6-18-2022

Unraveling User Perceptions of Interorganizational Information Sharing

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

Manuel Trenz
University of Goettingen, trenz@uni-goettingen.de

Chee-Wee Tan
Copenhagen Business School, ct.digi@cbs.dk

Daniel Veit
University of Augsburg, daniel.veit@wiwi.uni-augsburg.de

UNRAVELING USER PERCEPTIONS OF INTERORGANIZATIONAL INFORMATION SHARING

Research in Progress

Christina Wagner, University of Augsburg, Augsburg, Germany, christina.wagner@uni-a.de
Manuel Trenz, University of Goettingen, Goettingen, Germany, trenz@uni-goettingen.de
Chee-Wee Tan, Copenhagen Business School, Copenhagen, Denmark, ct.digi@cbs.dk
Daniel Veit, University of Augsburg, Augsburg, Germany, daniel.veit@uni-a.de

Abstract

Collecting large amounts of user information is becoming an increasingly important source of value for businesses. Such data sets may be expanded through engaging in value co-creation with other organizations. Sharing user information across organizations, however, might evoke users' privacy concerns. Existing mechanisms and concepts developed in prior information privacy research on sharing information between one user and one organization may no longer apply as multiple organizations become involved. This creates the necessity to understand more granularly how users perceive privacy situations that involve sharing their information across organizations – and how their concerns may be alleviated through control mechanisms. Employing the lens of Communication Privacy Management (CPM) theory, we conceptualize this phenomenon as Interorganizational Information Sharing (IIS) and theorize on perceived uncertainty and control to unravel user perceptions in IIS. We present our ideas for a research model, as well as our planned methodology for empirical validation.

Keywords: Privacy, Interorganizational Information Sharing, Uncertainty, Control, Boundaries.

1 Introduction

Being able to collect and exploit large amounts of data has become an important source of value creation for many businesses (Grover et al., 2018). With the rise of data-based business models and digital platforms, the amount of data collected and used is increasing, and thereby the complexity of the data value chain they feed (Abbasi et al., 2016; Gregory et al., 2021). As organizational processes are increasingly digitized, new opportunities for organizations to share information among them and thereby engage in value co-creation with one another arise (Feldman and Horan, 2011; Grover and Kohli, 2012; Adjerid et al., 2018). Such value could entail improved and more personalized services for users (Karwatzki et al., 2017), or increased marketing opportunities through customer segmentation for organizations (Schneider et al., 2017).

Data-driven business models per se raise users' concerns for privacy (Grover et al., 2018). If data use extends beyond one organization, a user is confronted with even higher uncertainty, heightening those privacy concerns further (Acquisti et al., 2015). As a result, organizations face a tension between their information needs and the resulting value they might thereby create for their users – and the necessity to ensure their users' privacy to avoid losing them as customers (Gopal et al., 2018; Gerlach et al., 2019). We see this phenomenon in social media services that integrate third-party applications and share user information with those (Wang et al., 2011), public and private healthcare organizations that exchange individuals' health information to improve care coordination (Esmaeilzadeh, 2019, 2020), or digital fitness devices, such as the Apple watch, that enable the reading of data from fitness equipment of different providers directly into their own environment[1].

Users' perceptions and decisions related to information sharing with one organization have been subject of extensive study in prior information privacy research – uncovering mechanisms such as performing a risk-benefit trade-off (Dinev et al., 2006) and identifying a variety of constructs forming users' privacy perceptions related to this situation (Smith et al., 2011). Recently, the complexity of information sharing involving multiple parties or groups has been subject to broad theorizing and calls for further research (Conger et al., 2013; Bélanger and James, 2020). Prior research on information sharing between organizations has, however, mostly been aimed at understanding how this exchange of information may create economic and business value (Feldman and Horan, 2011; Adjerid et al., 2018; Gopal et al., 2018) – largely neglecting the role of the user that such information may stem from and/or their privacy perceptions that result specifically from this situation.

