reactions, and contextual cues (such as the presence or absence of cute panda pictures) 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 affective states. Fischhoff et al. (1978) showed that anxiety drives public perception of hazards such as alcoholic beverages, handguns, or nuclear power. Also, they 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. Finucane et al. (2000) 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, whereas the reverse is true for negative affect (Finucane and Holup 2006). Called the *affect heuristic* (Finucane et al. 2000; Slovic et al. 2007), this effect highlights the potential of affective states to influence individuals' decision making and behavior. In this research, we adopt these findings and postulate that affective states also have the potential to override rational considerations in the situation-specific privacy assessment.

Theoretical Model and Hypotheses

Building on the foundations described above, Figure 1 depicts our theoretical model. In line with previous research, the intention to disclose personal information is modeled as an outcome of the perceived risks and benefits resulting from data disclosure, and assessment in a concrete situation may override dispositional factors like privacy concerns (Dinev and Hart 2006; Li et al. 2011; Xu et al. 2009). However, we introduce (1) general institutional trust as an additional general factor and (2) affective states as an additional situational factor capable of overriding rational considerations (Hsee and Rottenstreich 2004).

General Factors in the Privacy Calculus Model

Intentions to disclose personal information are usually seen as a result of a rational, joint assessment of perceived risks and perceived benefits of privacy disclosure. 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), yet findings in behavioral economics suggest that risk and benefit perceptions are correlated negatively in individuals' minds (Finucane et al. 2000; Fischhoff et al. 1978). Arguably, these findings will also apply in a privacy context. As also suggested by recent IS literature (Dinev et al. 2012), we hence conceptualize perceived risks and benefits to be interdependent, with perceived benefits mediating the

relationship between privacy calculus antecedents and perceived risks of privacy disclosure.

Apart from this modification, we follow prior research stating that (1) users are more likely to disclose personal information when they perceive potential value from disclosure and (2) users are more likely to disclose personal information when they perceive fewer risks associated with disclosure (Dinev and Hart 2006; Li et al. 2011; Xu et al. 2009).

> *H1: Perceived benefits of privacy disclosure will be negatively associated with perceived risks of privacy disclosure.*
> *H2: Perceived risks of privacy disclosure will be negatively associated with intention to disclose information.*
> *H3: Perceived benefits of privacy disclosure will be positively associated with intention to disclose information.*

Furthermore, we have discussed the distinctive influence of general and situational factors in a model of privacy calculus: While most studies have focused on *general* privacy concerns, situation-specific factors may override dispositional tendencies and persuade individuals to disclose their information despite general worries (Li et al. 2011; Wilson and Valacich 2012). We account for this distinction by modeling general privacy concerns as an antecedent to situation-specific risk assessment. In line with prior research (Li et al. 2011; Wilson and Valacich 2012), we also assume that situation-specific risk assessment only *partially* mediates the negative association between general privacy concerns and the intention to disclose information.

