# Communication Privacy Management in the Digital Age – Effects of General and Situational Privacy Concerns

*Research-in-Progress*

**Sabrina Hauff**
University of Augsburg
sabrina.hauff@wiwi.uni-augsburg.de

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

## Abstract

Internet users are increasingly concerned about their information privacy in a world with organizations that collect and combine personal information to enhance services and secret services that keep citizens under surveillance. Prior research has focused on how privacy concerns influence individuals' intentions to disclose information. However, scholars have recently challenged two assumptions. First, the sole reliance on willingness to disclose information has been questioned due to the observance of an intention-behavior gap. Second, some authors have distinguished between general and situation-specific information privacy concerns and call for more research on these concerns. Drawing from Communication Privacy Management Theory, we address both of these issues and develop a theoretical model that shows how general and situation-specific privacy concerns are raised, related, and impact information disclosure behavior. Moreover, we outline our methodology by describing how an experimental setting will be used to explore the influence of general and situation-specific privacy concerns.

**Keywords**

General privacy concerns, situational privacy concerns, communication privacy management theory, information disclosure behavior, context dependency

## Introduction

Information privacy is of growing interest in today's society. Recent topics like the NSA-affair alert people as to how their information is stored and analyzed by third parties (The Guardian 2013). Especially in an online context, people are often unknowingly sharing private information. About 70-90% of the European online population see privacy threats in an online context, but only up to 10% actively manage their privacy (BCG 2013). Similar results can be found for Americans: 89% of American adults say that they worry about information privacy at least sometimes, thereby referring to activities like shopping online, using social networks, and banking online (TRUSTe 2013).

Moreover, the topic is also of interest from an organizational perspective. Just recently, the social network Facebook bought the messaging service WhatsApp for $19 billion. However, as soon as this acquisition was announced, many German users immediately switched to other services that offer better encryption of their messages. They are afraid of major privacy and security issues when continuing the usage of WhatsApp and the inclusion of information shared on both services Facebook and WhatsApp (Dillet 2014).

From a theoretical perspective, privacy is a well-established concept. Research is done in various areas like marketing, law, management or psychology (Bélanger and Crossler 2011). Yet, the concept gained new interest with the advent of information and communication technologies, where the focus shifted

from physical privacy to information privacy (Smith et al. 2011). In addition, differences between the interests of individuals, who want to protect and control their private information, and organizations, who like to acquire as much information as possible since personalized information is very valuable for them, are intensified (Xu et al. 2011).

However, while the gap between individual's intentions and their actual behavior is well-known in other research areas (Bhattacherjee and Sanford 2009; Sniehotta 2009), previous privacy studies mainly focus on investigating how privacy concerns influence information disclosure intentions (Bélanger and Crossler 2011; Li 2011; Smith et al. 2011). They rely on the theory of reasoned action (TRA) by Fishbein and Ajzen (1975) as well as the theory of planned behavior (TPB) by Ajzen (1991) to argue that an investigation of intentions is sufficient when analyzing the outcomes of privacy concerns (Li 2012). Recent literature raises the issue of a "privacy paradox": While people state to have high privacy concerns, they do not behave accordingly. Their intentions do not match their behavior (Norberg et al. 2007). Since only a minority of studies investigates the behavior of individuals and the privacy paradox, there is a call for more research (Smith et al. 2011; Li 2011).

Moreover, prior literature raised the issue of differentiating general and situation-specific privacy concerns, arguing that macro-environmental and socio-relational factors on the one hand and organizational and task-environmental factors on the other hand pose distinct impacts on these two types of concerns (Li 2011). However, research that addresses these concerns is still limited in two ways: First of all, a clear distinction of the nature and the antecedents of these two concerns need further investigation. Second, the interplay between the two types of concerns and their influence on disclosure behavior has to be clarified.

We raise the following research questions: *How are general and situation-specific information privacy concerns related with each other? How do general and situation-specific privacy concerns influence individuals' disclosure behavior of private information?*

By addressing these questions, we attempt to contribute to the aforementioned unsolved issues by 1) focusing on the effect privacy concerns have on the actual information disclosure behavior of individuals, 2) investigating the role of general and situation-specific privacy concerns and their relationship and 3) using Communication Privacy Management Theory (CPMT) as lens to investigate privacy related behavior. This theory offers great explanatory power for our research questions and has received only limited attention (Chen et al. 2009; Metzger 2007; Xu et al. 2011). To accomplish these goals, we first provide an overview of the relevant literature regarding intentions and actual behavior, general and situational concerns, and CPMT. We then discuss our theoretical model and its accompanying hypotheses. This is followed by an explanation of our planned methodology. We conclude with a discussion of our expected contribution.