Given the legal environment in the European Union, privacy regulations in the form of the GDPR are in place that require a lawful basis for organizations to process users' information, mostly through obtaining users' consent (General Data Protection Regulation, 2016). Considering, however, that individual privacy behavior is impacted by automized cognitive processes and biased perceptions (Dinev et al., 2015), we need to understand the perceptions that a user has in this phenomenon that we term *Interorganizational Information Sharing* (IIS) and define as the intentional sharing of user information among organizations, where a user is directly sharing information with at least one organization. Uncertainty in privacy decision-making is deemed as relevant to understand the complexity that users face in such a situation. To understand, how these perceptions may be affected, we look at control perceptions, and their actionable conceptualization as control mechanisms. To approach the stated problematization, we pose the following research question: *How do users perceive IIS and how do control mechanisms impact those perceptions and the resulting intentions to allow IIS?*

Grounded in an extensive review of related information privacy research, we theorize on control and uncertainty to gain a granular understanding of users' perceptions of the sharing of their information between organizations. First, we define and delimit our phenomenon of interest, IIS. Second, we derive our granular understanding of users' perceptions related to this phenomenon. Finally, we want to explore control mechanisms as a way in which organizations can ensure their users' privacy when employing IIS so that both users and organizations can benefit from the possibilities of value co-creation. Our goal

[1] https://support.apple.com/en-us/HT212187 (2022/03/09)

is here to guide those organizations in finding a balance between the complexity of too many controls that may lead to users' overwhelm and providing too little control that may lead to insufficient privacy for their users. We expect our findings to be of impact for both subsequent research endeavors in the field of information privacy as well as practitioners engaging in IIS.

2 Literature Review and Theoretical Foundation

In the following, we outline related literature streams that inform the development of our research model.

2.1 Interorganizational Information Sharing

Prior research has considered various constellations of a multi-party nature that may be inherent to information sharing. One constellation is the interdependency of private information disclosed on a social media service which may be owned by several users (e.g., a picture of two individuals posted on Facebook by one of those individuals is also owned by the other individual in that picture) (e.g., Humbert et al., 2019; Kamleitner and Mitchell, 2019; Wirth et al., 2019). Another stream of research focuses on the exchange of information between organizations with the aim of creating economic and business value (e.g., Feldman and Horan, 2011; Adjerid et al., 2018; Gopal et al., 2018). In a Marketing context, security aspects of IIS, as well as the design of requests to encourage users to opt-in to allowing an organization to engage in IIS are explored (e.g., Schneider et al., 2017; Bidler et al., 2020). What is, however, only rarely considered in theses works is the users' perspective of the exchange of user information between organizations. Exceptions to this lie in the context of patients' electronic health information sharing (Angst and Agarwal, 2009; Esmaeilzadeh, 2019, 2020) and in the sharing of citizen information in a government context (Fedorowicz et al., 2010). The sharing of user information between organizations has been referred to differently, however we will term this phenomenon IIS, and rethink the applicability of previously used constructs that explain dyadic privacy decisions to understand it further.

One concept inherent to IIS is the secondary use of information, being defined as "the practice of using data for purposes other than those for which they were originally collected" (Bélanger and Crossler, 2011, p. 1018). Our understanding of IIS is inspired by the work of Culnan (1993), who built a foundation for understanding and situating this concept. To theoretically unpack our phenomenon of IIS, we begin by introducing associated terminologies, inspired by Communication Privacy Management (CPM) Theory (Petronio, 2002). Particularly, we differentiate among three parties in IIS: (1) the user (henceforth referred to as the *information owner*) is an an individual who, as a customer of an information co-owner, shares information with the latter as part of a customer-relationship; (2) the organization that the user is currently a customer of (henceforth referred to as the *information co-owner*) is a party authorized by the information owner to have access to selected information; (3) the external organization that is interested in accessing (parts of) the co-owned information (henceforth referred to as the *information consumer*). The object 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. Figure 1 displays the process in which information flows between information owner, information co-owner, and information consumer graphically, where T0 represents the initial situation of information sharing between information owner and information co-owner, that precedes the situation where the information co-owner is engaging in IIS in T1.

