12-12-2021

Users' privacy perceptions in interorganizational information sharing

Christina Wagner
University of Augsburg, christina.wagner@uni-a.de

Manuel Trenz
University of Goettingen

Daniel Veit
University of Augsburg

Chee-Wee Tan
Copenhagen Business School

Users' Privacy Perceptions in Interorganizational Information Sharing

Christina Wagner[1]
University of Augsburg,
Augsburg, Germany

Manuel Trenz
University of Goettingen,
Goettingen, Germany

Daniel Veit
University of Augsburg,
Augsburg, Germany

Chee-Wee Tan
Copenhagen Business School,
Copenhagen, Denmark

ABSTRACT

Existing privacy theories shed light on the mechanisms at work when users decide to share information with an organization – yet do not sufficiently encompass the common practice of sharing user information across organizations. This research study introduces the concept of Interorganizational Information Sharing (IIS) and theorizes on boundary uncertainty and boundary control to develop a model of privacy perceptions in IIS. To empirically validate this model, we collect data through an online survey in the context of smart fitness devices. Our research aims at advancing and articulating the concept of IIS, conceptualizing privacy perceptions based on that understanding, and subsequently relating those perceptions to behavioral intentions to protect privacy in IIS. We thereby contribute to IS privacy literature, considering the complexity of information sharing relationships in a granular manner.

Keywords: Privacy, Information Sharing, Interorganizational, Uncertainty, Control, Boundary, Communication Privacy Management

[1] Corresponding author. christina.wagner@uni-a.de +49 821 598 - 4409

INTRODUCTION

The sharing of user information across organizations is a predominant practice in the information economy. From an organization's perspective, the sharing of user information with affiliates is desirable in that it not only boosts revenue, it also often culminates in the delivery of customer services with added value. Despite potential benefits for users, such as a personalized service experience, sharing information across organizations might also evoke users' privacy concerns.

Notwithstanding significant advances in prior research in uncovering the mechanisms underlying users' decisions to share information with an organization, such as performing a risk-benefit trade-off (e.g., Dinev and Hart 2006), there is comparatively limited progress made in understanding users' reactions to the sharing of their information with other organizations after an initial disclosure. This perspective may capture the complexity of information sharing relationships that we see in the real world (Conger et al. 2013).

In general, third-party information sharing encompasses both authorized and unauthorized use of information by organizations. In this research project, we concentrate on *the authorized and intentional sharing of user information among organizations, of which the individual is directly sharing or has directly shared information with at least one organization* and term this phenomenon **Interorganizational Information Sharing** (IIS). IIS can be found in a variety of contexts associated with the internet and is becoming increasingly relevant as more and more user information is stored digitally. Social media services may integrate third-party applications and share user information with those (Wang et al. 2011). Publisher websites may outsource certain components of their websites and present content provided by third party

providers (Gopal et al. 2018). Public and private healthcare organizations may exchange individuals' health information to improve care coordination (Esmaeilzadeh 2020).

In this study, we want to unravel the roles of control and uncertainty in informing users' privacy perceptions about IIS and in dictating potential actions they might take to protect their privacy. In doing so, we endeavor to answer the following research question: *How do users' privacy perceptions in IIS impact their subsequent behavioral intentions to protect their privacy in the context of smart fitness devices?*

To answer this research question, we develop the concept of IIS and articulate its unique characteristics. On that basis, we conceptualize privacy perceptions in IIS and propose a relationship with behavioral intentions to protect one's privacy in IIS. These hypotheses are tested and validated empirically through an online survey in the context of smart fitness devices. Finally, we discuss our results and their implications.

THEORETICAL FOUNDATION

Interorganizational Information Sharing (IIS)

Acknowledging prior research on information disclosure situations between two parties (Smith et al. 2011), the exchange of information between multiple parties has also been considered in different ways. One stream of research has focused on value creation through information sharing between organizations (e.g., Adjerid et al. 2018; Feldman and Horan 2011) at an organizational level. Also at an organizational level, some studies have added the dimension of information security and privacy issues to this information exchange (e.g., Anderson et al. 2017; Gopal et al. 2018). At an individual level, understanding has been gained regarding value creation through information sharing between individuals within organizations (e.g., Bannister 2001; Davison et al. 2013; Olivera et al. 2008). In the context of social media,

interdependent privacy is considered, i.e., information may be owned by several users (e.g., Kamleitner and Mitchell 2019). What remains to be understood at the individual level are users' perceptions of the sharing of their information between organizations that leads to value creation.

