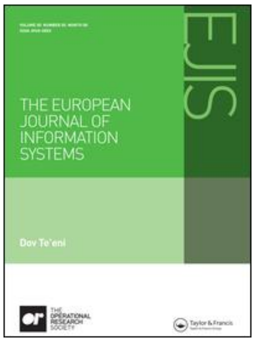

European Journal of Information Systems

ISSN: 0960-085X (Print) 1476-9344 (Online) Journal homepage: https://orsociety.tandfonline.com/loi/tjis20

Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study

Zafer D. Ozdemir, H. Jeff Smith & John H. Benamati

To cite this article: Zafer D. Ozdemir, H. Jeff Smith & John H. Benamati (2017) Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study, European Journal of Information Systems, 26:6, 642-660, DOI: 10.1057/s41303-017-0056-z

To link to this article: https://doi.org/10.1057/s41303-017-0056-z

Published online: 15 Feb 2018.

European Journal of Information Systems (2017) 26, 642–660
© 2017 The OR Society. All rights reserved 0960-085X/17
www.palgrave.com/journals

EMPIRICAL RESEARCH

Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study

Zafer D. Ozdemir[1], H. Jeff Smith[2] and John H. Benamati[3]

[1] Department of Information Systems and Analytics, Farmer School of Business, Miami University (Ohio), 800 E. High Street, Room 3011, Oxford, OH 45056, USA; [2] Department of Information Systems and Analytics, Farmer School of Business, Miami University (Ohio), 800 E. High Street, Room 3116, Oxford, OH 45056, USA; [3] Department of Information Systems and Analytics, Farmer School of Business, Miami University (Ohio), 800 E. High Street, Room 3095, Oxford, OH 45056, USA

Correspondence: H. Jeff Smith, Department of Information Systems and Analytics, Farmer School of Business, Miami University (Ohio), 800 E. High Street, Room 3116, Oxford, OH 45056, USA.
Tel: +1 (513) 529-2093;
E-mail: jeff.smith@MiamiOH.edu

Abstract
Academic studies typically view privacy threats as originating solely from organizations. With the rise of social media, such a view is incomplete because consumers increasingly face risks from peers' misuse of data. In this paper, we study information privacy in the context of peer relationships on commercial social media sites. We develop a model that considers relationships between the constructs of privacy experiences, privacy awareness, trust, risk, and benefits and how those relationships impact individuals' disclosure behaviors. We test the model by creating a survey that includes a number of measures that were taken directly from or were closely based on measures from prior studies. We conduct seven pilot tests of undergraduate students in order to validate the survey items. Working with the online survey firm Qualtrics, we gather a dataset of 314 Facebook users' responses to our validated survey, and we test our model using partial least squares techniques. We find that both privacy experiences and privacy awareness are quite significant predictors of privacy concerns. We also find that trust, risk, benefits, and privacy concerns work together to explain a large amount (37%) of the variance in disclosure behaviors. We discuss implications for practice and for future research.

European Journal of Information Systems (2017) **26**(6), 642–660.
doi:10.1057/s41303-017-0056-z; published online 26 October 2017

Keywords: privacy concerns; peer; behavioral outcomes; disclosure

Introduction

Current technologies allow companies to collect and process personal information on individuals at an unprecedented scale, and such collection and processing of data have made information privacy one of the most important ethical, legal, social, and political issues of the information age (e.g., Culnan & Bies, 2003; Lowry *et al*, 2011; Milberg *et al*, 2000; Rose, 2006). The increase in digitized personal information due to advances in Internet technologies and especially the mass adoption of social networking pose additional challenges (Angst & Agarwal, 2009; Malhotra *et al*, 2004). Across the social spectrum, there is a growing acceptance among consumers that their information privacy is no longer manageable, as confirmed by recent public opinion polls. According to Pew Research (2016), 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used. The TRUSTe/National Cyber Security Alliance US Consumer Privacy Index (TRUSTe, 2016) revealed that 45% of Internet users were more concerned about their online privacy in 2016 compared to a year earlier. These elevated concerns

Special Issue Editors:
Paul Benjamin Lowry, Tamara Dinev, Robert Willison

Received: 6 January 2016
Last Revised: 28 May 2017
Accepted: 14 June 2017

directly affect the way consumers engage with businesses online. According to a survey of 53,000 households by the US Census Bureau (Morris, 2016), privacy concerns led 45% of online households to refrain from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet.

The rise of social networking has the potential to compound these problems substantially (Ku, 2013). With more than 1 billion daily active users just on Facebook, there is a growing need to gain insight into the role that these sites play in consumers' privacy concerns (Karahasanovic *et al*, 2009). Personal interactions are becoming increasingly transparent to the general public, blurring the boundary between personal and public communication and raising concerns about online privacy (Livingstone, 2008). While individuals share a substantial amount of content on Facebook despite having concerns about privacy (Debatin *et al*, 2009), such information sharing may decline over time as Facebook and other social networking sites continue to reach wider audiences and users better understand the implications of their voluntary information disclosures.

Already, Facebook users worry about managing inappropriate friend requests and dealing with the unintended spread of information among different social groups to which one belongs created by Facebook's flattened friend hierarchy, since everyone is given access to the same personal information by default (Raynes-Goldie, 2010). Also by default, Facebook allows users to post and tag photographs of their friends without their explicit consent. While users can prescreen posts and tags about them,[1] we are not sure to what extent users take advantage of this feature. If a user does not prescreen others' posts about herself on a regular basis, an inappropriate post can be viewed until it is deleted by the owners or until the user untags herself and reports the incident to Facebook. In essence, each user profile is co-constructed through public wall posts, tagged status updates, tagged pictures, and comments (Marwick & Ellison, 2012; Vitak, 2012). This problem is exacerbated by the "warranting principle," which posits that third-party information is more believable than the information actors provide about themselves (Davis & Jurgenson, 2014). In an interesting study, Walther *et al* (2009) demonstrated that social media audiences give greater credence to other-generated content than self-generated content. Accordingly, Facebook users increasingly realize that they should not accept every friend request, that they should disclose personal information selectively, and that they should periodically "clean" inappropriate posts on their walls. In our view, Facebook's recent decision to give greater control to its users regarding their friends has been a move in the right direction.

The need for privacy research in the peer context

In a year-long ethnographic study, Raynes-Goldie (2010) noted that Facebook users distinguished between two types of privacy concern based on who or what uses personal information. Concerns about the misuse of personal information entrusted to an *institution* (company or organization) are distinct from concerns about the misuse of personal information entrusted to *peers* (individuals) within one's social domain. Raynes-Goldie (2010) found that participants in the study were more concerned about the latter than the former. Consistent with Raynes-Goldie's (2010) findings, we categorize this distinction regarding information privacy into two contexts: institutional and peer. A review of privacy research in the information systems literature reveals that privacy has been investigated almost exclusively in the institutional context and has considered individuals' perceptions of privacy-related threats only from institutions. This is because academic work has typically viewed privacy threats as originating from companies, organizations, and governments. However, with the rise of social media and social networking, it is becoming abundantly clear that such a view is incomplete, because consumers increasingly face substantial risk due to what peers can do with the data to which they are given access. Such capabilities and risks can, over time, lead to elevated levels of concern in the peer context and therefore considerably affect the way consumers interact and reveal personal information on social networking sites.

Even so, privacy researchers have devoted scant attention to concerns and behaviors associated with peers' access and use of information about others. In a set of three 2011 review articles that looked across the existing domain of privacy research (Bélanger & Crossler, 2011; Li, 2011; Smith *et al*, 2011), no examples of research associated with privacy concerns and outcomes were noted in the peer context, by which we mean peers' access to and use of information about others on asynchronous commercial social media platforms. These review articles cited a limited number of articles dealing with group-level privacy concerns, but the foci of the cited articles differ from the domain specified herein. Relying on the assumption that sharing of peer-level information began only with the emergence of social media outlets as of the mid-2000s, we examined the articles from 2006 to 2016 in the eight journals in the Senior Scholars Basket (AIS, 2016). In total, this search revealed 42 articles addressing individuals' privacy concerns regarding uses of data and the subjects' responses thereto along with three articles addressing corporate privacy policies (see "Appendix 1" section). Only two of these 42 articles developed and tested models that included any direct or indirect measures of concerns or perceived risks associated with peers' use of data subjects'

[1] See https://www.facebook.com/help/247746261926036. We thank an anonymous reviewer for pointing this out.

information and how those concerns/risks are associated with disclosure behavior in a commercial, asynchronous social media context:

- Krasnova *et al* (2010) relied on a survey of online social network users to investigate the roles of privacy concerns, trust, risk, and benefits in explaining self-reported disclosure of personal information on social networking sites. However, Krasnova *et al* (2010) distinguished between the peer and institutional contexts only in their trust scale.
- Yu *et al* (2015) surveyed a student sample to test a large model in order to understand the role of affect in determining self-disclosures on social network Web sites. As one component of this model, they included a construct called "privacy risk" that addressed peer privacy concerns in three of its four items. However, this was not the focus of the study, so there was no attempt to test an antecedent structure that might specifically address such peer privacy concerns.