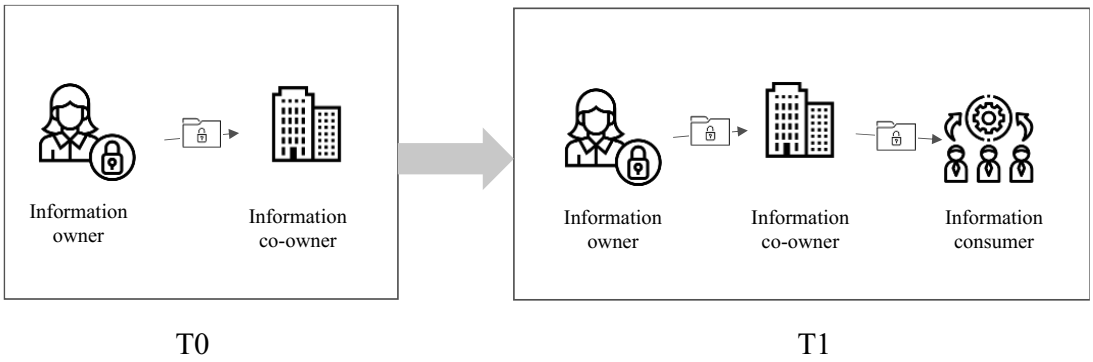

Figure 1. A process view of IIS.

We further delineate IIS from related information sharing phenomena by specifying four characteristics and associated consequences, as displayed in Table 1. IIS is mainly characterized by involving multiple stakeholders (Fedorowicz et al., 2010), and by information asymmetries between these stakeholders (Akerlof, 1970). This results in a difficulty of the information owner to assess potential actions and consequences to be expected from different stakeholders potentially accessing their information – and is multiplied by the difficulty of the information co-owner to assess potential actions and consequences to be expected from the information consumer accessing information they share with them.

Characteristic of IIS	Consequence
IIS involves multiple stakeholders	Difficulty in assessing potential actions and consequences of all stakeholders involved
Information asymmetries between information owner and information co-owner	The information co-owner assumes the role of an agent to protect the information owner's privacy
Information asymmetries between information owner and information consumer	Difficulty for the information owner to assess potential actions and associated consequences to be expected from an information consumer potentially accessing their information
Information asymmetries between information co-owner and information consumer	Difficulty for the information owner to assess the information co-owner's information sharing activities with the information consumer – they might behave in ways that the information co-owner does not know about and cannot prevent

Table 1. Characteristics of IIS.

2.2 Uncertainty

In many privacy situations, as noted by Acquisti and Grossklags (2012), it is unrealistic to assume that known probabilities over possible outcomes exist because of the high complexity and information asymmetries between information owner and information co-owner (Acquisti and Grossklags, 2012). In IIS, these complexities and information asymmetries become even more pronounced as more parties become involved in information sharing. This renders it difficult for the information owner to assess potential consequences arising from IIS. Perceived uncertainty relates to the individual's inability to evaluate these consequences as a result of imperfect information (Pavlou et al., 2007; Al-Natour et al., 2020).

Uncertainty can be associated with its source and with its content (Al-Natour et al., 2020). In IIS, the source of uncertainty may be any relationship through which an information owner's information may be accessed. The content of uncertainty refers to its object, i.e., the information practices of the party accessing the owner's information. Nesting the source and content perspectives to approach uncertainty

in IIS, we can view the source of uncertainty as two different types (privacy uncertainty and boundary uncertainty), where the content of uncertainty is different for each source.

First, uncertainty may stem from the relationship between information owner and information co-owner related to the privacy of the information shared between those two. We term this type of uncertainty as *privacy uncertainty*. Based on the conceptualization of privacy uncertainty by Al-Natour et al. (2020), we can distinguish three dimensions of content of privacy uncertainty regarding an information owner's difficulty in assessing (1) what information is collected by the information co-owner (*Collection privacy uncertainty*), (2) how this information is used by the information co-owner (*Use privacy uncertainty*), and (3) how this information is protected by the information co-owner (*Protection privacy uncertainty*).

Second, once we consider the possibility of an outside party accessing the information shared between information owner and information consumer, we speak of *boundary uncertainty*. Boundary uncertainty stems from the relationship between information owner and information co-owner, related to the privacy of the information that is subject to flowing across boundaries between information co-owner and information consumer. Our conceptualization of boundary uncertainty leans on Al-Natour et al.'s (2020) conceptualization of privacy uncertainty and is inspired by the theoretical lens of CPM theory (Petronio, 2002).