To theoretically unpack the concept of IIS, we begin by introducing associated terminologies. Particularly, we differentiate among three parties in IIS: the user (henceforth referred to as the information owner), the organization that the user is currently a customer of (henceforth referred to as the information co-owner), and the external organization that is interested in accessing the co-owned information (henceforth referred to as the information consumer). Our terminology is inspired by Communication Privacy Management (CPM) Theory (Petronio 2002). The target of IIS is any information that the information co-owner has collected about the information owner that they may potentially share with an information consumer. Table 1 depicts the key terminologies in IIS.

Table 1. Parties in IIS

Term	Definition	Example
Information owner	An individual who, as a customer of an information co-owner, shares information with the latter as part of a customer-relationship	Facebook user, smart fitness device user
Information co-owner	Party authorized by the information owner to have access to selected information	Facebook, smart fitness device provider
Information consumer	External party (to be) authorized to have access to (parts of) the information the information co-owner has collected on the information owner	Third-party service provider, other smart fitness device providers

Based on the preceding conception of IIS and inspired by the concept of information asymmetries (Akerlof 1978), we arrive at four unique characteristics that distinguish IIS from adjacent information sharing phenomena – displayed in Table 2. In line with these characteristics of IIS, we derive two focal concepts to understand users' privacy perceptions in IIS, namely boundary uncertainty and boundary control.

Table 2. Characteristics of IIS

#	Characteristic
1	*IIS involves multiple stakeholders:* Increases complexity; difficulty in assessing potential actions and associated consequences of all stakeholders involved
2	*Information asymmetries between information owner and information co-owner:* Information co-owner assumes role of an agent to protect information owner's privacy when it comes to sharing disclosed information with an information consumer
3	*Information asymmetries between information owner and information consumer:* Information consumer remains intransparent; difficulty for information owner to gauge potential actions and associated consequences to be expected from information consumer potentially accessing their information
4	*Information asymmetries between information co-owner and information consumer:* Difficulty for information owner to assess information co-owner's information sharing activities; information consumer might behave in ways that information co-owner does not know about and cannot prevent

Boundary uncertainty

All of the characteristics of IIS, as presented above, culminate in an increase in complexity and information asymmetries between multiple parties. Inspired by a discussion by Acquisti and Grossklags (2012) on perceived privacy risk and uncertainty in an environment in which it is unrealistic to assume that known probabilities over possible outcomes exist, we argue that a relevant concept to understand privacy perceptions in IIS is perceived uncertainty.

Al-Natour et al. (2020) advanced privacy uncertainty as a novel construct, defined as "the [information owner's] difficulty in assessing how the privacy of his or her information is maintained when it is disclosed" (Al-Natour et al. 2020, p. 1045). They theoretically differentiate between two aspects of uncertainty: (1) its sources, such as the organization that is about to share information or an external party that may want to access that information; and (2) its content, such as what information is collected, how it is used, or how it is protected. Al-Natour et al. (2020) built their conceptualization around the understanding of uncertainty as its content.

Due to the characteristic of IIS of involving multiple parties, we are inspired by the perspective of privacy uncertainty as its sources, theoretically grounded in CPM Theory

(Petronio 2002). CPM Theory provides a framework to understand information sharing that involves more than two parties. When information becomes co-owned by both information owner and information co-owner, both have certain rights and responsibilities over that information. Surrounding this co-owned information is what is termed in CPM Theory a boundary. When an outside party wants to gain access to co-owned information, information owner and information co-owner negotiate collective boundary management rules. These rules refer to distinct aspects of boundary opening or closing towards that outside party. Petronio (2002) differentiates three aspects: Linkage, ownership, and permeability. In the light of CPM Theory, we rely on the terminology of boundaries and define **boundary uncertainty** as *an information owner's difficulty in assessing how the privacy of his or her information currently shared with an information co-owner is maintained when considering the possibility of IIS*. Derived from the viewpoint of collective boundary management, boundary uncertainty is conceptualized as consisting of three dimensions. Details can be obtained from Table 3.

