Perceived Threats of Privacy Invasions: Measuring Privacy Risks (Extended Abstract)

Sabrina Hauff[1], Manuel Trenz[1], Virpi Kristiina Tuunainen[2], and Daniel Veit[1]

[1] University of Augsburg, Faculty of Business and Economics, {sabrina.hauff, manuel.trenz, veit}@wiwi.uni-augsburg.de

[2] Aalto University, School of Economics, virpi.tuunainen@aalto.fi

Online services have become an integral part of our everyday lives. We shop online, we spend time in social networks, or use search engines to identify relevant information. In order to benefit from these easy and convenient ways of buying, communicating, and gathering data, we often share personal data. Companies such as Facebook, Google, and Amazon can use the gained knowledge to improve their service offerings and thus to increase their profits. However, even though people willingly trade personal information for such benefits, surveys continuously find that people are concerned about their privacy in today's digital and data-driven economy (BCG 2013). Thus, the question arises how privacy perceptions influence people's behavior.

Previous research has addressed this question by investigating how privacy concerns, defined as the worries that individuals have with respect to a potential loss of privacy due to organizational practices, are associated with individuals' behavioral reactions (Smith et al. 2011). Two established operationalizations for privacy concerns exist: The concern for information privacy (CFIP) scale (Smith et al. 1996) which differentiates between four different dimensions of privacy concerns, namely the concerns that personal data is collected, is used in an unauthorized way, is improperly accessed, and is erroneous, and the scale of internet users' information privacy concerns (IUIPC) which comprises the dimensions of collection, control, and awareness (Malhotra et al. 2004). Overall, these two operationalizations cover how individuals perceive organizations to handle their data without differentiating whether and how exactly these organizational practices actually impact individuals.

We offer a complementary perspective on how to investigate the influence of privacy on individuals' actual online behavior. We argue that individuals only change their behavior when they perceive to be impacted by third party behavior so that noticeable consequences for themselves might result from third party actions (Dowling 1986). Following this argumentation, the well-established and frequently used conceptualizations of privacy concerns (Malhotra et al. 2004; Smith et al. 1996) may not always cover this behaviorally relevant component. To give an example, secondary use of personal data can steeply increase the value of a personalized information service by improving the algorithms of the organization overall. However, only if individuals fear to be negatively affected by this secondary use, they actually adapt their behavior accordingly. This is the case if they face specific risks such as a financial loss, a reputational damage, or being

manipulated in their behavior. Thus, risks have direct behavioral consequences while concerns may or may not be attached to risks.

Based on these arguments, our paper has two objectives: First, we develop scales for the different dimensions of privacy risks as predictors of information disclosure behavior. Second, we compare their explanatory power to the well-established construct of privacy concerns.

To develop privacy risk scales, we followed the five steps by MacKenzie et al. (2011) to generate, validate, and refine our items. (1) We developed a conceptual definition of the latent variables. Thereby, we rely on the commonly used two components of risk, namely the severity of adverse consequences and their probability of occurrence, and we draw from existing literature on risks in other contexts (Featherman and Pavlou 2003; Glover and Benbasat 2010) and from the taxonomy of perceived consequences of privacy-invasive practices (Hauff et al. 2015). Thus, we define privacy risks as the extent to which an individual believes that privacy-invasive practices occur and negatively impact a person in a certain situation. This construct refers to a perception as it describes the perceived risk that a person realizes to face in a context. Moreover, we conceptualize privacy risks as multi-dimensional construct that applies to the entity of individuals. We identify the privacy risk dimensions social, psychological, physical, legal, independence-related, and resource-related. (2) We generated items that represent the latent variables. Therefore, we relied on existing scales for risks that were developed for other contexts wherever possible (Featherman and Pavlou 2003; Stone and Grønhaug 1993) and on statements from seven focus groups which we conducted. Then, the content validity of those items had to be assessed to ensure their suitability. Thus, we used an open sorting with four experienced raters based on the guidelines of Moore and Benbasat (1991) and an item rating to assess the items' content adequacy (MacKenzie et al. 2011). We further adjusted and shortened our instrument accordingly. (3) Next, we formally specified the measurement model by modeling privacy risk as a composite latent construct that comprises our six privacy risk dimensions. We measure all first-order risk dimensions reflectively while the dimensions are formative indicators of the second-order construct privacy risk. (4) We evaluated the scales in a small pre-study to test the comprehensibility of the items and of the scenario that we planned to use in the main study, and assessed reliability and validity to refine our items. (5) The last step of our scale development process aimed at validating our measurement model in a large-scale survey. Moreover, we wanted to investigate privacy risks in a nomological network and make a first comparison to the established construct of privacy concerns. Using a privacy calculus perspective, we investigated how privacy risks or respectively privacy concerns and privacy benefits influence online users' actual information disclosure behavior. We conducted our empirical study in the context of e-commerce and social networking, since data collection is particularly critical in this area. In the first step, participants were asked to actually share personal information in a given scenario where individuals were introduced to a start-up that wants to offer a personalized online magazine and asks for personal information to evaluate and better target its service. In a second step, they were questioned about their perceptions of this situation. The questionnaire was distributed among participants of an undergraduate business lecture at a German university in February 2015. We received 141 completed questionnaires. While we used our newly developed scales to assess privacy risks, we relied on existing scales for measuring privacy concerns (Smith et al. 1996; van Slyke et al. 2006) and perceived benefits (Krasnova et al. 2010). Lastly, we calculated the values of our dependent variable information disclosure behavior by counting the number of information pieces that a person disclosed in the survey (Joinson et al. 2010). We assessed the measurement models and had sufficient values for construct reliability and validity as well as discriminant validity. We also assessed our second-order formative constructs privacy risks,