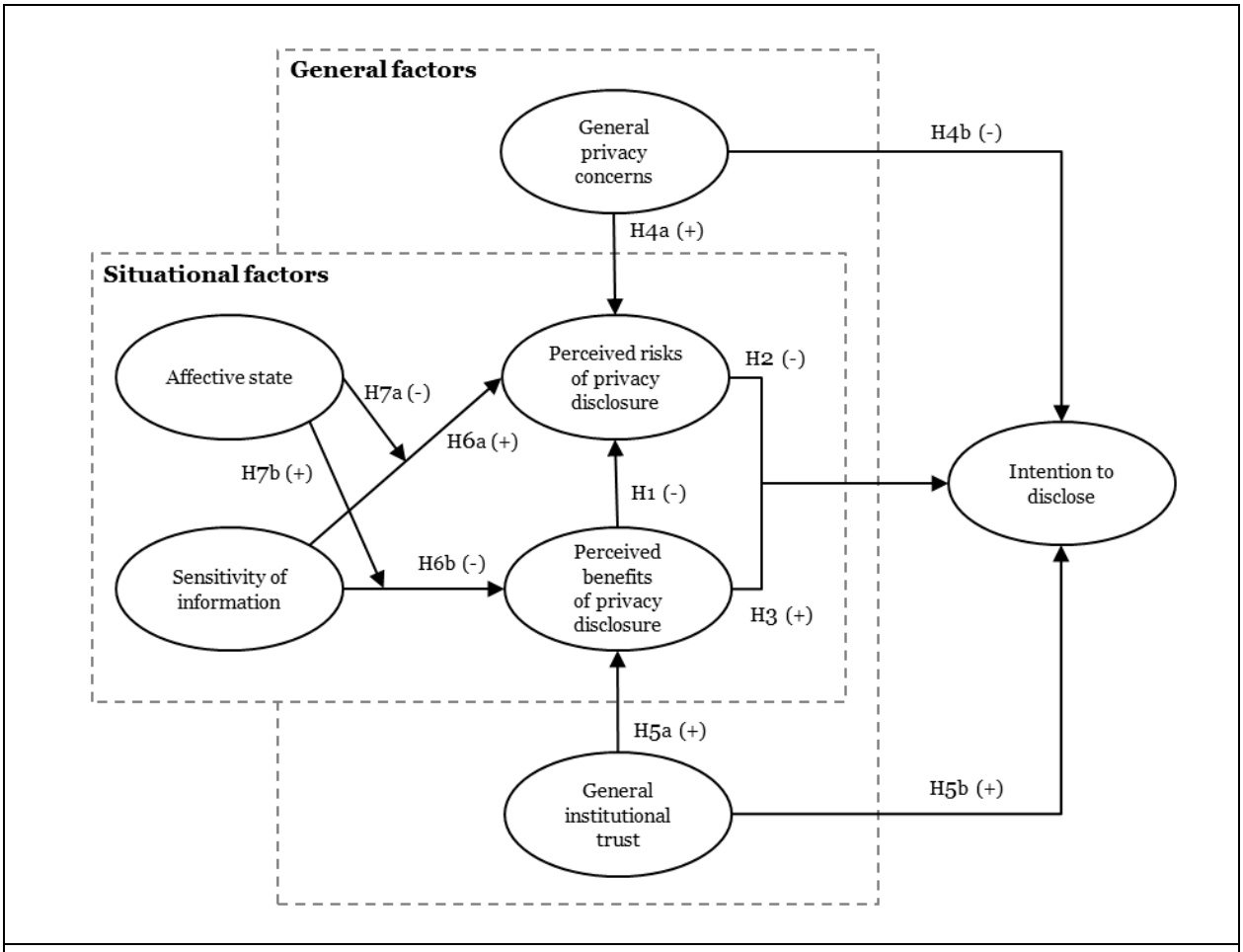

Figure 1. Theoretical Model

Moreover, we have argued that institutional trust constitutes a second general factor, subject to interference by situation-specific privacy valuation. 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. However, we also believe that users will rely on general *and* situation-specific factors when assessing their intentions to disclose information. Therefore, we hypothesize perceived benefits of privacy disclosure to only partially mediate the relationship between institutional trust and intentions to disclose.

H4a: General privacy concerns will be positively associated with perceived risks of privacy disclosure.
H4b: General privacy concerns will be negatively associated with the intention to disclose information.
H5a: General institutional trust will be positively associated with perceived benefits of privacy disclosure.
H5b: General institutional trust will be positively associated with the intention to disclose information.

Situational Factors in the Privacy Calculus Model

While the previous hypotheses indicate that dispositional factors affect intentions to disclose information, we also postulate that situational factors may override these general tendencies. As such, prior research has identified numerous factors that may determine the joint assessment of perceived risks and perceived benefits of privacy 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 a primarily cognitive evaluation of potential losses connected to the provision of *this* (special) information.

H6a: A higher perceived sensitivity of information to disclose will positively impact perceived risks of privacy disclosure.
H6b: A higher perceived sensitivity of information to disclose will negatively impact perceived benefits of privacy disclosure.