## Theoretical Background

While there are several definitions of information privacy, they have one thing in common: They typically "include some form of control over the potential secondary uses of one's personal information" (Bélanger and Crossler 2011, p. 1018), meaning that information is used for other purposes than it was collected for. The literature reviews by Bélanger and Crossler (2011), Smith et al. (2011), and Li (2012) give a thorough summary of the different research streams in information privacy. Among them is the exploration of how to define and measure privacy concerns and an investigation of privacy concern as dependent and independent variable. As can be seen, privacy concerns are used as the central construct in the existing research. They refer to the worries or anxieties that people associate with a potential loss of privacy (Bansal et al. 2010).

### *Intentions, Disclosure Behavior, and the Privacy Paradox*

Research has found that information privacy concerns affect individuals' disclosure intentions in an online context. Results are available for the willingness to share personal information with websites (Bélanger et al. 2002; Dinev and Hart 2006), intentions to use e-commerce services (Metzger 2007; Pavlou et al. 2007) and, more recently, also for social network sites (Lo and Riemenschneider 2010; Shin 2010). The postulated relationship is that the higher the concerns, the lower the intentions to share data. Relying on TRA and TPB, researchers argue that these intentions influence the actual behavior. Yet,

Bélanger and Crossler (2011) as well as Smith et al. (2011) both sum up that a privacy paradox exists in some cases: Intentions do not lead to the expected behavior but people disclose much more personal, financial, or demographic information than they intended to do (Jensen et al. 2005; Norberg et al. 2007; Premazzi et al. 2010). Potential explanations for the privacy paradox comprise bounded rationality and different mental discounting of near-term benefits and future privacy risks (Acquisti 2004), dyadic relationships (Zimmer et al. 2010), and a differentiation between general and situation-specific privacy concerns, saying that general concerns impact intentions, but can be overruled by situational cues which mainly influence disclosure behavior (Joinson et al. 2010). Next to these studies, only few others exist that actually measure the influence of privacy concerns on behavior, e.g. Metzger (2007), Jensen et al. (2005), and Norberg and Horne (2007). However, almost all studies were conducted in an e-commerce context and besides Joinson (2010), none of them differentiated between general and situation-specific privacy concerns.

## General and Situation-specific Information Privacy Concerns

While general privacy concerns refer to "an individual's [general] attitude or state of concern towards the use of their private information by companies" (Faja and Trimi 2006, p. 10), situation-specific concerns represent "the perceptions of the individual on how [a service operator] will handle personal information and how serious [he or she] is about a customer's information privacy" (Faja and Trimi 2006, p.10). The two concepts differ in their focus and in the factors which give rise to these concerns. Li (2011) suggests that general privacy concerns are mostly influenced by an individual's personal characteristics and macro-environmental factors like culture or governmental regulations, while situation-specific privacy concerns are mainly impacted by context-dependent factors like organizational and task-related aspects and an individual's interpretation of these impacts. Thus, general concerns are quite stable since their antecedents do not frequently change, while situation-specific concerns are highly dynamic, being formed within a situation depending on who the other actors are and what information is requested. Most privacy studies have either focused on investigating the relationship between general privacy concerns and behavioral intentions (e.g. Dinev and Hart 2006) or between situation-specific concerns and behavioral intentions (van Slyke et al. 2006). However, the relationship between the two concepts as well as their impact on actual disclosure behavior has received only limited attention (Li 2011, Joinson 2010). Li (2014) analyzes general and situation-specific concerns, yet general concerns are limited to the concept of disposition to privacy and the research focuses on disclosure intentions. Besides that, several authors present work on these concerns in recent research-in-progress papers (Kehr et al. 2013; Wilson and Valacich 2012), but empirical validation is still missing and thus part of the present study.