CPM theory explains how individuals manage the dialectic tension between revealing and concealing private information, based on the metaphor of boundaries as the line between public and private information. Central to this theory is the idea that an individual believes that their private information belongs to them and therefore they have the right to control where it goes. Once this individual (the information owner) grants someone else access to that information, the boundary around their personal information extends from a personal to a collective boundary. The party granted access becomes a co-owner of that information and shares responsibilities with the original owner for managing this now co-owned information, such as sharing it with an information consumer (Petronio, 2002; Child et al., 2009). CPM theory's rules for information disclosure decisions between two parties have been frequently applied in prior privacy research (e.g., Anderson and Agarwal, 2011; Karwatzki et al., 2017). More recently, studies aiming at understanding privacy situations involving more than two parties have used the perspective of collective boundaries as a theoretical lense (e.g., Lin and Armstrong, 2019; Wirth et al., 2019; Bélanger and James, 2020) – wherefore we also view this lense as appropriate to understand privacy perceptions in IIS. The three types of rules developed by Sandra Petronio to manage collective boundaries can be inferred to distinguish three aspects that the content of boundary uncertainty may relate to: an information owner's difficulty in assessing (1) who the information co-owner is sharing information collected about them with (*Boundary linkage uncertainty*), (2) what information is shared with others (*Boundary ownership uncertainty*), and (3) the conditions under which the information co-owner is sharing this information with others (*Boundary permeability uncertainty*).

These different types of uncertainty, i.e., privacy uncertainty and boundary uncertainty, relate to different stages of precedence. In general, privacy uncertainty, such as regarding the information co-owner collecting the information owner's information, forms a prerequisite for boundary uncertainty, such as regarding which information consumers this information is shared with. It is evident, that information that the information co-owner cannot access, they also cannot share with an outside party.

2.3 Control

Our distinction between different levels of precedence related to uncertainty leads our endeavor to understand more granularly how these different types and dimensions of uncertainty may be affected. Inherent to privacy and boundary uncertainty is the aspect of information asymmetries. Prior studies have attempted explain the alleviation of information asymmetries through providing the information owner with means to control their information (Pavlou et al., 2007; Dimoka et al., 2012; Al-Natour et al., 2020).

In CPM theory, based on the supposition that information belongs to the information owner, control is a central element to maintain and determine this ownership (Petronio, 2002). Exposing 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). Further, prior research on privacy control has underlined the necessity to distinguish between objective privacy control and perceived privacy control – where only perceptions of control are relevant in impacting an individuals' privacy evaluations (Brandimarte et al., 2013). Privacy control perceptions may be increased through control mechanisms that an information owner can employ. Tavani (2007) distinguishes between three aspects that an individual may control: Choice (the ability to choose how, under what circumstances, and to what degree to disclose information), consent (the ability to give consent and withdraw), and correction (the ability to correct one's data) (Tavani, 2007). Prior research has gained insights on the effects of specific instantiations of control mechanisms on privacy perceptions and sharing behavior (e.g., Burtch et al., 2015; Spiekermann and Korunovska, 2017) as well as derived design recommendations for control mechanisms (e.g., Wang et al., 2011; Lee et al., 2017; Symeonidis et al., 2018; Kamleitner and Mitchell, 2019).

In IIS, the information co-owner – as an agent to protect the information owner's privacy – can provide the information owner with control mechanisms to give them control over the information that they share with them. These control mechanisms can relate to different types: First, they may serve as means to control the flow of information between the information owner and the information co-owner. Second, they may serve as means to control the data flows between information co-owner and information consumer. Based on (Xu et al., 2012), we define *control mechanisms* as "factors that may increase [...] [the information owner's] amount of control over the release and dissemination of [...] [their] information" (Xu et al. 2012, p. 1346).

Examples for control mechanisms provided to the information owner by the information co-owner can be found for example in Facebook's privacy settings. Facebook offers various options for their users to control what information is collected about them, how it is used, or which other parties have access to it[2].

2.4 Allowing IIS

Studies on information systems privacy regarding disclosure decions involving two parties have mostly focused on disclosure intentions as the result of a privacy decision (Malhotra et al., 2004; Smith et al., 2011). Building on prior studies on privacy considering the IIS phenomenon in an electronic health information context (Angst and Agarwal, 2009; Esmaeilzadeh, 2019), we are interested in whether the information owner will allow the information co-owner to engage in IIS. This decision comes temporally after the information owner has already agreed to share information with the information co-owner to engage in a customer-relationship with them (see Figure 1). In line with previous studies on electronic health information sharing, we will consider the *intention to allow the information co-owner to engage in IIS* and define it as an opt-in decision in terms of "the extent to which the [information owner] would agree to have her information […] shared with [information consumers by the information co-owner]" (Angst and Agarwal, 2009, p. 350).