Thus, to date there has been no study that has used a nonstudent sample to examine peer-level privacy concerns, antecedents thereto, and related behaviors in an asynchronous context on a commercial social networking platform. It is obvious, therefore, that privacy researchers have very seldom taken into account privacy threats that originate specifically from peers in their research models addressing individuals' behaviors on commercial social network sites, and this calls for research that complements and advances cumulative findings of privacy research in the traditional institutional context. Accordingly, we pose the following overarching research question:

> What explains individuals' peer-level information privacy concerns and disclosure behaviors in asynchronous information sharing on commercial social networking sites?

This paper makes important contributions in three areas associated with the peer context in the privacy domain. First, it represents one of the first attempts to measure peer privacy concerns and some antecedents thereto. Second, the distinct relationships between privacy concerns and privacy-related behaviors such as information disclosure are clarified in the peer context. Third, we provide additional insights into the relationships between risk, trust, benefits, and outcomes in the peer privacy context.

Background on privacy-related constructs

The APCO framework In an oft-cited interdisciplinary review of privacy research, Smith *et al* (2011) considered privacy-related studies from diverse disciplines such as information systems, economics, psychology, marketing, law, philosophy, social science, and political science. They tabulated 320 articles and 128 books and book sections that were published from the 1960s until the early 2010s. They determined that almost all privacy-related empirical research can be viewed within an "antecedents – privacy concerns – outcomes" (APCO) framework. However, those previous studies focused almost exclusively on institutional-level collection and use of personal information, not on peer-level interactions. This was not surprising given the fact that peer-level exchanges of such information emerged only within the past few years.

Even so, we view the APCO framework itself as robust enough to guide exploratory research in the peer context for two reasons. First, although no known theories have been posited for the APCO linkages in the peer context, the longstanding acceptance of the privacy concerns construct as the salient underpinning of privacy-related decision-making models suggests that it merits inclusion in an exploratory peer-focused model. Once that premise is accepted, it seems intuitively prudent to include predictably salient antecedents thereto. Further, any model of decision-making behavior should culminate with a dependent variable that is associated with an important real-world behavior. As information disclosure is one of the most frequently embraced dependent variables in empirical privacy research, it seems appropriate to embrace it in an exploratory study such as this one. Second, the simplicity of the APCO framework lends it great intuitive appeal, as it can be easily understood by researchers and practitioners alike. As an addition to this framework, we also include variables that were identified by Smith *et al* (2011) as having been considered in some previous empirical studies: trust, risk, and benefits. We certainly do not claim the APCO framework to be the only *possible* alternative for investigating privacy-related decision-making at the peer level, and we will reflect on other alternatives in the Implications for Research section. However, given that this is the first exploratory study to enter this domain, it seems to provide the most promising starting framework. Also note that, as it is impossible to postulate and test a model containing even a modest number of such antecedents in an early, exploratory study of peer privacy such as this one, we focus our attention on constructs that, in our view, are most likely to be salient in the peer context.

$A \rightarrow PC$ The antecedents to privacy concerns ($A \rightarrow PC$) linkage in the APCO framework refers to various antecedents and their effects on privacy concerns – that is, "how individual privacy concerns can be shaped" (Xu *et al*, 2011, p. 800) by antecedents. A large number of potential antecedents have been examined in the institutional privacy context: some in the category of individual personality traits (e.g., introversion/extroversion), some in the category of individuals' prior exposure (e.g., privacy awareness, privacy experiences), and some of a contextual nature (e.g., information type).[2] Rather than selecting a few individual

[2] See Smith *et al* (2011) for a review.

personality traits or contextual factors from among the myriad of options in those categories, we focus on prior exposure based on the work of Pavlou & Gefen (2005) who validated, using a psychological contract violation framework, the role of prior experience in the context of a marketplace composed of *individual* buyers and sellers. In that light, we consider how individuals' privacy awareness of privacy-related subjects (PA, (Smith *et al*, 2011) called "knowledge" by Li (2011)) and how their perceptions of previous privacy-invading experiences (PE, (Smith *et al*, 2011) called "experience" by Li (2011)) may impact their levels of privacy concern. Smith *et al* (1996) provided elementary tests using single measurement items of these constructs' relationships with institutional privacy concerns, but they have heretofore not been considered in the peer context. Thus, we propose developing multi-item measures to investigate a similar relationship in the peer context in a larger path model.

PC → O Turning to the privacy concerns-to-outcomes (PC → O) linkage in the APCO framework, all three reviews of information privacy literature (Bélanger & Crossler, 2011; Li, 2011; Smith *et al*, 2011) refer to the disclosure of personal information as an important outcome variable. This appears even more applicable in the peer than in the institutional context, since it is ultimately the disclosure of personal information that attracts users and therefore enables both commercial and nonprofit social media applications.

Trust and risk The PC → O linkage is not fully deterministic, however, as some intermediate variables such as trust and risk have been shown to have significant impacts. Despite the multitude of studies on institutional privacy concerns that include trust in their models (e.g., Bansal *et al*, 2010, 2015; Eastlick *et al*, 2006; Kehr *et al*, 2015; Metzger, 2004; Schoenbachler and Gordon, 2002; Xu *et al*, 2005), trust's role within this research stream is still unclear, with some authors viewing it as an antecedent to privacy concerns, while others view it as an outcome variable. The role of risk is even less clear, since only rarely has it been considered as an explanatory construct within the studies that focus directly on the relationship between privacy concerns and outcomes, even though, as Pavlou (2003, p. 109) succinctly argues, "the implicit uncertainty of using a global open infrastructure has rendered risk an inevitable element…." In the peer context, we expect risk and especially trust to be salient because of past research from a variety of disciplines that confirmed the role of interpersonal trust in predicting behavior, such as intention to act on recommendation (Matook *et al*, 2015), exchanging information in a virtual community (Ridings *et al*, 2002), commitment to gamers in a massive multiplayer online game community (Park & Chung, 2011), reciprocating to an investment partner (Berg *et al*, 1995), and performance in the workplace (McAllister, 1995). In short, while previous research grounded in the institutional privacy context has not fully clarified the role of trust and risk in explaining privacy-related outcomes, it is clear that they are important and generalizable constructs that likely play some role along the PC → O path in the peer context.

Benefits An additional construct that is likely salient in the peer context is the perceived benefit that consumers derive in return for disclosing personal information. In technology acceptance research, studies have found consistently that the usefulness of information technology (IT) is an important antecedent to the intention to use IT (e.g., Davis *et al*, 1989; Venkatesh & Davis, 2000). Social networks are particularly useful to their users from a peer rather than institutional perspective as they facilitate maintaining and building personal and professional relationships (Krasnova *et al*, 2010). Few individuals, if any at all, use a social network such as Facebook to find personalized products and services from institutions. While a user may find personalized content and services on Facebook through advertisements, it is much more likely for the user to use the site to benefit from peers than from institutions. We therefore expect perceived benefits to play an important role in determining behavioral outcomes in the peer context.

We reiterate that because this study is one of the first to examine privacy in the peer context across the APCO framework, we have made overt choices from among the numerous constructs that have heretofore been included in studies of the institutional context. Although we have attempted to include constructs that, in our view, will be most likely to have general explanatory power over a large domain of social media users, out of necessity other important constructs have been omitted. As we will discuss in a subsequent section on Implications for Research, we recommend that follow-on studies expand the domain of constructs under consideration.

We next develop the theoretical model and hypotheses for the study. In the following section, we describe our research method and then present the analysis and the results. We conclude with a discussion of the implications of this study for both researchers and practitioners.