## Communication Privacy Management Theory

Several theories have been applied in privacy research, e.g. Utility Theory, Social Contract Theory, and Social Response Theory. Li (2012) gives a comprehensive overview. In our study, we apply CMPT, which is based on the fundamental work of Westin (1967, 2003) and Altman (1975, 1976), due to several reasons: First of all, the theory goes beyond a mere focus on privacy concerns. It helps to understand how concerns arise based on personal and situational factors. Moreover, it explains actual disclosure behavior and sheds light on potential repercussions if an individual's privacy is violated. Last, it takes a holistic view by investigating the relationship between discloser and recipient. Thus, CPMT is an appropriate lens that can help us to address our research questions. It is explained in detail in the following.

CPMT addresses the tension between disclosure and privacy by examining how people manage their privacy boundaries and under which circumstances they disclose or conceal private information based on a system of rules that guides disclosure decisions. The theory was originally developed to explain face-to-face or telephone-based communication (Petronio 1991), but has lately also been applied to information exchange scenarios in the internet (Child et al. 2009; Metzger 2007).

CPMT explains how people develop a set of rules over time to decide which information should be disclosed to whom in which context. Rules evolve due to repeated situations with certain actors, but can also change over time due to new environmental factors. Thereby, individuals aim at best protecting their privacy while at the same time maximizing their benefits of disclosing information (Petronio 2002). In a web context, benefits comprise e.g. the convenience of online shopping or the opportunity of self-expression and relationship management in social networks. Risks include a loss of control over private information as well as a loss of status or money if sensitive information is misused.

When a person decides to disclose information, privately owned information becomes co-owned. The involved risks lead people to erect privacy boundaries around them to control which information should become public and which should remain private. Petronio (2002) introduces three processes of boundary management: 1) Boundary rule formation, which refers to how privacy rules develop based on various aspects like situational criteria (context, motivation, risk-benefit) and personal criteria (gender, culture, personality). 2) Boundary coordination, which can be split up into the management of boundary permeability (how thick or thin the boundary is and what information is shared with whom), boundary linkage (how strongly or loosely owners are connected), and boundary ownership (who has which responsibilities and rights regarding the spread of information). 3) Boundary turbulences, which arise when boundaries are not coordinated as strictly as they should be. Thus, an individual's desired level of privacy is not maintained. In an internet context, turbulences arise when collected information is misused, stolen, or mistakenly disclosed. This can result in mistrust, uncertainty, and unwillingness to disclose information in the future.

In privacy research, CPMT has received limited attention and has only been applied in few studies, e.g. by Metzger (2007) who investigates information withholding and falsification, Chen et al. (2009) who analyze peers' disclosure of one's information, and Xu et al. (2011) who research the formulation of privacy rules considering institutional privacy assurances and risk-control assessments.

## Theoretical Model and Hypotheses

Our research model builds on the foundations described above. It is depicted in Figure 1. Disclosure behavior is modeled as an outcome of general as well as situation-specific information privacy concerns and perceived benefits of disclosing information. Moreover, several antecedents of general and situation-specific concerns are depicted. The hypotheses are developed as follows.

### *Context-independent Factors*

The concepts of general and situation-specific information privacy concerns differ in their focus, being either framed as the general tendency to worry about information privacy or the situational anxiety about information privacy that is evoked by situational cues. This distinction between general and situational beliefs was studied in other research areas as well, showing that general beliefs have an impact on situational beliefs (e.g. self-efficacy (Agarwal et al. 2000), trust (McKnight and Chervany 2002)). Even more, prior literature gives insights into how general concerns arise from context-independent factors, e.g. from privacy disposition (Li 2014), personality traits (Junglas et al. 2008), and culture values (Bellman et al. 2004). Li (2011) proposes a positive relationship between general and situation-specific concerns and suggests its empirical validation. We basically follow his argumentation: General privacy concerns describe an individual's overall fears how his or her information might be collected and misused across all contexts. They determine the fundamental beliefs of information privacy. Hence, the higher the general concerns, the higher the situational concerns and we hypothesize

*H1: General information privacy concerns positively influence situation-specific privacy concerns.*

### *Context-dependent Factors*

Perceptions about situation-specific information privacy concerns are influenced not only by general concerns but also by context-dependent factors (Li 2014, Joinson 2010). This is in line with CPMT which names two important contextual criteria that impact privacy rule formation, namely the party an individual interacts with and the information that is requested in a specific situation. We operationalize these two criteria by investigating the trustworthiness of the service operator and the sensitivity of requested information. Trust is highlighted by Joinson et al. (2010) as important factor in the relationship between the discloser and the recipient of information. Information sensitivity refers to what information is disclosed in which relationship (Petronio 2002).