[2] https://www.facebook.com/help (2022/03/09)

3 Research Model

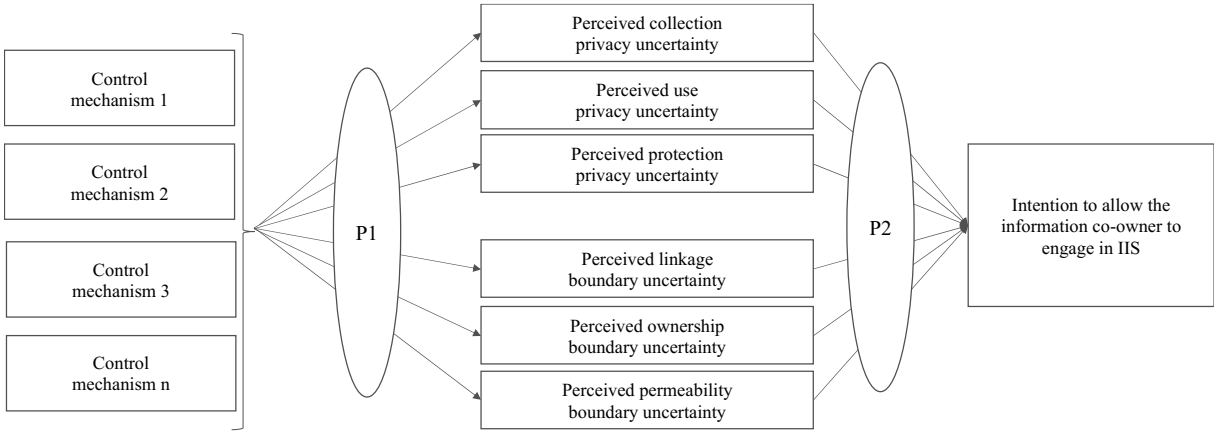

Figure 2. Research model.

Our proposed research model, as displayed in Figure 2, aims at understanding how an information owner's perceptions of privacy and boundary uncertainty are impacted by different types of control mechanisms, and how they relate to the information owners allowing the information co-owner to engage in IIS.

First, perceived uncertainty may be reduced through the users' perception of their ability to exert control over their privacy. In general, controllability is a determinant of risk-taking (Slovic, 1987). In research on information privacy, the negative relationship between control and risk has been supported widely (Xu et al., 2012). Control mechanisms reduce the perception of information asymmetries about how the information co-owner may handle the information owner's privacy through increasing perceived control. Higher perceptions of uncertainty are associated with higher information asymmetries about how the information co-owner may protect the information owner's privacy. Therefore, the presence of control mechanisms is expected to reduce perceptions of uncertainty. We expect that different types of control mechanisms affect different dimensions of perceived uncertainty differently, however, overall, negatively:

Proposition 1 (P1): C*ontrol mechanisms reduce perceptions of privacy and boundary uncertainty.*

Second, we expect that the information owner's overall perceived uncertainty impacts their intention to allow the information co-owner to engage in IIS negatively. Based on a general aversion of uncertainty and ambiguity of human beings (Ellsberg, 1961), we anticipate that information owners will try to act in ways that will reduce the potential for negative consequences by not allowing the information co-owner to engage in IIS. Within the general direction of this relationship and based on the idea of precedence, we propose that different dimensions of perceived uncertainty may interact with one another to form the information owner's intention to allow IIS. Factors which are associated with preceding levels (e.g., perceived collection privacy uncertainty) might reduce the effect of subsequent levels (e.g., perceived linkage boundary uncertainty). Our argumentation will be fully explicated in a future extension of this study. To stay within the boundaries of a research-in-progress paper, we so far formally propose:

Proposition 2 (P2): *Perceived privacy and boundary uncertainty reduce the intention to allow the information co-owner to engage in IIS.*

4 Methodology

After finalizing our research model, we will subject this model to an empirical test. We describe the procedure of the proposed empirical study below.