privacy concerns, and benefits using the guidelines of Cenfetelli and Bassellier (2009). We used partial least squares structural equation modelling (PLS-SEM using SmartPLS; Ringle et al. 2015) to examine our models. The results of our analysis showed that in a model with both privacy risks and benefits as predictors of information disclosure, privacy risks ($\beta = -0.400$, $p<0.001$) and benefits ($\beta = 0.358$, $p<0.001$) significantly influence information disclosure behavior as hypothesized. Adjusted R^2 is 0.231. This also confirms the nomological validity of our privacy risk construct. In a second model, we investigated privacy concerns and benefits as predictors of information disclosure behavior. In this case, benefits significantly impact behavior ($\beta = 0.279$, $p<0.001$) while privacy concerns do not ($\beta = -0.352$, $p>0.5$). Adjusted R^2 is 0.199. In a third model, we included both privacy concerns and privacy risks in addition to benefits. Privacy risks ($\beta = -0.314$, $p<0.001$) and benefits ($\beta = 0.334$, $p<0.001$) significantly impact behavior, while privacy concerns do not ($\beta = -0.205$, $p>0.5$). Adjusted R^2 is 0.261.

Our results show that we developed valid measurement scales for privacy risks which offer promising avenues for a further exploration of how privacy perceptions influence individuals' behavior and thus provide several interesting contributions for theory and practice.

We contribute to theory by advancing the understanding of privacy risks as multi-dimensional concept that has the dimensions of social, legal, physical, resource-related, independence-related, and psychological risks. All those dimensions describe the extent to which individuals perceive to be affected by a privacy invasion through third parties. Thus, we offer a novel perspective on how to measure information privacy as previous conceptualizations neglected to capture the perceived impact of negative consequences that can arise from sharing information online.

Our study has also practical implications. Many business models such as those of social network site providers or e-commerce platforms depend on the collection and analysis of user data. Therefore, they are very interested in better understanding the circumstances of individual information disclosure, reasons that might prevent disclosure, and how to mitigate problematic influences. Our conceptualization of privacy risks can help organizations to recognize why consumers hesitate to share information and which risks may have to be mitigated by the service design to prevent discouraged users.

We see several promising avenues for future research. In particular, more heterogeneous samples should be used and the influence of privacy risks in other contexts such as financial or health scenarios should be explored to see which risk dimensions are prevalent there. Investigating how third parties can actively mitigate privacy risks is another promising research direction.

References

BCG (2013) The Value of Our Digital Identity. https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/. Accessed on 29.6.2013

Cenfetelli RT, Bassellier G (2009) Interpretation of Formative Measurement in Information Systems Research. MIS Quarterly 33(4):689–707

Dowling GR (1986) Perceived Risk: The Concept and Its Measurement. Psychology & Marketing 3(3):193–210

Featherman MS, Pavlou PA (2003) Predicting E-Services Adoption: A Perceived Risk Facets Perspective. International Journal of Human-Computer Studies 59(4):451–474

Glover S, Benbasat I (2010) A Comprehensive Model of Perceived Risk of E-Commerce Transactions. International Journal of Electronic Commerce 15(2):47–78

Hauff S, Veit D, Tuunainen V (2015) Towards a Taxonomy of Perceived Consequences of Privacy-Invasive Practices. In: Proceedings of the 23rd European Conference on Information Systems (ECIS). Münster, Germany

Joinson AN, Reips U-D, Buchanan T, Schofield CBP (2010) Privacy, Trust, and Self-Disclosure Online. Human–Computer Interaction 25(1):1–24

Krasnova H, Spiekermann S, Koroleva K, Hildebrand T (2010) Online Social Networks: Why We Disclose. Journal of Information Technology 25(2):109–125

MacKenzie SB, Podsakoff PM, Podsakoff NP (2011) Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. MIS Quarterly 35(2):293–334

Malhotra NK, Kim SS, Agarwal J (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15(4):336–355

Moore GC, Benbasat I (1991) Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Information Systems Research 2(3):192–222

Ringle CM, Wende S, Becker J-M (2015) SmartPLS.

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35(4):989–1016

Smith HJ, Milberg SJ, Burke SJ (1996) Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly 20(2):167–196

Stone RN, Grønhaug K (1993) Perceived Risk: Further Considerations for the Marketing Discipline. European Journal of Marketing 27(3):39–50

van Slyke C, Shim JT, Johnson R, Jiang J (2006) Concern for Information Privacy and Online Consumer Purchasing. Journal of the Association for Information Systems 7(6):415–444