Trustworthiness and trust have been identified as important factors in privacy research. In our context, trustworthiness describes the ability, benevolence, and integrity of a trustee to reliably protect an individual's personal information, while trust refers to an individual's intention to accept vulnerability to a trustee due to positive expectations regarding the trustee's behavior (Colquitt et al. 2007). However, the terms trust and trustworthiness have often been used interchangeably in privacy literature which might explain why different results have been found regarding trust. For example, trust can have a dominating
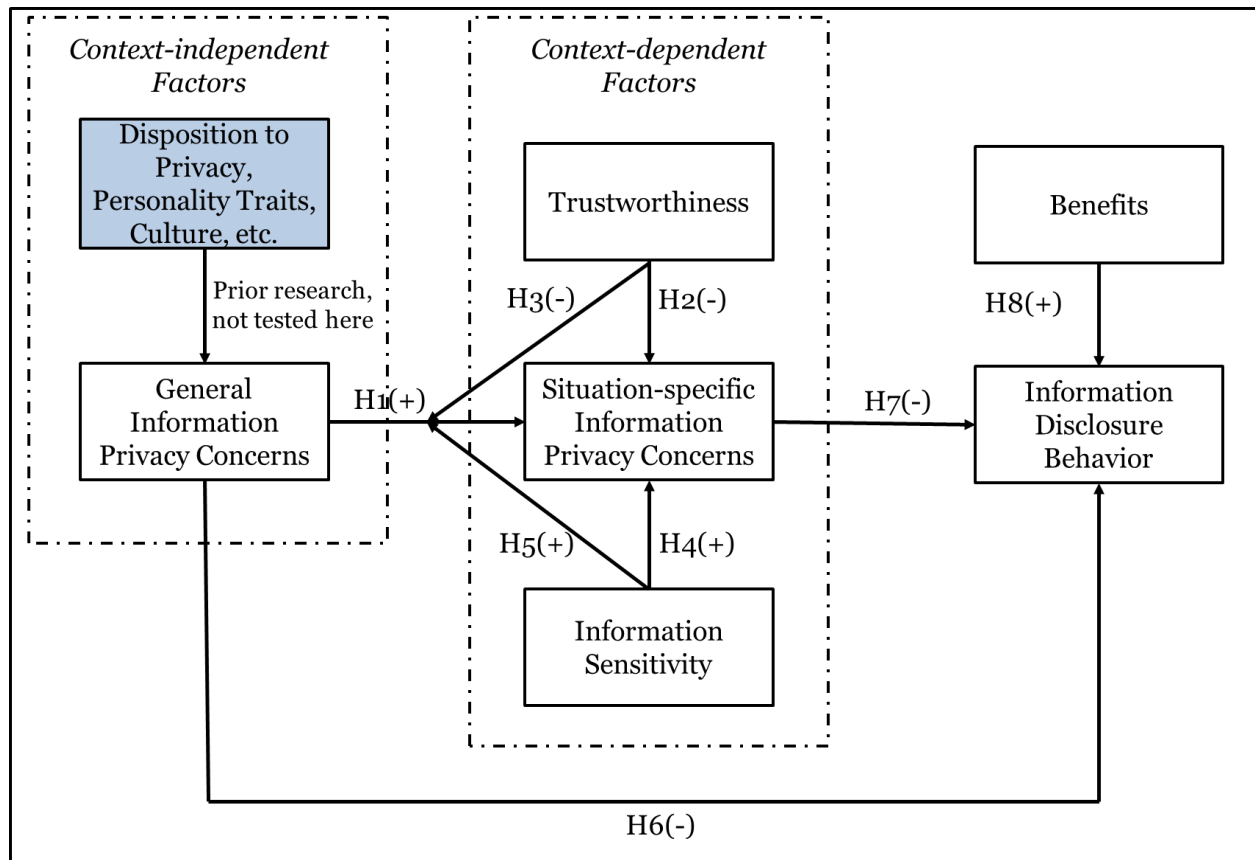
**Figure 1. Theoretical Model**

role over privacy concerns (Premazzi et al. 2010; van Slyke et al. 2006). In other studies, trust has been investigated as mediating (Joinson et al. 2010; Xu et al. 2005) or moderating variable (Bansal et al. 2010; Malhotra et al. 2004) of the relationship between privacy concerns and behavioral intentions. We investigate trustworthiness as defined above. Taking CPMT as theoretical lens, trustworthiness can be seen as contextual factor involved in rule-formation. If the website is perceived trustworthy, individuals are more likely to open their privacy boundary: they believe that the service operator is able to protect private information, does not want to harm the trustors, and adheres to moral and ethical principles. Therefore, we propose that trustworthiness lowers situation-specific concerns and moderates the relationship between general and situation-specific concerns:

*H2: The higher the trustworthiness of the service provider, the lower the situation-specific concerns.*

*H3: The positive impact of general information privacy concerns on situation-specific privacy concerns is weaker if the trustworthiness of the service provider is high.*

Information sensitivity varies with individual differences (Bansal 2010). Moreover, several studies support that information sensitivity influences privacy concerns (Bansal et al. 2010; Malhotra et al. 2004) and that participants withhold highly sensitive information to a greater extent than less sensitive information (Metzger 2007). We want to provide clarification whether sensitivity influences general or situation-specific concerns since both has been proposed (Li 2011). We suggest that sensitivity not only depends on personal characteristics but also on contextual factors. Some information might be disclosed more willingly in one context than in another, e.g. dependent on the receiver of the information or perceived repercussions of disclosure behavior. CPMT investigates this issue under the concept of boundary turbulences. They occur when private information is unknowingly and unwillingly disclosed by a co-owner of the information, leading to mistrust and uncertainty. Thus, if an individual is aware of the potential consequences of boundary turbulences and considers them severe and likely to occur, we

postulate that information sensitivity is perceived to be higher. Moreover, in case highly sensitive information is requested by a service operator, people account more importance to their general concerns if they are high, as well as vice versa. We hypothesize

*H4: The more sensitive the information requested by a service provider, the higher the situation-specific concerns.*

*H5: The positive impact of general information privacy concerns on situation-specific privacy concerns is higher if the sensitivity of requested information is high.*

### The Calculus: Risks versus Benefits

CPMT suggests that privacy boundaries are opened and closed based on rules that individuals develop over time. Aim of these rules is to find a trade-off between the risks and benefits of information disclosure. This is similar to the privacy calculus and follows prior research by assuming that users disclose more information if they perceive potential value from their behavior and if the perceived risks associated with the behavior are low (Dinev and Hart 2006; Xu et al. 2009). Yet, previous studies approximate behavior by measuring intentions even though discrepancies have been observed. We take actual behavior as our dependent variable.

A person's general as well as situation-specific privacy concerns determine the perceived risks since they describe the worries of an individual regarding information disclosure. High concerns lead to perceived high risks and thick privacy boundaries while the opposite is true for low concerns. Overall, we hypothesize:

*H6: General information privacy concerns negatively influence information disclosure behavior.*

*H7: Situation-specific information privacy concerns negatively influence information disclosure behavior.*

*H8: Perceived benefits positively influence disclosure behavior.*

## Proposed Methodology

We will employ a 2x2 between subjects experimental design, manipulating trustworthiness of the service operator and information sensitivity.

### Sample

We will use a representative sample of German adults, thereby ensuring that we include different age groups and people from different geographic locations or academic backgrounds, to name but a few criteria.

### Measurement

To ensure construct validity, scales from previous studies will be used whenever possible (for general privacy concerns: Malhotra et al. (2004), situation-specific concerns: Yi (2014), trustworthiness: Mayer and Davis (1999), information sensitivity: Metzger (2007), benefits: Xu et al. (2009)). The measures will be adapted to the context of our study. We will apply several procedures to assure the precise measurement of our constructs like defining the domain and dimensionality of our constructs, followed by ensuring construct validity and comprehensibility through the use of raters (Moore and Benbasat 1991) and analyzing content validity (MacKenzie et al. 2011). The preliminary instrument will be pilot tested, shortened, refined, and validated for its statistical properties. Moreover, we will also pilot test our manipulations (described below) to ensure that they work as intended. To measure information disclosure behavior, we will follow the suggestion of Wilson and Valacich (2012) by measuring both disclosure and the magnitude of disclosure.