Dual-process models of thinking, however, postulate an experiential (affect-driven) and a rational (rule-based) mode of thinking to co-exist and to interact (Epstein 1994; Finucane and Holup 2006). Furthermore, the affect heuristic (Slovic et al. 2007) suggests that affective states may influence valuation of risks and benefits, and rule-based or affect-based thinking may be induced by providing suitable contextual cues (e.g. pictures of cute panda bears, Hsee and Rottenstreich 2004, study 3). In line with this research, we postulate that a positive affective state will result in a benefit overestimation and a risk underestimation (Slovic et al. 2007), regardless of how sensitive the information is perceived.

H7a: The positive impact of a higher perceived sensitivity of information to disclose on perceived risks of privacy disclosure will be stronger if consumers are in a neutral affective state compared to a positive affective state.
H7b: The negative impact of a higher perceived sensitivity of information to disclose on perceived benefits of privacy disclosure will be stronger if consumers are in a neutral affective state compared to a positive affective state.

In summary, we hypothesize positive affect to override a *rational* assessment of risks and benefits, implying a biased and irrational risk-benefit valuation, resulting in irrational decisions on the intention to disclose information. On the other hand, neutral affect will lead to a differential cognitive evaluation of risks and benefits, where intentions to disclose should only depend on the sensitivity of information.

Proposed Methodology

The study will be designed as a 2x2 cross-sectional online experiment and conducted as part of a requirements analysis for a smartphone application on car driving developed by an insurance firm. More

precisely, the application is designed to record and track individual driving behavior and to provide feedback for better and safer driving. For this purpose, the app may record several types of data, including GPS coordinates and position, velocity, travel date, time and distance as well as acceleration behavior, car type and driver characteristics. Furthermore, the data collected by the app may be shared with the insurance firm. Using a pre-prototype approach (Davis and Venkatesh 2004), we will experimentally manipulate information sensitivity and affect, while simultaneously measuring dispositional factors such as general privacy concerns and institutional trust.

Sample and Procedure

The study will focus on potential future users of driving behavior apps, that is, younger drivers who have been shown to be more likely to engage in risky driving (Scott-Parker et al. 2009). Focusing on this particular group will help to ensure internal validity as participants across the experimental groups are relatively homogeneous (Dennis and Valacich 2001). In order to increase external validity, we also intend to test our model with additional studies that rely on different kinds of samples and domains, such as health applications.

Participants will be recruited by a marketing research company and incentivized monetarily for participating. After clicking on the web link leading to the survey, they will be randomly assigned to one of the four experimental conditions. They will first read an instruction text explaining the general purpose of the app, after which the app will be introduced using a standardized, brief description of the app idea and functionalities together with one of six scenarios. That is, the app will either request information high or low in sensitivity and will feature a screenshot that is either positive or neutral in affect. After viewing the app presentation page, participants will respond to the dependent variables. To avoid biases resulting from priming effects, privacy concerns and institutional trust will be measured some weeks before the actual experiment (Decoster and Claypool 2004).

Measurement

To ensure construct validity, scales from previous studies will be adapted wherever possible. Perceived risks and benefits will be adapted from Xu et al. (2009) and general privacy concerns from Malhotra et al. (2004). General institutional trust as well as intentions to disclose will be assessed using scales by Dinev and Hart (2006). We will also include control variables like personal interest, smartphone and previous privacy experiences and perceived enjoyment as well as demographic variables such as age, gender and culture. Furthermore, we will account for differences in risky driving behavior including the violations subscale of the Driver Behavior Questionnaire (DBQ, Reason et al. 1990). Following the marker-variable technique procedure proposed by Malhotra et al. (2006), a non-related scale will be integrated to control for common method variance. In order to check for the effectiveness of our manipulation, we will ask participants to rate (1) their current affective state applying the positive-affect-negative-affect scale (PANAS, Tellegen et al. 1988) and (2) their discomfort with information disclosure for types of data with varying sensitivity (Mothersbaugh et al. 2012).