Model and Hypotheses

As shown in Figure 1, the research model includes the following constructs in the peer context: privacy experiences, privacy awareness, privacy concerns, risk, trust, benefits, and information disclosure.

Because this is one of the first studies to consider peer-level information privacy concerns and disclosure behaviors in asynchronous information sharing on commercial social networking sites, there is no direct theoretical base to which we can appeal for guidance. Even so, we recognize the work of Pavlou & Gefen (2005), who considered a model of perceptions of peers' behaviors in

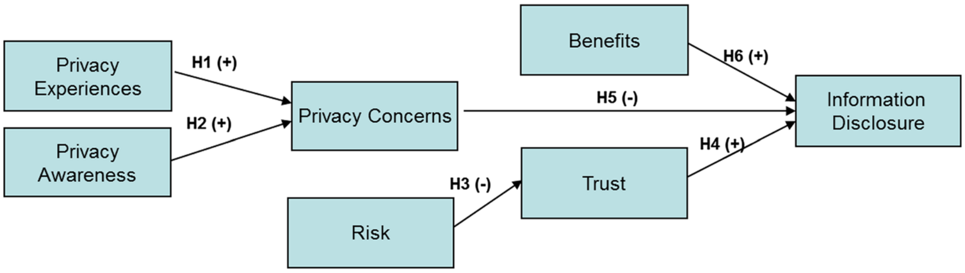

Figure 1 Peer privacy concerns research model.

an online marketplace and reactions thereto. Pavlou & Gefen (2005) relied on the concept of psychological contract violation (PCV), which had its origins in studies of organizational relationships (e.g., Morrison & Robinson, 1997; Pate & Malone, 2000; Robinson, 1996; Rousseau, 1989). "PCV may occur when people think they are not getting what they expect from a contractual agreement" (Pavlou & Gefen, 2005, p. 374), even if the expectation is grounded in something other than a legal contract – for example, an assumed or implied "contract" with a peer. Additionally, and very important when one considers individuals' responses to a larger group of peers in an online environment, "PCV changes people's emotions and attitudes, not only toward the party who they perceive did them wrong, but also toward other parties who are perceived as belonging to the same group" (Pavlou & Gefen, 2005, p. 376).

Pavlou & Gefen (2005) used PCV as a central element of dyadic relationships (that is, buyer–seller) in online marketplaces such as eBay. Their model included antecedents such as past experiences, trust and risk, the benefit-related variable price premiums, and transaction behavior as the outcome variable. Because their model was not focused on privacy concerns, per se, the analogy to the APCO framework is not a perfect one, but we argue that PCV – by virtue of its direct applicability to both individual online dyads and broader communities of peers – should also impact privacy concerns in the peer context. We therefore consider peer-level constructs and hypotheses in our own model and offer exploratory derivations of each based on the PCV-based model from Pavlou & Gefen (2005).

Privacy experiences

Just as Pavlou & Gefen (2005) found that an individual's negative prior experience(s) in buying from others in an online marketplace led to a PCV, we anticipate that individuals who have had what they perceive as negative peer privacy experiences in the past will express higher levels of concern about peer information privacy. Indeed, this has held at the institutional level: "individuals who have been exposed to or been the victim of personal information abuses…have stronger concerns regarding information privacy" (Smith *et al*, 2011, p. 998). We argue that it should also hold in the peer context.

Even if their prior negative experiences have been associated with only a limited number of peers, such as a certain Facebook friend re-sharing some information in a manner that an individual found inappropriate, we expect that the affected individual would extrapolate from that experience to their broader community of peers. By definition, peer privacy concerns emanate from a perception regarding that entire community; analogizing to PCV, such peer privacy concerns "denote…a specific perception regarding the extent to which the community…communally failed to fulfill their contractual obligations" (Pavlou & Gefen, 2005, p. 383). Hence, we analogize:

H1 *Stronger perceptions of negative privacy experiences will be associated with higher concern for information privacy in the peer context.*

Privacy awareness

Privacy awareness has been defined as "the extent to which an individual is informed about…privacy practices" (Smith *et al*, 2011, p. 998). This construct has its origins in Smith *et al*'s (1996) early instrumentation work on privacy concerns. Smith *et al* (1996) found in an institutional (rather than a peer) context that individuals who had been exposed to stories in the media or other sources about privacy matters exhibited higher levels of privacy concern. Although privacy awareness was not included in Pavlou and Gefen's (2005) model, its past inclusion in institutional models suggests that individuals may well ground their privacy concerns in what they have read or heard about peer privacy matters as in their own experiences, as was highlighted in H1 above. In essence, by reading or hearing of others' privacy experiences in the peer context, they may vicariously impute a perception of a privacy violation (analogous to a PCV). Thus, we hypothesize:

H2 *Higher levels of privacy awareness will be associated with higher concern for information privacy in the peer context.*

Peer-risk and trust

Individuals are more likely to place trust in members of a group with which they are familiar (Foddy *et al*, 2009), such as a peer group of Facebook friends. Assuming that the dyadic peer relationship is extrapolated to the larger peer community, as was supposed above and which is grounded in PCV, we argue that an individual who perceives risk associated with one or more peer relationships will tend to trust such relationships less and exercise caution when approaching them. It follows that the individual would equate such risk perceptions, from wherever they may emanate, with a heightened sense of danger and, hence, diminished trust of such relationships.

Within the framework of privacy calculus, Dinev and Hart (2006) have argued and found empirical support for the notion that the perception of increased risk lowers trust, which in turn decreases the willingness to disclose personal information to organizations. While some researchers of trust maintain that trusting beliefs enhance trusting intentions by lowering risk beliefs (Malhotra *et al*, 2004; McKnight *et al*, 2002; Pavlou & Gefen, 2005), Mayer *et al* (1995) define trust as "the willingness to assume risk" and behavioral trust as "the assuming of risk," in effect agreeing with Dinev & Hart's (2006) conceptualization that higher risk can reduce trust. In addition, empirical evidence from prior e-commerce research – albeit in the institutional context – supports the expectation of a negative relationship between risk and trust (Bansal *et al*, 2010; Jarvenpaa *et al*, 1999, 2000; Pavlou, 2003). This leads to:

H3 *Higher perceptions of risk will be associated with lower perceptions of trust in the peer context.*

Information disclosure

Although some privacy studies in the e-commerce domain have considered behavioral outcomes associated with online purchase intention/behavior (e.g., Eastlick *et al*, 2006), it is obvious that the commonly measured outcome of information disclosure intention/behavior (e.g., Sheehan, 1999) is more salient in the peer context. We also note that most researchers have chosen self-reported intentions, often with respect to a hypothetical scenario, rather than observed or even self-reported behaviors as their ultimate dependent variable (Smith *et al*, 2011). This is likely due to the difficulty associated with measuring actual behaviors in this domain, although there are some notable exceptions such as Hui *et al* (2007). However, because it is conceivable that a "privacy paradox" may exist (Norberg *et al*, 2007), it is preferable to consider behaviors, rather than intentions, as an outcome variable. To that end, we measure subjects' self-reported disclosures to peers as our outcome variable, and we link those outcomes to both trust toward peers (in H4) and peer information privacy concerns (in H5).

With respect to trust toward peers, Pavlou & Gefen (2005) found that trust toward peers in online marketplaces linked tightly to transactional behaviors in those marketplaces, and they explained this relationship using a PCV argument. So, just as higher trust led to greater involvement in online peer transactions in their study, we anticipate that higher levels of trust will lead to higher levels of information disclosure in online social communities. Similarly, increased trust in recommendations by peers led to increased intentions to act on those recommendations (Matook *et al*, 2015) and more information to be exchanged in a virtual community (Ridings *et al*, 2002). This is consistent with recent work in the institutional context which found that trust influences disclosure intentions or behaviors (Bansal *et al*, 2016; Lowry *et al*, 2014) and that trust is important in online truster–trustee relationships (Moody *et al*, 2014). Thus, we hypothesize:

H4 *A higher level of trust toward peers is related to a higher level of information disclosure in the peer context.*

Following a similar logic, it follows that higher levels of peer privacy concern will result in an analogous behavior to that observed in the Pavlou & Gefen's (2005) study – that is, individuals will respond by inhibiting the behavior that linked to such concerns. In the case of online marketplaces, that behavior is a decreased willingness to transact with peers; in the immediate context, it should be a reluctance to disclose personal information to peers. We therefore hypothesize:

H5 *Individuals with a higher concern for information privacy are less likely to disclose personal information in the peer context.*

Benefits

The nascent literature on social networking informs us regarding the various kinds of benefits users derive from interacting with their peers on these sites. One important benefit of using a social networking site is the gratification of socio-emotional needs (Rau *et al*, 2008). Relationships are vital to human beings, and individuals have the need and motivation to socially connect to others through personal interactions (Blatt, 1990; Hinde, 1979). Social networks are designed to easily maintain existing relationships and explore new ones (Zhao *et al*, 2012). One could even argue that the main function of online social networks is to satisfy "our human tendencies toward togetherness" (Weaver & Morrison, 2008, p. 100). We thus expect individuals who benefit more from the fulfillment of their social needs to disclose more information to their peers over a social networking site.