### Experimental Procedure

Several weeks before the experiment, a pre-survey will be conducted to collect measures about the participants' general information privacy concerns. With the pre-survey and the experiment being apart in time, we want to avoid potential priming effects of the participants when disclosing information.

The experiment will be conducted online. It is framed as a survey about people's lifestyle. Participants will be asked different questions, for example about how they spend their leisure time and about their personal background (e.g. income, religious orientation, sexual behavior, health status, family circumstances, and contact details). Afterwards, they will be presented with an additional survey interface, saying that the surveying institution aims at improving its service and thus likes to ask several questions. Among several irrelevant items, we hide questions concerning trustworthiness, information sensitivity, and situation-specific privacy concerns.

The experiment is done in conjunction with the following two manipulations. Information sensitivity will be manipulated by either asking for non-identifiable and insensitive data, e.g. whether people do sports in their free-time and which travel destination they like best, or for highly sensitive and personal information, e.g. what their annual income is or how many sexual partners one had. Trustworthiness will be manipulated using different surveying institutions and ways of presenting the data collection. In the high trustworthiness condition, we will use a highly reputable institution like a university. A contact person as well as a privacy policy will be displayed. Overall, the survey will have a serious and professional appearance. The opposite is true for the low trustworthiness condition, e.g. using an unknown online research institute, displaying neither a contact person nor a privacy policy, and the survey appears less professional, e.g. by displaying advertisements and spelling mistakes.

## Contribution and Conclusion

Our proposed study should allow us to make several important contributions. From a theoretical perspective, first and most significantly, we contribute by clarifying the role of general and situation-specific information privacy concerns. By manipulating trustworthiness and information sensitivity, we hope to better understand how situation-specific privacy concerns are formed and how and under which conditions the influence of general privacy concerns on situation-specific concerns varies. Second, as noted in the previous sections, actual behavior has seldom been studied in privacy research, especially in a context outside e-commerce. Thus, we likely contribute by gaining insights into how general and situation-specific privacy concerns influence individuals' disclosure behavior. Third, we apply CPMT as theoretical lens to guide our hypotheses development. Since it has received only limited attention in privacy research, we like to contribute by showing that CPMT can be incorporated in this context and that it allows us to derive new insights on how privacy rules are formed and applied to disclosure decisions.

Our research also has likely practical implications. Considering individuals' high concerns about information privacy, it is of interest for people and organizations to develop a better understanding how concerns arise, how they might be manipulated, and how they influence information disclosure decisions. This knowledge allows internet users to make more conscious decisions about their privacy management and helps organizations to adjust and manage their services in a way that encourages users to share information with them.

Overall, this research seeks to expand the understanding of information privacy disclosure in an online context. It offers new contributions by empirically investigating general and situation-specific privacy concerns, their relationship, and their impact on disclosure behavior. By manipulating trustworthiness and information sensitivity, we hope to add to the body of literature on how disclosure decisions are made in the light of privacy concerns.

## REFERENCES

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the 5th ACM Conference on Electronic Commerce*, M. Kearns, McAfee, R. P., and É. Tardos (eds.), New York, USA, pp. 21–29.

Agarwal, R., Sambamurthy, V., and Stair, R. M. 2000. "Research Report: The Evolving Relationship Between General and Specific Computer Self-Efficacy—An Empirical Assessment," *Information Systems Research* (11:4), pp. 418–430.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Monterey, CA: Brooks/Cole Publishing Company.

Altman, I. 1976. "Privacy: A Conceptual Analysis," *Environment and Behavior* (8:1), pp. 7–29.

Bansal, G., Zahedi, F., 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.

BCG. 2013. "The Value of Our Digital Identity," (https://www.bcgperspectives.com/content/articles/ digital_economy_consumer_insight_value_of_our_digital_identity/; accessed January 17, 2014).

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., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *The Journal of Strategic Information Systems* (11:3), pp. 245–270.

Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *The Information Society* (20:5), pp. 313–324.

Bhattacherjee, A., and Sanford, C. 2009. "The Intention–Behaviour Gap in Technology Usage: The Moderating Role of Attitude Strength," *Behaviour & Information Technology* (28:4), pp. 389–401.

Chen, J., Ping, W., Xu, Y., and Tan, B. 2009. "Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context," in *Proceedings of the 30th Conference on Information Systems*, J. F. Nunamaker Jr. and W. L. Currie (eds.), Phoenix, Arizona, December 15-18, pp. 494-512.