Experimental Manipulation

Since we focus on a new kind of application (i.e., driving behavior apps), we cannot draw on existing materials and will develop experimental materials aimed at manipulating the degree of information sensitivity and the level of affect in a controlled manner.

Sensitivity of Information

To assess which kinds of personal information people consider more or less sensible in the context of driving behavior apps, we conducted a pilot study with 54 drivers aged between 18 and 27. In the study, we asked participants to indicate which information they would *not* disclose as part of a driver behavior analysis. Participants indicated that they would be least likely to disclose information about their location (named by 67% of participants) and potential speed violations (named by 50%). Hence, these two types of information will serve as our manipulation of high information sensitivity. That is, the driving behavior

app will request these two kinds of information in the high sensitivity conditions. On the other hand, the pilot study also indicated that information about distance travelled (named by only 17% of participants) and use of indicator light (also named by 17% of participants) were not considered as particularly sensitive pieces of information. Thus, these types of information will serve as our manipulation of low sensitivity.

Affect

As reported by prior research, rule-based thinking and affect-based thinking can be induced by affect-poor or 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 expect cute and appealing screenshots to be equally effective. This is in line with prior research in ergonomics that shows that aesthetically appealing screenshots raise positive feelings in users (e.g. Sonderegger and Sauer 2010; Sonderegger et al. 2012). We therefore plan to design and pilot-test a set of potentially affect-raising screenshots in the context of our application. An example of possible screenshots is given in Figure 2.

(a) positive affect (b) neutral affect

Figure 2. Examples of screenshots inducing (a) positive or (b) neutral affective states.

Conclusion and Contribution

By integrating research streams regarding the privacy calculus model as (1) a model of general and situational factors that is (2) bounded by irrational behavior, our research provides unique insights into the dynamics of decision making in information privacy. That is, we hope to add to the literature that emphasizes the role of irrational behavior in privacy by demonstrating that affective states play a crucial role in situation-specific privacy assessments. Furthermore, our research may also extend the IS literature by showing that both general and situational factors are relevant in the context of privacy calculus. From a practical viewpoint, we strive to underline the value of positive user experience for users and organizations and hope to convey an improved understanding of the relevance of users' dispositional tendencies in the development of information systems.

References

Acquisti, A. 2004. "Privacy in electronic commerce and the economics of immediate gratification," in *Proceedings of the 5th ACM conference on Electronic commerce*, New York, NY, USA, pp. 21–29.

Acquisti, A. 2009. "Nudging privacy: The behavioral economics of personal information," *IEEE Security & Privacy* (7:6), pp. 82–85.

Acquisti, A., and Grossklags, J. 2005. "Privacy and rationality in individual decision making," *IEEE Security & Privacy* (3:1), pp. 26–33.

Anderson, C. L., and Agarwal, R. 2011. "The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information," *Information Systems Research* (22:3), pp. 469–490.

Bansal, G., Zahedi, F. "Mariam", and Gefen, D. 2010. "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems* (49:2), pp. 138–150.

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

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104–115.

Damasio, A. R. 1994. "Descartes' error: Emotion, rationality and the human brain," *New York: Putnam* , p. 352.

Davis, F. D., and Venkatesh, V. 2004. "Toward preprototype user acceptance testing of new information systems: implications for software project management," *IEEE Transactions on Engineering Management* (51:1), pp. 31 – 46.

Decoster, J., and 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* (8:1), pp. 2–27.

Dennis, A. R., and Valacich, J. S. 2001. "Conducting Experimental Research in Information Systems," *Communications of the Association for Information Systems* (7:1).

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

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2012. "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts," *European Journal of Information Systems* .

Epstein, S. 1994. "Integration of the cognitive and the psychodynamic unconscious.," *American psychologist* (49:8), pp. 709–724.

Finucane, M. L., Alhakami, A., Slovic, P., and Johnson, S. M. 2000. "The affect heuristic in judgments of risks and benefits," *Journal of behavioral decision making* (13:1), pp. 1–17.