Table 3. Definitions of dimensions of boundary uncertainty

Dimension	Definition
Boundary linkage uncertainty	An information owner's difficulty in assessing who the information co-owner is sharing information collected about the information owner with
Boundary ownership uncertainty	An information owner's difficulty in assessing what information collected by the information co-owner is shared with an information consumer
Boundary permeability uncertainty	An information owner's difficulty in assessing under what conditions the information co-owner is sharing information collected by them with an information consumer

Boundary control

Espousing the lens of control agency (Xu et al. 2012), one can differentiate between the "effects of personal control, in which the self acts as the control agent to protect privacy" and "proxy control, in which powerful others […] act as the control agents to protect privacy" (p.

1346). In IIS, we view the information co-owner as the agent to protect the information owner's privacy when it comes to sharing that information with other parties. Personal privacy control can be increased, for example, when the information co-owner gives the information owner the ability to choose the conditions and degree to which they want to disclose information (Laufer and Wolfe 1977). However, an increase in objective privacy control is not necessarily associated with an increase in perceived privacy control, due to judgement fallacies (Brandimarte et al. 2013). We will thus focus on personal control perceptions. Synthesizing extant literature on perceived privacy control (Brandimarte et al. 2013; Xu et al. 2011, 2012) and once more applying the terminology of CPM Theory, we define **boundary control** as *the information owner's belief about their ability to manage the release and dissemination of information between the information co-owner and the information consumer*.

Behavioral intentions to protect privacy in IIS

Prior information privacy research has often focused on initial disclosure intentions as the dependent variable of interest (Dinev and Hart 2006; Esmaeilzadeh 2020; Smith et al. 2011; Zhao et al. 2012). A handful of studies have considered different types of behaviors as an outcome of a privacy decision, such as withholding or falsifying information (Metzger 2007).

Considering that in IIS the initial information disclosure has already occurred, we will extend this concept to capture the intention to allow (i.e. authorize) boundary opening – the prerequisite to enabling the information co-owner's sharing of information collected about the information owner with an information consumer – as one way through which the information owner can protect their privacy in the light of IIS.

Going one step further, an information owner might take actions to revoke the information owner's access rights to their disclosed information as another way to protect their

privacy in IIS. An exemplary execution of withdrawing access rights from the information co-owner would be deleting specific information they have previously shared. What is of interest in IIS is therefore whether or not an information owner would want to withdraw any information they have already disclosed, captured by their withdrawal intention.

RESEARCH MODEL

We propose a relationship between boundary control, boundary uncertainty, and the intention to allow boundary opening, as well as to withdraw information from the information co-owner in the light of IIS as depicted by our research model in Figure 1.