Although grounded in institutional models, previous research that relies on privacy calculus has viewed privacy-related behaviors as resulting from an individual's assessment of the costs and benefits associated with the disclosure (Smith *et al*, 2011). Dinev & Hart (2006) relied on expectancy theory (Van Eerde & Thierry, 1996; Vroom, 1964), which assumes that individuals make behavioral choices based on their expectations of the outcomes from each alternative. The decisions are frequently modeled as having multiple components, such as estimations of the desirability of each outcome, and instrumentality, which can be associated with either the relationship between outcomes or the probability of obtaining an outcome. This suggests that individuals who perceive socio-emotional benefits from peer interactions on a social network and who believe accrual of those benefits to be a likely outcome from their own information disclosures will behave accordingly. We therefore hypothesize:

H6 *Individuals who perceive more benefit from interacting with peers on a social network are more likely to disclose personal information to their peers on that site.*

Method

We relied on an online survey of Facebook users. We next discuss the data collection for that survey and the measures in that survey.

Data

Our data were collected through Qualtrics.com, an online survey software provider. Qualtrics restricted participation to Facebook users in the USA over 18 years of age. We chose Facebook friends for peers due to the popularity of this social media site and the massive amount of personal information that is shared through it. Descriptive information concerning the 314 subjects who completed the survey is shown in Table 1.

Measures

We derived measures for the majority of the constructs in the study either directly from or closely based on measures developed and validated in prior studies. All measures used a 1–5 Likert scale (see "Appendix 2" section for a list of all measurement items and scales). Table 2 summarizes the basis of the survey items for the constructs.

Inspired by the single-item measures employed by Smith *et al* (1996), we developed the items for privacy awareness (PA) and privacy experience (PE) first for the institution context and then adapted these items to the peer context by replacing "organizations" with "someone I know." Privacy concerns were derived from a combination of items from Dinev & Hart (2006), Krasnova & Veltri (2010), and Krasnova *et al* (2010). Measures for the remaining constructs (risk, benefits, and information disclosure) were derived from Krasnova *et al* (2010).

We developed and validated the items by conducting seven different pilot surveys of undergraduate students at two major US universities – one in the Midwest and one in the West. The sample sizes of these pilot surveys were 232, 175, 172, 190, 172, 129, and 118. Business students of the respective institutions were taking a required introductory Information Systems course. We used the first five samples mainly to develop the items for PA and PE and the last two to validate the peer scales for these two measures as well as to confirm the other measures adjusted from existing scales. During this iterative item development process, we assessed each measurement model by looking at the reliability of the indicators, the internal reliability of the measurement scales, and the discriminant validity of the indicators. In completing each assessment of the measures, we reviewed any items with questionable face validity to ensure that they were not essential to the meaning of the construct, and we removed the items that we deemed as nonessential and reran the PLS analysis. We carefully reworded some items for clarity and then asked another group of students to respond to the revised items. We then subjected their responses to the same PLS analysis and repeated this process until we were satisfied with the properties of the measurement items.

Table 1 Subject demographics

Demographics	*Attribute*	*N*
Gender	Male	134
	Female	180
Ethnicity	White	283
	Asian	18
	Hispanic	81
Age	Over 55	65
	46–55	65
	36–45	73
	26–35	65
	18–25	42

Table 2 Origins of measurement items

Construct	*Source*
Privacy awareness	Developed from Smith *et al* (1996)
Privacy experience	Developed from Smith *et al* (1996)
Privacy concern	Based on Dinev and Hart (2006), Krasnova and Veltri (2010), and Krasnova *et al* (2010)
Risk	Based on Krasnova *et al* (2010)
Trust	Based on Krasnova *et al* (2010)
Benefits	Based on Krasnova *et al* (2010)
Information disclosure	Based on Krasnova *et al* (2010)

We finalized the measures by examining the reliability of the indicators, the internal reliability of the measurement scales, and the discriminant validity of the indicators through the iterative sequence of PLS analyses. The resulting items became the construct scales used in the final data collection.

Analysis

Statistical analysis

We utilized a partial least squares (PLS) technique – specifically, SmartPLS version 3.2.4 (Ringle *et al*, 2015) – to both confirm the measurement model and test the hypotheses in the causal model. The use of PLS is appropriate given the exploratory nature of the study as well as the complexity of the theoretical model (Chin & Newsted, 1999; Lowry & Gaskin, 2014).

Measurement model confirmation

Using confirmatory analysis through PLS, we tested the measurement model for item and scale reliability, internal consistency, and convergent/discriminant validity. “Appendix 3” section includes the loadings and cross-loadings of all indicators on their intended and on other constructs for the model.

To demonstrate item reliability, the item loadings should ideally be higher than .707; however, slightly lower loadings for individual items are usually acceptable when loadings for other items measuring the same construct are greater than .707 (Chin & Newsted, 1999). Only two of the 37-item loadings did not exceed .707. These two items loaded between .69 and .70, and each measured constructs with multiple other items well above .707. After reviewing these two items for face validity, we decided to keep them in order to more fully capture the meaning of the constructs.

We examined the composite reliability (CR) score and the average variance extracted (AVE) for the constructs to assess scale reliability and internal consistency. CR scores greater than .70 in exploratory research or .80 in more mature streams of research indicate adequate reliability (Fornell & Larcker, 1981). The AVE scores should exceed .50 (Chin & Newsted, 1999). All of our CR scores exceeded .90, and all AVE scores were .61 or higher. The CR and AVE scores for all first-order factors are shown in Table 3.

To test for discriminant validity, we first examined item cross-loadings (see “Appendix 3” section) to ensure that each item loaded at least .10 higher on its own construct than any other construct (Gefen & Straub, 2005). We also compared the square root of the AVE for each construct with correlations of that construct with all other constructs. All square roots (in bold on the diagonal in Table 3) exceeded the correlations. All measures passed all of these tests.

To assess the extent of common method variance (CMV), researchers can include measures that are theoretically unrelated to at least one other measure in the survey. When CMV is not present, the predicted correlation between these measures is expected to be zero. Lindell & Whitney (2001) concluded that this zero correlation can be identified ad hoc in the absence of such a predetermined variable by using the smallest correlation among manifest variables in the model as a proxy for determining CMV. They propose adjusting the correlations in the measures using the determined CMV. When CMV is small or zero as predicted, the effect of the adjustment on the correlation matrix is also very small or zero. The smallest correlation between manifest variables is .001 in the model, which suggests that CMV is not a concern according to the approach described in Lindell & Whitney (2001).

Finally, to ensure that multi-collinearity was not a problem, we examined the variance inflation factor (VIF) for each combination of predictor constructs in the model. The VIFs of all combinations were less than 1.18, well below the recommended maximum threshold of 5 (Hair *et al*, 2017).