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.

Colquitt, J. A., Scott, B. A., and LePine, J. A. 2007. "Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of their Unique Relationships with Risk Taking and Job Performance," *Journal of Applied Psychology* (92:4), pp. 909–927.

Dillet, R. 2014. "Bye Bye, WhatsApp: Germans Switch To Threema For Privacy Reasons," (http://techcrunch.com/2014/02/21/bye-bye-whatsapp-germans-switch-to-threema-for-privacy-reasons/; accessed February 28, 2014).

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

Faja, S., and Trimi, S. 2006. "Influence of the Web Vendor's Interventions on Privacy-Related Behaviors in E-Commerce," *Communications of the Association for Information Systems* (17), pp. 2–68.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley.

Jensen, C., Potts, C., and Jensen, C. 2005. "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior," *International Journal of Human-Computer Studies* (63:1), pp. 203–227.

Joinson, A. N., Reips, U.-D., Buchanan, T., and Schofield, C. B. P. 2010. "Privacy, Trust, and Self-Disclosure Online," *Human–Computer Interaction* (25:1), pp. 1–24.

Junglas, I. A., Johnson, N. A., and Spitzmüller, C. 2008. "Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-Based Services," *European Journal of Information Systems* (17:4), pp. 387–402.

Kehr, F., Wentzel, D., and Mayer, P. 2013. "Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect," in *Proceedings of the 36th International Conference on Information Systems,* R. Baskerville and M. Chau (eds.), Mailand, Italy, December 15-18, pp. 3355-3365.

Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of AIS* (28), pp. 453–496.

Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), pp. 471–481.

Li, Y. 2014. "The Impact of Disposition to Privacy, Website Reputation and Website Familiarity on Information Privacy Concerns," *Decision Support Systems* (57), pp. 343–354.

Lo, J., and Riemenschneider, C. 2010. "An Examination of Privacy Concerns and Trust Entities in Determining Willingness to Disclose Personal Information on a Social Networking Site," in *Proceedings of the 16th Americas Conference on Information Systems,* M. Santana, J. N. Luftman, and A. S. Vinze (eds.), Lima, Peru, August 12-15, pp. 2944-2956.

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.

Mayer, R. C., and Davis, J. H. 1999. "The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-Experiment," *Journal of Applied Psychology* (84:1), pp. 123–136.

McKnight, D. H., and Chervany, N. L. 2002. "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology," *International Journal of Electronic Commerce* (6), pp. 35–60.

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

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

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.

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. 1991. "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples," *Communication Theory* (1:4), pp. 311–335.

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

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., and Hofacker, C. F. 2010. "Customer Information Sharing with E-Vendors: The Roles of Incentives and Trust," *International Journal of Electronic Commerce* (14:3), pp. 63–91.

Shin, D.-H. 2010. "The Effects of Trust, Security and Privacy in Social Networking: A Security-Based Approach to Understand the Pattern of Adoption," *Interacting with Computers* (22:5), pp. 428–438.

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

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

Sniehotta, F. F. 2009. "Towards a Theory of Intentional Behaviour Change: Plans, Planning, and Self-Regulation," *British Journal of Health Psychology* (14:2), pp. 261–273.

The Guardian. 2013. "NSA Prism Program Taps into User Data of Apple, Google and Others," (http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; accessed August 13, 2013).

TRUSTe. 2013. "2013 TRUSTe US Consumer Confidence Index," (http://www.truste.com/us-consumer-confidence-index-2013/; accessed August 13, 2013).

Westin, A. F. 1967. *Privacy and Freedom*, New York, USA: Atheneum Press.

Westin, A. F. 2003. "Social and political dimensions of privacy," *Journal of Social Issues* (59:2), pp. 431–453.

Wilson, D., and Valacich, J. 2012. "Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus," in *Proceedings of the 33rd International Conference on Information Systems*, R. Baskerville and M. Chau (eds.), Orlando, FL, December 15-18, pp. 4152-4163.

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., and Tan, B. C. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk," in *Proceedings of the 26th Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, December 11-14, pp. 897-910.

Xu, H., Teo, H.-H., Tan, B. C., 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.

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., and Grover, V. 2010. "Knowing your Customers: Using a Reciprocal Relationship to Enhance Voluntary Information Disclosure," *Decision Support Systems* (48:2), pp. 395–406.