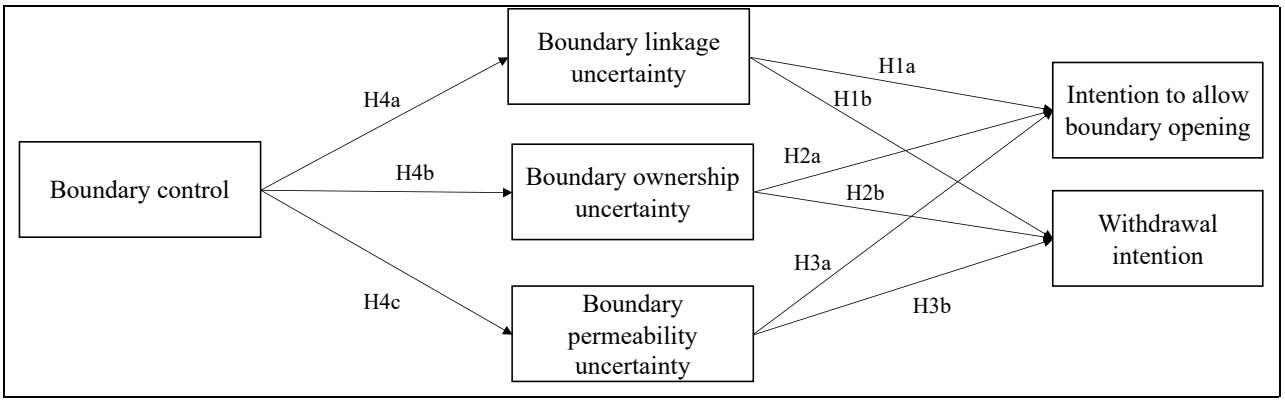

Figure 1. Research model

First, we argue that boundary uncertainty is associated with privacy-related behavior in IIS. Individuals are in general ambiguity and uncertainty averse (Ellsberg 1961). In prior research on information systems privacy, risk perceptions are found as one of the main hinderances to information disclosure (e.g., Xu et al. 2012). Similarly, we anticipate that information owners will try to act in ways that will reduce the potential for negative consequences which may arise from the information co-owner behaving in ways that place the information owner's privacy at risk. If the information owner perceives high uncertainty regarding *which information consumers* the information co-owner shares their information with, the lack of information about the potential information consumers might hinder them from

evaluating potential consequences of the information consumer's actions. Not allowing boundary opening might be seen as one option to protect their privacy, considering to withdraw information already disclosed as another. We therefore hypothesize that:

Hypothesis 1: *Boundary linkage uncertainty is (a) negatively related with the intention to allow boundary opening and (b) positively related with withdrawal intentions.*

If information owners perceive high uncertainty regarding *what information* the information co-owner might share with an information consumer, the lack of knowledge about the type of information that the information consumer may access is hindering them from determining potential negative consequences of any potential use of that information. By not agreeing to share this information within IIS, or by withdrawing information already disclosed to an information co-owner, the information owner can prevent the information consumer from using information they do not want to them to. We therefore hypothesize that:

Hypothesis 2: *Boundary ownership uncertainty is (a) negatively related with the intention to open boundaries and (b) positively related with withdrawal intentions.*

If information owners perceive high uncertainty regarding *the conditions* under which the information co-owner might share their information with an information consumer, their inability to evaluate potential consequences of that information sharing for their privacy may stem from two sources: First, it may stem from their inability to know whether the information co-owner will consider their interests when deciding about the way in which they share information with an information consumer. Second, the information owner might additionally worry about whether the way that the information co-owner shares information makes it easier for an information consumer to disregard any of the information co-owners' terms of sharing. Again, an option that the information owner may see to protect their privacy may be to not allow boundary

opening or to withdraw information already shared with the information co-owner. We therefore hypothesize further:

Hypothesis 3: *Boundary permeability uncertainty is (a) negatively related with the intention to open boundaries and (b) positively related with withdrawal intentions.*

Finally, even though an information owner may authorize IIS, they may still perceive little control over how IIS is executed. If they do, however, perceive boundary control, this is expected to be negatively related to all dimensions of boundary uncertainty. In general, controllability has been found a determinant of risk taking (Slovic 1987). In research on information systems privacy the negative relationship between control and risk has been supported widely (Xu et al. 2012). Boundary control reduces the perception of information asymmetries about how the information co-owner may handle the information owner's information when it comes to IIS. Consequentially, control perceptions over how the information co-owner is handling the information sharing with the information consumer reduce the difficulty in assessing (a) who the information co-owner is sharing information with, (b) what information they are sharing, and (c) under what conditions they are sharing information. We therefore hypothesize that:

Hypothesis 4: *Boundary control is negatively related with (a) boundary linkage uncertainty, (b) boundary ownership uncertainty, and (c) boundary permeability uncertainty.*

METHODOLOGY

To empirically test our research model, we conducted an online survey in the context of smart fitness devices. Data from 119 German gym members was collected via the research platform Prolific Academic in July 2021. A panel sample was considered appropriate for the study as it enabled access to study participants that had experience with gyms. Participants were

presented a scenario where they were to imagine that their gym was offering them the opportunity to benefit from enhanced training analyses if they were to allow an exchange of information collected about them by their gym with different providers of smart fitness devices. This context and scenario are deemed as suitable to represent an interesting instantiation of IIS, as it considers the complexity of involving several information consumers (providers of smart fitness devices) whom information owned by the information owner (a gym member) is shared with through an information co-owner (their gym).