Results

Table 4 and Figure 2 show the results of the tests of our model. All six hypotheses were supported, five at the $p < 0.001$ level and the sixth at $p < 0.05$. Privacy experience influences privacy concerns (H1; $p < .001$). Privacy awareness also influences privacy concerns ($p < .001$), supporting H2. Risk strongly affects trust, supporting H3 ($p < .001$). Trust (H4), privacy concerns (H5), and benefits (H6) all significantly influence information disclosure, trust, and benefits at the $p < .001$ level and privacy concerns at the $p < .05$ level. The model also explained a large percentage of the variance in the dependent

Table 3 Reliability estimates and validity coefficients for the model

Latent construct	*CR*	*AVE*	*PA*	*PE*	*PC*	*Bn*	*R*	*T*	*ID*
Privacy awareness	.90	.65	**.81**						
Privacy experience	.93	.76	.38	**.87**					
Privacy concerns	.96	.81	.46	.34	**.90**				
Benefits	.91	.62	.02	−.06	.00	**.79**			
Risk	.94	.79	.33	.31	.39	−.06	**.89**		
Trust	.96	.84	−.08	−.25	−.27	.28	−.44	**.91**	
Information disclosure	.93	.61	−.08	.00	−.17	.55	−.20	.38	**.78**

Table 4 Hypotheses test results

Hypothesis	*Relationship*	*Path estimate*	*T Stat*	*Significance level*	*Supported*
Peer privacy concerns hypotheses					
H1	PE → PC	0.20	4.11	<.001	Yes
H2	PA → PC	0.39	7.78	<.001	Yes
H3	R → T	−0.44	8.14	<.001	Yes
H4	T → ID	0.22	3.76	<.001	Yes
H5	PC → ID	−0.11	2.14	<.05	Yes
H6	Bn → ID	0.48	11.06	<.001	Yes

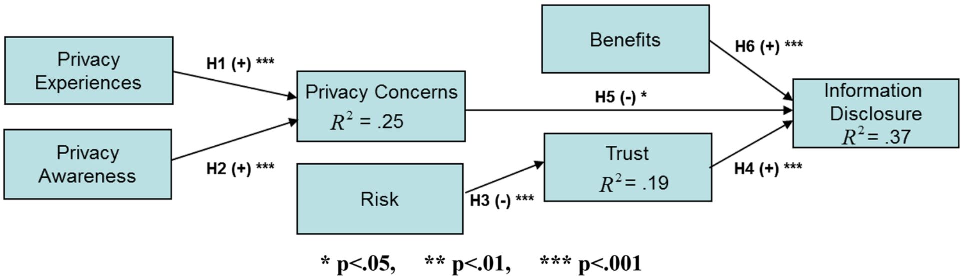

Figure 2 Results.

variables: R^2 values were .25, .19, and .37 for privacy concerns, trust, and information disclosure, respectively. By all indications, the model very strongly represents the data collected from our random sample of Facebook users.

Discussion

This paper makes important contributions in three areas. First, it represents one of the first attempts to measure privacy concerns and some antecedents thereto in the peer context. Second, the distinct relationships between privacy concerns and privacy-related behaviors have been clarified in the peer context. Third, we have provided additional insights into the relationships among risk, trust, and benefits in the privacy domain.

In the next section, we consider the implications for practice. We then discuss some limitations of this study and reflect on potential avenues for future research.

Implications for practice

From a practical standpoint, the important implications from this study are from the perspective of commercial providers of social networking platforms in which peers interact in an asynchronous mode. Disclosure of personal information to peers stands as a critical success factor in these providers' business models, so they must be alert to any factors that either impede or incite such disclosure behavior. In our opinion, the most readily addressed constructs will likely be perceived risks and perceived benefits.

Perceived risks associated with peers' behavior, which impact levels of trust and, in turn, disclosures, can be dampened by providing more granular control opportunities for individuals as they disclose their personal information. Of particular note is the ability to easily group one's peers so that information sharing can be easily contextualized to small groups. Also, increased granularity in controls at the individual level can be provided; for example, a social media user could be allowed to control who can and cannot see his/her pictures, who can "tag" him/her, which peers or groups of peers can have access to limited information such as status updates rather than deeper information. Particularly if such control options are linked to a simplified grouping structure, this should provide for greater control over use and reuse of personal information among one's peers. Accordingly, the recent decision by Facebook to allow greater control over the "following" of peers, which deepens the granular options, was a wise one.

Perceived benefits in peer social networks can be increased by providers' realization that individuals are more likely to disclose personal information with those whom they feel a connection. This suggests that further investments in tools that scrutinize the web of an individual's existing relationships to suggest new peer relationships may be fruitful. Similarly, tightened algorithms to target information (as in news feeds) that prompt additional sharing among peers and careful avoidance of missteps that could lead to negative experiences or the awareness of them could prove worthy areas for investment.

The constructs of privacy awareness and privacy experiences in the peer context may prove to be especially frustrating to providers because they represent the accrual – over time and from numerous experiences – of individuals' exposure to various peer situations and accounts from others regarding the domain. Since these constructs represent individuals' composite responses to numerous factors, no single provider can directly control either. Even so, a provider can take steps to minimize negative and maximize positive factors associated with both of these factors.

Regarding privacy experiences, a provider can, at a minimum, work to educate its own users regarding expectations. For example, prior to allowing new users to register in the social networking domain or renewing an existing membership, users could be required to agree to a statement that details privacy-related expectations with respect to the information provided by others. In addition, providers may include in their own policies a provision for disciplining or expelling users who do not meet these norms, and they can add a mechanism that enables easy reporting of privacy abuses. Also, a provider can implement additional measures to increase users' perceptions of control via "notice" and "choice" (Culnan & Bies, 2003, p. 331). For example, as they post, users can be shown a pop-up box that explains the extent of distribution of their posted comments. The pop-up box could note that, absent any further action on the user's part, the posted comments will be viewable not only by their online friends but also – under certain conditions – by those friends' friends.[3] At that point, the user could be given the option of restricting the viewing of the post to their own friends or even a subset thereof. Providing these options to the users is ultimately in the interest of providers, since ongoing privacy abuses may very well lead victims of these abuses to limit their information disclosure to their peers, as shown by this study. In addition to those actions that providers can take on their own, they can work together with industry groups to formulate a coordinated educational response and to promulgate a clear set of general statements regarding online peer-related behavior that should generalize across providers and sites.

Regarding privacy awareness, as this construct is in many respects a function of media attention and the viral nature of information sharing today, providers can invest in industry initiatives to highlight positive efforts such as those mentioned above. While care should be taken to avoid cynical initiatives that could suggest an industry unwillingness to confront its own obligations regarding privacy, it could prove worthwhile to engage in industry-wide public relation efforts to both educate media representatives and clarify the protections that are in place.

Although the above suggestions were targeted narrowly to the domain of this study (i.e., commercial social network providers in an asynchronous context), it should be noted that peer privacy concerns are increasingly moving beyond social acquaintances and relatives to include professional peer relationships. Social media usage has altered how individuals interact with each other in their professional dealings (Mello, 2012). Organizations increasingly use social media as a professional work tool to generate value by enabling information and knowledge sharing as well as supporting innovation, creativity, and collaboration among employees on corporate intranets (Mangelsdorf, 2007; Pettersen & Brandtzaeg, 2012). As organizations rely more on social media internally, the need to understand the nature of privacy concerns and their influence on behaviors elevates.

Implications for research

We partition our discussion of implications for research into three parts: important implications based on a finding from this study, incremental additions to enhance the existing framework, and theoretical reconsiderations.

Implications based on a finding from this study In our view, the most important finding from this study that should have immediate implications for other peer-level studies is this: Both previous privacy experiences and privacy awareness are very important constructs in the peer privacy context. Previously, these two constructs had received very limited attention in the literature (e.g., Pavlou & Gefen, 2005; Smith *et al*, 1996), but the fact that they together explained 25% of the variance in peer privacy concerns suggests that they are quite salient in peer-level modeling. We strongly encourage other researchers who are entering this domain of privacy-related decision-making in the peer context to include both privacy experiences and privacy awareness in their models.

Incremental additions to enhance the existing framework In keeping with the tradition in information privacy research, we embraced the APCO framework in this study, by considering certain antecedents, privacy concerns, and behavioral outcomes. As will be discussed in the next subsection, there may well be other theories that could prove suitable in the peer context. However, assuming some researchers prefer to extend this current stream, we consider three areas in which incremental additions to the existing framework are warranted: additional constructs, measurement, and institutional–peer interactions.

First, because this was one of the first studies to consider perceptions and behaviors in the peer context of the privacy domain, we included only a limited number of constructs in both the "antecedent" (A) and "outcomes" (O) components of the APCO framework

[3] This second-order viewing is often possible when a user's friend comments on his or her post. The friend's friends are then able to see not only the comment but also the original post.

along with risk and trust. Further, we included only one additional variable: benefits. As shown in Tables 5, 6, and 7, however, numerous other constructs have been identified in review articles of the institutional context. We have indicated which of these constructs, in our estimation, have the highest likelihood of proving salient in the peer context.