Finucane, M. L., and Holup, J. L. 2006. "Risk as Value: Combining Affect and Analysis in Risk Judgments," *Journal of Risk Research* (9:2), pp. 141–164.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., and Combs, B. 1978. "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sciences* (9:2), pp. 127–152.

Hsee, C. K., and Rottenstreich, Y. 2004. "Music, Pandas, and Muggers: On the Affective Psychology of Value," *Journal of Experimental Psychology: General* (133:1), pp. 23–30.

Hui, K. L., Tan, B. C. Y., and Goh, C. Y. 2006. "Online information disclosure: Motivators and measurements," *ACM Transactions on Internet Technology (TOIT)* (6:4), pp. 415–441.

Keith, M., Thompson, S., Hale, J., and 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., and 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* (44:2), pp. 544–564.

Kowatsch, T., and Maass, W. 2012. "Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts," *Proceedings of the 7th Mediterranean Conference on Information Systems*, pp. 200-211.

Krasnova, H., Veltri, N., and Günther, O. 2012. "Self-disclosure and Privacy Calculus on Social

Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), pp. 127–135.

Li, H., Sarathy, R., and Xu, H. 2011. "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors," *Decision Support Systems* (51:3), pp. 434–445.

Loewenstein, G. F., Weber, E. U., Hsee, C. K., and Welch, N. 2001. "Risk as feelings," *Psychological bulletin* (127:2), pp. 267–286.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research* (15:4), pp. 336–355.

Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research," *Management Science* (52:12), pp. 1865–1883.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2012. "Disclosure Antecedents in an Online Service Context The Role of Sensitivity of Information," *Journal of Service Research* (15:1), pp. 76–98.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.

Nyshadham, E. A., and Castano, D. 2012. "Affect and Online Privacy Concerns," *SSRN* .

Pavlou, P. A., and Gefen, D. 2004. "Building effective online marketplaces with institution-based trust," *Information Systems Research* (15:1), pp. 37–59.

Reyna, V. F. 2004. "How People Make Decisions That Involve Risk A Dual-Processes Approach," *Current Directions in Psychological Science* (13:2), pp. 60–66.

Scott-Parker, B., Watson, B., and King, M. J. 2009. "Understanding the psychosocial factors influencing the risky behaviour of young drivers," *Transportation Research Part F: Traffic Psychology and Behaviour* (12:6), pp. 470–482.

Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. 2004. "Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality," *Risk analysis* (24:2), pp. 311–322.

Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G. 2007. "The affect heuristic," *European Journal of Operational Research* (177:3), pp. 1333–1352.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information privacy research: an interdisciplinary review," *MIS Quarterly* (35:4), pp. 989–1016.

Sonderegger, A., and Sauer, J. 2010. "The influence of design aesthetics in usability testing: Effects on user performance and perceived usability," *Applied Ergonomics* (41:3), pp. 403–410.

Sonderegger, A., Zbinden, G., Uebelbacher, A., and Sauer, J. 2012. "The influence of product aesthetics and usability over the course of time: a longitudinal field experiment," *Ergonomics* (55:7), pp. 713–730.

Tellegen, A., Watson, D., and Clark, L. A. 1988. "Development and validation of brief measures of positive and negative affect: the PANAS scales.," *Journal of personality and social psychology* (54:6), pp. 1063–1070.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The effect of online privacy information on purchasing behavior: An experimental study," *Information Systems Research* (22:2), pp. 254–268.

Wakefield, R. 2013. "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems* .

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

Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. 2011. "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision Support Systems* (51:1), pp. 42–52.

Xu, H., Teo, H. H., Tan, B. C. Y., and Agarwal, R. 2009. "The role of push-pull technology in privacy calculus: the case of location-based services," *Journal of Management Information Systems* (26:3), pp. 135–174.

Zajonc, R. B. 1980. "Feeling and thinking: Preferences need no inferences.," *American psychologist* (35:2), pp. 151–175.