Our dependent variables are operationalized based on the 7-point semantic scale for the intention to give information employed by Malhotra et al. (2004). To measure boundary control, we rely on Xu et al.'s (2012) 7-point Likert scale (e.g., "I believe that my gym gives me control over which information is shared with third parties"). To operationalize our newly developed concept of boundary uncertainty, we adhered to the structured scale development procedure advocated by MacKenzie et al. (2011), which is part of a separate research paper. An exemplary item for boundary linkage uncertainty is "I am uncertain about who is allowed access to this information by my gym". We further controlled for age, gender, education, marital status, and employment status.

FINDINGS

Due to the rather exploratory nature of the study and our goal of predicting key driver constructs, PLS-SEM was regarded as the most suitable means for analysis (Hair et al. 2017). PLS-SEM was found to perform as effective as comparable techniques in detecting paths and not falsely detecting non-existent paths (Goodhue et al. 2012). Our measurement model indicates high internal validity with Average Variance Extracted (AVE) values above .5, Composite Reliability and Cronbach Alpha values above .7, and factor loadings above .7. In accordance

with the Fornell-Larcker criterium, the square root of the AVE of each construct is greater than its correlation with any other construct, accounting for discriminant validity (Fornell and Larcker 1981). Discriminant validity is further supported by the heterotrait monotrait ratio of correlations, which is well below the threshold of .85 (Henseler et al. 2015). Further, Variance Inflation Factors (VIF) for all combinations of our latent variables are well below the recommended threshold of 5, alleviating concerns of multicollinearity (Hair et al. 2011). Details on the results for the measurement model are displayed in the Appendix.

To assess the structural model, we estimate parameter significance by employing bootstrapping with n = 5,000 samples with SmartPLS 3 (Hair et al. 2017). We can find support for hypothesis 3a for the relationship between boundary permeability uncertainty and intentions to allow boundary opening (β = -.357, *t*-value = 3.373). Additionally, it should be mentioned that at a significance level of .1 hypothesis 1a regarding the relation between boundary linkage uncertainty and intentions to allow boundary opening would be supported as well (β = -.196, *t*-value = 1.871). Further, all path coefficients between boundary control and all boundary uncertainty dimensions are negative and significant at .05, supporting hypothesis 4. Other paths were not found significant. R square values for intention to allow boundary opening and withdrawal intention lie at .142 and .010 respectively. Further details can be obtained from the Appendix.

DISCUSSION

These findings indicate interesting relationships between different dimensions of boundary uncertainty and intentions to act in certain ways to protect one's privacy. More specifically, the permeability dimension of boundary uncertainty, which is about the conditions under which the information co-owner is sharing information about the information owner, is

negatively related to the intention to allow boundary opening and thereby authorize IIS. Additionally, the linkage dimension of boundary uncertainty, which is about who information is shared with in IIS, might impact the intention to agree to open boundaries negatively as well. We derive from these findings, that users value the conditions under which the information co-owner is sharing information with an information consumer more than the type of information that is being shared, or who the information consumer is. If users know that the information co-owner will handle the information sharing process with care, the who and the what of IIS play only a minor role.

So far, we find no support for our hypotheses regarding the uncertainty stemming from IIS leading to an information owner wanting to withdraw information already disclosed. We view withdrawal intention as going one step further than simply not allowing boundary opening – and explain our insignificant findings with the additional effort and inconveniences for the user that may be associated with engaging in information withdrawal.

Furthermore, we see strong negative relations between boundary control and boundary uncertainty. This opens the question as to how such boundary control may look like – which may be addressed in future extensions of this research project.