Table 5 Antecedents to privacy concerns

Source	*Antecedents*
Bélanger and Crossler (2011)[a]	Group dynamics
	Individual differences (*)
	Demographics (gender, age, education)
	Self-efficacy
	Personality traits (e.g., amicability)
	Government involvement (*)
Li (2011)[b]	Individual factors: (*)
	Demographic
	Personality traits
	Knowledge and experience
	Computer anxiety
	Computer self-efficacy
	Need for privacy
	Social-relational factors: (*)
	Social norms
	Macro-environmental factors:
	Culture
	Governmental regulations (*)
	Organizational and task environmental factors:
	Reputation
	Privacy interventions
	Social presence
	Information contingency: (*)
	Information sensitivity
	Types of information
Smith *et al* (2011)	Privacy experiences (*)
	Privacy awareness (*)
	Culture/climate (*)
	Demographic differences: (*)
	Gender
	Age
	Ethnicity
	Education
	Income
	Personality differences: (*)
	Introversion/extroversion
	Independent-self/interdependent-self
	"Big Five" personality traits
	Social awareness

Entries in Tables 5, 6, and 7 represent our own interpretations of the authors' references in their figures and text. For the purposes of documenting Bélanger & Crossler (2011)'s model, we include not only the constructs that are shown in Figure 2 but also other constructs that are referenced in their text.

[a] Bélanger & Crossler (2011) include separate constructs for "group" and "individual" privacy concerns. We have included all variables that are antecedents to *either* of these types.

[b] Li (2011) includes separate constructs for "general," "specific," and "societal" privacy concerns. We have included all variables that are antecedents to *any* of these types.

(*) Recommended for peer context.

Table 6 Mediators/moderators between privacy concerns and intentions/behaviors

Source	*Mediators/moderators/external variables*
Bélanger and Crossler (2011)	Fair information practices (moderator)
	Internet literacy (moderator)
	Individual differences (moderator)
	Monetary incentives (moderator)
	Trust (mediator) (*)
	Risks (mediator) (*)
Li (2011)	Trust (mediator) (*)
	Risks (mediator) (*)
	Perceived benefits (*)
Smith *et al* (2011)	Risks (mediator) (*)
	Benefits (mediator) (*)
	Trust (mediator and moderator) (*)
	Privacy notice/seal (mediator)

(*) Recommended for peer context

Most promising will likely be those associated with individual-level traits. In past research, personality differences such as introversion versus extroversion (Lu & Hsiao, 2010), independent-self versus interdependent-self (Xu, 2007), and social awareness (Dinev & Hart, 2006) have been shown to be associated with individuals' institutional privacy concerns, and it is reasonable to assume that similar relationships should hold for at least some of these constructs in the peer context. Additionally, some contextual factors identified by other researchers since the review articles' publication in 2011 could well prove salient in the peer context. Such factors include the level of perceived control over personal information (Xu *et al*, 2012), the privacy assurance alternatives that are provided to users (Zhao *et al*, 2012), and the levels of image discrepancy, decision control, and overlap in social networks (Chen *et al*, 2015). In addition to serving as combined antecedents to privacy concerns, such factors could potentially moderate other relationships in a behavioral model. Further exploration of these constructs seems to be a promising avenue.

Second, much fruitful work could be done to create and validate measurement scales for constructs in the peer context such as privacy awareness, privacy experiences, privacy concerns, benefits, risks, and information disclosure. In this study, we followed the generally accepted path for research at this juncture (i.e., exploration and testing of previously unconsidered models) and developed new measures for some peer-related constructs. Importantly, we confirmed that our measures exhibited both convergent and discriminant validity. Even so, to the extent that researchers wish to publish pure "instrumentation" articles, well-documented guidelines for creating and validating such scales exist (Straub, 1989; Straub *et al*, 2004). Some

Table 7 Privacy-related intentions/behaviors

Source	*Intentions/behaviors*
Bélanger and Crossler (2011)	Willingness to share information with e-commerce merchants or e-government agencies Willingness to participate in e-commerce or e-government interactions Preferences for regulatory environments (*) Willingness to be profiled (*) Falsification of personal information (*) Identity modification Use of privacy protection software Creation of privacy tools and technologies
Li (2011)	Provide information for transactions Protect information (*)
Smith *et al* (2011)	Willingness to disclose information (*) Willingness to engage in commerce Regulation preferences/actions: (*) Privacy as a right/commodity Self/government regulation

(*) Recommended for peer context

steps in those guidelines, such as purification of constructs, are not normally included in studies at this juncture, but could be added. "Instrumentation" articles that document the development of such scales would serve as a major contribution to the literature.

Third, it is conceivable that there could be interactions between individuals' perceptions of an institution and the individuals' behaviors toward peers within that institution's social network. The complexities of such interactions go beyond the threshold of existing theories, but this would be a fruitful area for additional exploration.

Theoretical reconsiderations The above discussion was concerned with incremental additions that could enhance the APCO framework in the peer context. However, it may well be that the APCO framework, while having stood the test of time as an organizing template in the institutional context, may not prove the most salient for the peer context. In that light, we offer three suggestions for theoretical reconsiderations.

First, an appeal to additional theoretical bases in social psychology could prove fruitful. Because the "peers" in the peer context could be numbered as few as one or as many as dozens, it would appear that two different streams of social psychological theory might be relevant: dyadic and group. Dyadic theories are associated with perceptions and behaviors between two individuals (Moreland, 2010). Such theories would readily apply in the world of instant messaging and in situations where an individual is concerned about perceived misuse of his or her personal information by others who have access to such information.

More helpful in many situations in the peer context will be social psychological theories associated with small groups. As explained by Witte (2013), there are four different approaches to small group research, but in our view only two of them would lend themselves well to application in the peer context. The first would be sociological small group research, in which studies might focus on rules and roles in a peer network and how they impact behavioral outcomes. For example, if a rule or norm within an online peer group was "do not share anything said in this group with others," then this might well impact disclosure behaviors of group members. The second would be the applied version, in which studies would focus on "specific circumstances, people with idiosyncratic motivation, and a particular aim to be reached" (Witte, 2013, p. 3). Since most peer groups in social networks have some aim such as discussion of a shared hobby and their share of "people with idiosyncratic motivation," this version of small group theory might prove useful in the peer context.

Second, theories regarding individuals' cognitive decision-making approaches could prove helpful in the peer context. Earlier, following the precedent set by Dinev & Hart (2006), we briefly invoked expectancy theory (Van Eerde & Thierry, 1996; Vroom, 1964) in the context of the existing APCO framework. However, it is conceivable that this theory – if applied fully into the peer context – could provide an enlightened approach to modeling individuals' behavioral choices without requiring the assessment of privacy concerns. We might expect the subjects to make information disclosure decisions by considering the (un-)desirability of each potential outcome as well as the likelihood of each such outcome. For example, a subject might view making a new friend as a desirable outcome and having his or her personal information revealed inappropriately to a larger audience as an undesirable outcome, and (s)he might estimate the probability of each such outcome. Obviously, subjects would have to expend cognitive energy in such estimations, and studies might consider not only their actual behavioral decisions but also the factors that determine the level of cognitive energy they are willing to expend. Such an approach might mimic that taken in some privacy calculus studies, which often are only loosely linked to privacy concerns as demonstrated by Smith *et al.* (2011). Expectancy theory, however, is more easily adapted to a dyadic, peer level than is privacy calculus, at least as it has been applied in the past.

Another alternative might be the elaboration likelihood model (ELM) (Petty & Cacioppo, 1986), which holds that individuals' decision-making occurs along two different routes, which may be intermingled: a "central" route, in which high levels of cognitive effort are expended, and a "peripheral" route in which lower levels of cognitive effort are observed. Even on the "central" route, individuals may fall prey to cognitive biases and shortcuts that limit their ability to make purely rational judgments (Acquisti *et al*, 2015; Dinev *et al*, 2015). To the best of our knowledge, only the studies by Acquisti and colleagues (Acquisti, 2004; Acquisti & Grossklags, 2005; Acquisti *et al*, 2012; Tsai *et al*, 2011) and by Li and colleagues (Li *et al*, 2011; Li *et al*, 2008; Li, 2011) have relaxed the covert assumption that decisions are being made with high cognitive effort and without bias, and those studies were grounded in the institutional context. Especially in the peer context, it is likely that mood and emotions will be salient. These two constructs are commonly subsumed under the rubric of affect and are known to partially determine the extent to which the “central” and “peripheral” routes are employed (Petty & Wegener, 1998). Thus, it would behoove researchers to consider the extent to which low-effort processes and cognitive biases and shortcuts are at play in individuals’ decision-making within the peer context.