4.1 Planned data collection

At the current stage, our plan is to conduct a field survey to validate our research model in the context of smart fitness equipment. The survey would be run via a Germany-based provider of smart fitness equipment (machines and mobile application) on a sample of its users. IIS would be contextualized as the sharing of user information collected via different smart fitness equipment providers (such as gender, weight, training frequency, or training progress) with other providers of smart fitness equipment. Agreeing to allow IIS would provide the user benefits such as holistic training analyses and would not be necessary for the user to continue using the smart fitness equipment. This context would represent a timely instantiation of IIS that is well suited to test our research model, as it considers the complexity of involving several information consumers (several providers of smart fitness equipment) whom information owned by the information owner (a smart fitness equipment user) is shared with through an information co-owner (a provider of smart fitness equipment).

4.2 Measurement

Control mechanisms are measured through an open question, asking the user to describe each control mechanism that they are aware of. Perceived privacy uncertainty dimensions are operationalized based on the scale developed by Al-Natour et al. (2020). Measurements for different dimensions of perceived boundary uncertainty were developed through a structured scale development process (MacKenzie et al., 2011) – details of which will be part of an extended version of this research-in-progress paper. The intention to allow the information co-owner to engage in IIS is operationalized based on the measure for the intention to give information (Malhotra et al., 2004) and the measure for the intention to opt-in to electronic health information sharing (Angst and Agarwal, 2009). The survey will also collect various control variables.

4.3 Planned data analysis

Data analysis will involve two steps. First, we plan to code the qualitative data obtained through our measurement of control mechanisms inductively (Gioia et al., 2013). Second, the quantified dimensions of control mechanisms as well as the quantitative data on perceived uncertainty and the intention to allow the information co-owner to engage in IIS will then be analyzed through covariance-based structural equation modeling.

5 Potential Contribution

Through our conceptual development and our empirical study, we hope to theoretically contribute as follows: First, we shed light on the concept of IIS from the user perspective, distinguishing it from information sharing decisions with one organization, and defining this concept more broadly as to employ it to a variety of contexts. By doing so, we extend prior information privacy research through considering the complexity of information sharing relationships. Second, we gain an understanding of user perceptions of privacy that are specific to IIS as well as how those may be affected by different types of control mechanisms. Third, we view privacy perceptions interdependently. This might help future research to more granularly understand privacy decisions. Based on this increased understanding of user perceptions, practitioners can learn how to engage in value co-creation efforts through IIS, while at the same time respecting their users' privacy through providing optimal means of control.

References

Abbasi, A., Sarker, S. and Chiang, R. H. L. (2016). "Big Data Research in Information Systems: Toward an Inclusive Research Agenda." *Journal of the Association for Information Systems* 17 (2), pp. i–xxxii.

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015). "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221), pp. 509–514.

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

Adjerid, I., Adler-Milstein, J. and Angst, C. (2018). "Reducing Medicare Spending Through Electronic Health Information Exchange: The Role of Incentives and Exchange Maturity." *Information Systems Research* 29 (2), pp. 341–361.

Akerlof, G. A. (1970). "The Market for "Lemons": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84 (3), pp. 488–500.

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. 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.

Angst, C. M. and Agarwal, R. (2009). "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion." *MIS Quarterly* 33 (2), pp. 339–370.

Bélanger, F. and Crossler, R. E. (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4), pp. 1017–1042.

Bélanger, F. and James, T. L. (2020). "A Theory of Multilevel Information Privacy Management for the Digital Era." *Information Systems Research* 31 (2), pp. 510–536.

Bidler, M., Zimmermann, J., Schumann, J. H. and Widjaja, T. (2020). "Increasing Consumers' Willingness to Engage in Data Disclosure Processes through Relevance-Illustrating Game Elements." *Journal of Retailing* 96 (4), pp. 507-523.

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.

Burtch, G., Ghose, A. and Wattal, S. (2015). "The Hidden Cost of Accommodating Crowdfunder Privacy Preferences: A Randomized Field Experiment." *Management Science* 61 (5), pp. 949–962.

Child, J. T., Pearson, J. C. and Petronio, S. (2009). "Blogging, Communication, and Privacy Management: Development of the Blogging Privacy Management Measure." *Journal of the American Society for Information Science and Technology* 60 (10), pp. 2079–2094.