To specifically answer our research question, the results of our empirical study indicate that intentions to allow boundary opening and thereby authorize IIS are impacted by perceptions of uncertainty relating to the conditions under which the information co-owner is sharing information as well as who information is shared with. These perceptions of uncertainty are reduced through perceptions of boundary control.

Our study is also subject to limitations. First, our sample size is rather small and privacy behavior in IIS is captured by measuring intentions. In a future extension of this study, we plan

to conduct a field survey on a larger sample of gym users, potentially accessing behavioral data. Second, the context of our study has certain characteristics (service is paid for monetarily, information co-owner is a physical organization) that may not make our findings generalizable to other contexts. In a future extension of this study we might reproduce it in different contexts, such as social media (service in exchange for data, online information co-owner).

Theoretically, we contribute in two main ways: First, we introduce and articulate the concept of IIS from a user's perspective, a phenomenon very common in practice. This is deemed as an important addition to prior privacy research, as through the added complexity and uncertainty inherent to this phenomenon, existing explanations of privacy perceptions and behaviors need to be adapted. As far as possible, we rely our conceptualization on established concepts from information privacy research – in order to build on what has been established and at the same time make our findings comparable. Second, by theoretically grounding the complexity that we see in the ways information may be used by organizations in CPM theory, we gain a more granular understanding of privacy perceptions in IIS, as well as how they relate to behavioral intentions to protect one's privacy.

This study may also have implications to organizations interested in IIS as well as to policy makers. Understanding user's perceptions of information sharing between organizations is an important step towards enabling those organizations to create value while at the same time respecting their users' privacy. Our findings may inform organizations about how to evaluate strategic options regarding extending their business through IIS and what to consider to handle their users' privacy concerns with care when partaking in IIS. If organizations are not willing to employ IIS in ways that treat their users' privacy with care, legal reinforcement related to

unauthorized third-party information sharing needs to be strengthened as well as aligned between nations with different privacy regulations.

REFERENCES

Acquisti, A., and Grossklags, J. 2012. "An Online Survey Experiment on Ambiguity and Privacy," *Communications & Strategies* (88:4), pp. 19–39.

Adjerid, I., Acquisti, A., and Loewenstein, G. 2018. "Choice Architecture, Framing, and Cascaded Privacy Choices," *Management Science* (65:5), pp. 2267–2290.

Akerlof, G. A. 1978. "The market for 'lemons': Quality uncertainty and the market mechanism," in *Uncertainty in economics*, Elsevier, pp. 235–251.

Al-Natour, S., Cavusoglu, H., Benbasat, I., and Aleem, U. 2020. "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps," *Information Systems Research* (31:4), pp. 1037–1063.

Anderson, C., Baskerville, R. L., and Kaul, M. 2017. "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information," *Journal of Management Information Systems* (34:4), pp. 1082–1112.

Bannister, F. 2001. "Dismantling the Silos: Extracting New Value from IT Investments in Public Administration," *Information Systems Journal* (11:1), pp. 65–84.

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.

Conger, S., Pratt, J. H., and Loch, K. D. 2013. "Personal Information Privacy and Emerging Technologies," *Information Systems Journal* (23:5), pp. 401–417.

Davison, R. M., Ou, C. X. J., and Martinsons, M. G. 2013. "Information technology to support informal knowledge sharing," *Information Systems Journal* (23:1), pp. 89–109.

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

Ellsberg, D. 1961. "Risk, Ambiguity, and the Savage Axioms," *The Quarterly Journal of Economics* (75:4), pp. 643–669.

Esmaeilzadeh, P. 2020. "The Impacts of the Privacy Policy on Individual Trust in Health Information Exchanges (HIEs)," *Internet Research* (30:3), pp. 811–843.

Feldman, S. S., and Horan, T. A. 2011. "The Dynamics of Information Collaboration: A Case Study of Blended IT Value Propositions for Health Information Exchange in Disability Determination," *Journal of the Association for Information Systems* (12:2), pp. 189–207.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39–50.

Goodhue, D. L., Lewis, W., and Thompson, R. 2012. "Does PLS Have Advantages for Small Sample Size or Non-Normal Data?," *MIS Quarterly*, pp. 981–1001.