Third, much knowledge could be gained through temporal studies of the process through which peer-related concerns develop and then manifest themselves in behavioral outcomes. To date, only a few examples of process-based, privacy-oriented research exist, and all have been in the institutional context [e.g., Smith (1994)]. In this study, we focused solely on a cross-sectional variance model, which provided a “snapshot” of a phenomenon. We did not consider the passage of time or events that lead to changes of state. Generally speaking, process modeling requires a long-term research commitment to data gathering. Often through interviews, researchers attempt to clarify the trigger events that lead to different states of perception or behavior. Most often, process modeling is done in an organizational context, although it is certainly conceivable that researchers could attempt such a study to consider changes in individuals’ perceptions and behaviors. In the peer context, a process modeling initiative might involve an examination of changes in individuals’ levels of peer-directed concern and their behavior, over time, as they engage in social media contexts. One could envision, for example, a long-term interview schedule that allowed a researcher to follow individuals who engaged with social media applications with higher and lower levels of peer-related risks and benefits. How the individuals perceived the changes, and how they varied their behavior in response, would likely yield rich inferences. Researchers who would be willing to devote the time and energy required to address these processes in the peer context could find that their return on that investment is a huge one.

Limitations

Although the study’s findings are strong, we do note three possible limitations of the study. First, this study relies on self-reported rather than measured behaviors. It is conceivable that individuals may misreport their own behaviors, either in an attempt at self-justification or simply because of cognitive constraints. We note, however, that our Facebook-related survey items are quite specific and are less subject to such misreporting than are general self-reported items. While controlled laboratory studies might be of some use in extending our understanding of these phenomena, we argue that self-reporting of specific behavioral details provides external validity to this study.

Second, and related, it might be argued that there could be a demand effect because subjects were asked questions about privacy concerns prior to being asked about their actual behaviors on Facebook. We counter, however, that the combination of our specific queries about actual behaviors combined with our tests for common method bias should dampen such concerns. At worst, any demand effect should be less than what might be evident when measuring stated intentions, which is more commonly done than measuring behaviors in studies such as this one.

Finally, some might consider our US-based sample to be a limitation. However, to secure an international sample with broad demographics would be very difficult, particularly in light of language differences. In our view, our ability to generalize from a broad, nonstudent sample (albeit from within a single culture) justifies our approach.

Conclusion

To the best of our knowledge, this is the first study to consider the formulation of, and self-disclosure behavioral outcomes associated with, privacy concerns in the peer context. We found that perceptions and concerns in the peer context are very salient in driving individuals’ privacy-related behavioral choices on Facebook. Our findings open a door into a new domain of research, with potential for enlightening practitioners regarding their options, and the limits thereon, in influencing users’ behaviors, particularly in social media settings. Of course, much work remains to be done. We hope that other researchers will join us in considering this important domain of privacy research.

About the Authors

Zafer D. Ozdemir is a Professor at the Farmer School of Business, Miami University. His research focuses on economics of e-commerce and has appeared in scholarly journals such as *Information Systems Research*, *Journal of MIS*, *Decision Sciences*, *Decision Support Systems*, *Information & Management*, and *Communications of the ACM*, among others.

H. Jeff Smith is the George and Mildred Panuska Professor in Business in the Farmer School of Business at Miami University in Oxford, Ohio. His research focuses on ethical, societal, and regulatory issues associated with strategic uses of information technology. His research has appeared in many highly ranked journals.

John H. Benamati is a Professor of Information Systems and Chair of the Information Systems and Analytics Department at the Farmer School of Business, Miami University, Oxford, Ohio, USA. His major research and teaching interests are e-commerce trust, changing IT, information privacy, and IT management/strategy.

References

Acquisti A (2004) Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Electronic Commerce Conference*, pp 21–29, ACM Press, New York, NY.

Acquisti A, Brandimarte L and Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* **347**(6221), 509–514.

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

Acquisti A, John L and Lowenstein G (2012) The impact of relative standards on the propensity to disclose. *Journal of Marketing Research* **49**(2), 160–174.

AIS (2016) Senior scholars' basket of journals. http://aisnet.org/?SeniorScholarBasket. Accessed on August 30, 2016.

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

Angst CM 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), 339–370.

Awad NF and Krishnan MS (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* **30**(1), 13–28.

Bansal G, Zahedi FM 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), 138–150.

Bansal G, Zahedi FM and Gefen D (2015) The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems* **24**(6), 624–644.

Bansal G, Zahedi FM and Gefen D (2016) Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management* **53**(1), 1–21.

Bélanger F and Crossler R (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* **35**(4), 1017–1041.

Berg J, Dickhaut J and Mccabe K (1995) Trust, reciprocity, and social history. *Games and Economic Behavior* **10**(1), 122–142.

Blatt SJ (1990) Interpersonal relatedness and self-definition: Two personality configurations and their implications for psychopathology and psychotherapy. In *Repression: Defense mechanisms and personality* (Singer JL, Ed), pp 299–335, University of Chicago Press, Chicago, IL.

Chellappa RK and Shivendu S (2007) An economic model of privacy: A property rights approach to regulatory choices for online personalization. *Journal of Management Information Systems* **24**(3), 193–225.

Chen J, Ping JW, Xu Y and Tan BCY (2015) Information privacy concerns about peer disclosure in online social networks. *IEEE Transactions on Engineering Management* **62**(3), 311–324.

Chin WW and Newsted PR (1999) Structural equation modeling analysis with small samples using partial least squares. In *Statistical strategies for small sample research* (Hoyle R, Ed), pp 307–341, Sage Publications, Thousand Oaks, CA

Choi BCF, Jiang J, Xiao B and Kim SS (2015) Embarrassing exposures in online social networks: an integrated perspective of privacy invasion and relationship bonding. *Information Systems Research* **26**(4), 675–694.

Conger S, Pratt JH and Loch KD (2013) Personal information privacy and emerging technologies. *Information Systems Journal* **23**(5), 401–417.

Culnan MJ and Bies RJ (2003) Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues* **59**(2), 323–342.

Davis FD, Bagozzi RP and Warshaw PR (1989) User acceptance of computer technology: A comparison of two theoretical models. *Management Science* **35**(8), 982–1003.

Davis J and Jurgenson N (2014) Context collapse: theorizing context collusions and collisions. *Information, Communication & Society* **17**(4), 476–485.

Debatin B, Lovejoy JP, Horn A and Huges BN (2009) Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* **15**, 83–108.

Dinev T, Bellotto M, Hart P, Russo V, Serra I and Colauti C (2006) Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems* **15**, 389–402.

Dinev T and Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research* **17**(1), 61–80.

Dinev T, Hart P and Mullen MR (2008) Internet privacy concerns and beliefs about government surveillance: an empirical investigation. *Journal of Strategic Information Systems* **17**(3), 214–233.

Dinev T, Mcconnell AR and Smith HJ (2015) Informing privacy research through information systems, psychology, and behavioral economics: thinking outside the 'APCO' box. *Information Systems Research* **26**(4), 639–655.

Dinev T, Xu H, Smith HJ and Hart P (2013) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* **22**(3), 295–316.

Eastlick MA, Lotz SL and Warrington P (2006) Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment. *Journal of Business Research* **59**(8), 877–886.

Foddy M, Platow MJ and Yamagishi T (2009) Group-based trust in strangers: the role of stereotypes and expectations. *Psychological Science* **20**(4), 419–422.

Fornell C and Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* **18**(1), 39–50.

Gefen D and Straub DW (2005) A practical guide to factorial validity using PLS-graph: tutorial and annotated example. *Communications of the Association for Information Systems* **16**(5), 39–50.

Gerlach J, Widjaja T and Buxmann P (2015) Handle with care: how online network providers' privacy policies impact users' information sharing behavior. *Journal of Strategic Information Systems* **24**(1), 33–43.

Greenaway KE, Chan YE and Crossler R (2015) Company information privacy orientation: a conceptual framework. *Information Systems Journal* **25**(6), 579–606.

Hair JF, Hult GTM, Ringle CM and Sarstedt M (2017) *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM),* Sage Publications, Inc., Thousand Oaks, CA.