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

Culnan, M. J. (1993). ""How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use." *MIS Quarterly* 17 (3), pp. 341–363.

Dimoka, A., Hong, Y. and Pavlou, P. A. (2012). "On Product Uncertainty in Online Markets: Theory and Evidence." *MIS Quarterly* 36 (2), pp. 395–426.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006). "Privacy Calculus Model in E-Commerce – A Study of Italy and the United States." *European Journal of Information Systems* 15

(4), pp. 389–402.

Dinev, T., McConnell, A. R. and Smith, H. J. (2015). "Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box." *Information Systems Research* 26 (4), pp. 639–655.

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

Esmaeilzadeh, P. (2019). "An Empirical Evaluation of Factors Influencing Patients' Reactions to the Implementation of Health Information Exchanges (HIEs)." *International Journal of Human–Computer Interaction* 35 (13), pp. 1135–1146.

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

Fedorowicz, J., Gogan, J. L. and Culnan, M. J. (2010). "Barriers to Interorganizational Information Sharing in e-Government: A Stakeholder Analysis." *Information Society* 26 (5), pp. 315–329.

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.

General Data Protection Regulation (2016). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: March 9, 2022).

Gerlach, J. P., Eling, N., Wessels, N. and Buxmann, P. (2019). "Flamingos on a Slackline: Companies' Challenges of Balancing the Competing Demands of Handling Customer Information and Privacy." *Information Systems Journal* 29 (2), pp. 548–575.

Gioia, D. A., Corley, K. G. and Hamilton, A. L. (2013). "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology." *Organizational Research Methods* 16 (1), pp. 15–31.

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.

Gregory, R. W., Henfridsson, O., Kaganer, E. and Kyriakou, H. (2021). "The Role of Artificial Intelligence and Data Network Effects for Creating User Value." *Academy of Management Review* 46 (3), pp. 534–551.

Grover, V., Chiang, R. H. L., Liang, T.-P. and Zhang, D. (2018). "Creating Strategic Business Value from Big Data Analytics: A Research Framework." *Journal of Management Information Systems* 35 (2), pp. 388–423.

Grover, V. and Kohli, R. (2012). "Cocreating IT Value: New Capabilities and Metrics for Multifirm Environments." *MIS Quarterly* 36 (1), pp. 225–232.

Humbert, M., Trubert, B. and Huguenin, K. (2019). "A Survey on Interdependent Privacy." *ACM Computing Surveys* 52 (6), pp. 1–40.

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.

Karwatzki, S., Dytynko, O., Trenz, M. and Veit, D. (2017). "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization." *Journal of Management Information Systems* 34 (2), pp. 369–400.

Lee, Y.-T., Hsiao, W.-H., Lin, Y.-S. and Chou, S.-C. T. (2017). "Privacy-preserving data analytics in cloud-based smart home with community hierarchy." *IEEE Transactions on Consumer Electronics* 63 (2), pp. 200–207.

Lin, S. and Armstrong, D. J. (2019). "Beyond Information: The Role of Territory in Privacy Management Behavior on Social Networking Sites." *Journal of the Association for Information Systems* 20 (4), pp. 434–475.

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.

Pavlou, P. A., Liang, H. and Xue, Y. (2007). "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective." *MIS Quarterly* 31 (1), pp. 105–136.

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

Schneider, M. J., Jagpal, S., Gupta, S., Li, S. and Yu, Y. (2017). "Protecting Customer Privacy when Marketing with Second-Party Data." *International Journal of Research in Marketing* 34 (3), pp. 593–603.

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.

Spiekermann, S. and Korunovska, J. (2017). "Towards a Value Theory for Personal Data." *Journal of Information Technology* 32 (1), pp. 62–84.

Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J. and Preneel, B. (2018). "Collateral Damage of Facebook Third-Party Applications: A Comprehensive Study." *Computers & Security* 77, pp. 179–208.

Tavani, H. T. (2007). "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy." *Metaphilosophy* 38 (1), pp. 1–22.

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.

Wirth, J., Maier, C., Laumer, S. and Weitzel, T. (2019). "Perceived Information Sensitivity and Interdependent Privacy Protection: A Quantitative Study." *Electronic Markets* 29, pp. 359–378.

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.