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E., and Zhdanov, D. 2018. "How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas," *MIS Quarterly* (42:1), pp. 143-A25.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Richter, N. F., and Hauff, S. 2017. *Partial Least Squares Strukturgleichungsmodellierung (PLS-SEM)*, Munich, Germany: Vahlen.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed a Silver Bullet," *Journal of Marketing Theory and Practice* (19:2), pp. 139–152.

Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 115–135.

Kamleitner, B., and Mitchell, V. 2019. "Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements," *Journal of Public Policy & Marketing* (38:4), pp. 433–450.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22–42.

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp. 293–334.

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.

Metzger, M. J. 2007. "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication* (12:2), pp. 335–361.

Olivera, Goodman, and Tan 2008. "Contribution Behaviors in Distributed Environments," *MIS Quarterly* (32:1), p. 23.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*, New York, USA: State University of New York Press.

Slovic, P. 1987. "Perception of Risk," *Science* (236:4799), pp. 280–285.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 980–1016.

Wang, N., Xu, H., and Grossklags, J. 2011. "Third-Party Apps on Facebook: Privacy and the Illusion of Control," in *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, pp. 1–10.

Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798–824.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2012. "Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research* (23:4), pp. 1342–1363.

Zhao, L., Lu, Y., and Gupta, S. 2012. "Disclosure Intention of Location-Related Information in Location-Based Social Network Services," *International Journal of Electronic Commerce* (16:4), pp. 53–90.

APPENDIX

Abbreviations: Latent Variable (LV), Cronbach's Alpha (CA), Composite Reliability (CR), Average Variance Extracted (AVE), Boundary control (BC), Intention to allow boundary opening (IBO), Boundary linkage uncertainty (BLU), Boundary ownership uncertainty (BOU), Boundary permeability uncertainty (BPU), Withdrawal intention (WI)

Table 4. Reliability and validity of measurement model (Diagonals show the square root of the AVE, Correlations are shown below, heterotrait monotrait ratio of correlations in brackets)

LV	CA	CR	AVE	BC	IBO	BLU	BOU	BPU	WI
BC	0.899	0.903	0.899	0.912					
IBO	0.937	0.966	0.937	0.247	0.966				
				(0.264)					
BLU	0.832	0.974	0.832	-0.433	-0.249	0.940			
				(0.462)	(0.256)				
BOU	0.965	0.977	0.965	-0.383	-0.193	0.579	0.951		
				(0.407)	(0.198)	(0.597)			
BPU	0.977	0.951	0.977	-0.205	-0.340	0.388	0.636	0.899	
				(0.222)	(0.352)	(0.398)	(0.661)		
WI	0.934	0.999	0.934	-0.165	-0.276	0.060	0.101	0.078	0.949
				(0.186)	(0.282)	(0.06)	(0.100)	(0.083)	

Table 5. VIF values

	IBO	WI	BC	BLU	BOU	BPU
IBO	-	1.206	1.256	1.262	1.255	1.168
WI	1.027	-	1.085	1.087	1.090	1.092
BC	1.306	1.325	-	1.240	1.283	1.317
BLU	1.655	1.674	1.563	-	1.420	1.684
BOU	2.216	2.260	2.179	1.913	-	1.560
BPU	1.690	1.855	1.832	1.858	1.278	-

Table 6. Structural model results

Hypothesis	Path	Path coefficient	T statistic	P value
H1a	H1a: BLU > IBO	-0.196	1.871	0.061
H1b	H1b: BLU > WI	0.002	0.015	0.988
H2a	H2a: BOU > IBO	0.147	1.031	0.303
H2b	H2b: BOU > WI	0.085	0.516	0.606
H3a	H3a: BPU > IBO	-0.357	3.373	0.001
H3b	H3b: BPU > WI	0.024	0.156	0.876
H4a	H4a: BC > BLU	-0.433	5.019	<.001
H4b	H4b: BC > BOU	-0.383	4.618	<.001
H4c	H4c: BC > BPU	-0.205	2.118	0.034