Hann I-H, Hui K-L, Lee S-YT and Png IPL (2007) Overcoming online information privacy concerns: an information-processing theory approach. *Journal of Management Information Systems* **24**(2), 13–42.

Hinde RA (1979) *Toward Understanding Relationships*, Academic Press, London.

Hong W and Thong JYL (2013) Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly* **37**(1), 275–298.

Hu T, Kettinger WJ and Poston RS (2015) The effect of online social value on satisfaction and continued use of social media. *European Journal of Information Systems* **24**(4), 391–410.

Hui KL, Teo HH and Lee SYT (2007) The value of privacy assurance: an exploratory field experiment. *MIS Quarterly* **31**(1), 19–33.

Jarvenpaa SL, Tractinsky N, Saarinen N and Vitale M (1999) Consumer trust in an internet store: a cross-cultural validation. *Journal of Computer-Mediated Communication* **5**(2), 44–71.

Jarvenpaa SL, Tractinsky N and Vitale M (2000) Consumer trust in an internet store. *Information Technology Management* **1**, 45–71.

Jiang J, Heng CS and Choi BCF (2013) Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research* **24**(3), 579–595.

Junglas IA, Johnson NA and Spitzmueller 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), 387–402.

Karahasanovic A, Brandtzæg PB, Heim J, Lüders M, Vermeir L, Pierson J *et al* (2009) Co-creation and user-generated content – elderly people's user requirements. *Computers in Human Behavior* **25**(3), 655–679.

Kehr F, Kowatsch T, Wentzel D and Fleisch E (2015) Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal* **25**(6), 607–635.

Keith MJ, Babb JS, Lowry PB, Furner CP and Abdullat A (2015) The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal* **25**(6), 637–667.

Krasnova H, Spiekermann S, Koroleva K and Hildebrand T (2010) Online social networks: why we disclose. *Journal of Information Technology* **25**, 109–125.

Krasnova H and Veltri NF (2010) Privacy calculus on social networking sites: explorative evidence from Germany and USA. In *43rd Hawaii International Conference on System Sciences, Hawaii.*

Ku Y (2013) Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan. *Information & Management* **50**(7), 571–581.

Lee D-J, Ahn J-H and Bang Y (2011) Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. *MIS Quarterly* **35**(2), 423–444.

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

Li H, Sarathy R and Zhang J (2008) The role of emotions in shaping consumers' privacy beliefs about unfamiliar online vendors. *Journal of Information Privacy & Security* **4**(3), 36–62.

Li T and Unger T (2012) Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems* **21**(6), 621–642.

Li Y (2011) Empirical studies on online information privacy concerns: literature review and an integrative framework. *Communications of the Association for Information Systems* **28**(1), 453–496.

Lindell MK and Whitney DJ (2001) Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology* **86**(1), 114–121.

Livingstone S (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression *New Media Society* **10**(3), 393–411.

Lowry PB, Cao J and Everard A (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures. *Journal of Management Information Systems* **27**(4), 163–200.

Lowry PB and Gaskin J (2014) Partial least squares (PLS) structural equation modelling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it. *IEEE Transactions on Professional Communication* **57**(2), 123–146.

Lowry PB, Wilson DW and Haig WL (2014) A picture is worth a thousand words: source credibility theory applied to logo and website design for heightened credibility and consumer trust. *International Journal of Human–Computer Interaction* **30**(1), 63–93.

Lu HP and Hsiao KL (2010) The influence of extro/introversion on the intention to pay for social networking sites. *Information & Management* **47**(3), 150–157.

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

Mangelsdorf ME (2007) Beyond enterprise 2.0. *MIT Sloan Management Review* **48**(3), 50–55.

Marwick A and Ellison N (2012) There isn't wifi in heaven! Negotiating visibility on Facebook memorial pages. *Journal of Broadcasting & Electronic Media* **56**(3), 378–400.

Matook S, Brown SA and Rolf J (2015) Forming an intention to act on recommendations given via online social networks. *European Journal of Information Systems* **24**(1), 76–92.

Mayer RC, Davis JH and Schoorman FD (1995) An integrative model of organizational trust. *Academy of Management Review* **20**(3), 709–734.

Mcallister DJ (1995) Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal* **38**(1), 24–59.

Mcknight DH, Choudhury H and Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research* **13**(3), 334–359.

Mello JA (2012) Social media, employee privacy and concerted activity: brave new world or big brother? *Labor Law Journal* **63**(3), 165–173.

Metzger MJ (2004) Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication* **9**(4).

Milberg SJ, Smith HJ and Burke SJ (2000) Information privacy: corporate management and national regulation. *Organization Science* **11**(1), 35–57.

Miltgen CL and Peyrat-Guillard D (2014) Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems* **23**(2), 103–125.

Moody GD, Galletta DF and Lowry PB (2014) When trust and distrust collide online: the engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research & Applications* **13**(4), 266–282.

Moreland RL (2010) Are dyads really groups? *Small Group Research* **41**(2), 251–267.

Morris JB (2016) First look: internet use in 2015. http://www.ntia.doc.gov/blog/2016/first-look-internet-use-2015. Accessed on September 7, 2016.

Morrison EW and Robinson SL (1997) When employees feel betrayed: a model of how psychological contract violation develops. *Academy of Management Review* **22**(2), 226–256.

Norberg PA, Horne DR and Horne DA (2007) The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* **41**(1), 100–126.

Oetzel MC and Spiekermann S (2014) A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems* **23**(2), 126–150.

Park S and Chung N (2011) Mediating roles of self-presentation desire in online game community commitment and trust behavior of massive multiplayer online role-playing games. *Computers in Human Behavior* **27**(6), 2372–2379.

Pate J and Malone C (2000) Enduring perceptions of violation. *Human Resource Management Journal* **8**(6), 28–31.

Pavlou PA (2003) Consumer acceptance of electronic commerce – integrating trust and risk, with the technology acceptance model. *International Journal of Electronic Commerce* **7**(3), 101–134.

Pavlou PA and Gefen D (2005) Psychological contract violation in online marketplaces: antecedents, consequences, and moderating role. *Information Systems Research* **16**(4), 372–434.

Pettersen L and Brandtzaeg PB (2012) *Privacy Challenges in Enterprise 2.0*. Association of Internet Researchers Salford, UK.

Petty R and Cacioppo J (1986) *Communication and Persuasion: Central and Peripheral Routes to Attitude Change.* Springer, New York.

Petty R and Wegener D (1998) Attitude change: multiple roles for persuasion variables. In *Handbook of Social Psychology* (Gilbert D, Fiske S, Lindzey G, Eds), pp 323–390, McGraw-Hill, New York.

Pew Research (2016) The state of privacy in America: what we learned. http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/. Accessed on August 30, 2016.

Posey C, Lowry PB and Roberts TL (2010) Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems* **19**(2), 181–195.

Rau P-LP, Gao Q and Ding Y (2008) Relationship between the level of intimacy and lurking in online social network services. *Computers in Human Behavior* **24**(6), 2757–2770.

Raynes-Goldie K (2010) Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook. *First Monday* **15**(1–4), article 32.

Ridings CM, Gefen D and Arinze B (2002) Some antecedents and effects of trust in virtual communities. *Journal of Strategic Information Systems* **11**(3–4), 271–295.

Ringle CM, Wende S and Becker JM (2015) SmartPLS 3. SmartPLS GmbH, Boenningstedt. http://www.smartpls.com.

Robinson SL (1996) Trust and breach of the psychological contract. *Administrative Science Quarterly* **41**(4), 574–599.

Rose E (2006) An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management* **43**(3), 322–335.

Rousseau DM (1989) Psychological and implied contracts in organizations. *Employee Responsibilities Rights Journal* **2**(1), 121–139.

Schoenbachler DD and Gordon GL (2002) Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing* **16**(3), 2–16.

Sheehan KB (1999) An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing* **13**(4), 24–38.

Sheng H, Nah FF and Siau K (2008) An experimental study on ubiquitous commerce adoption: impact of personalization and privacy concerns. *Journal of the Association for Information Systems* **9**(6), 344–377.

Smith HJ (1994) *Managing Privacy: Information Technology and Corporate America,* University of North Carolina Press, Chapel Hill, NC.

Smith HJ, Dinev T and Xu H (2011) Information privacy research: an interdisciplinary review. *MIS Quarterly* **35**(4), 989–1015.

Smith HJ, Milberg JS and Burke JS (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly* **20**(2), 167–196.

Son J-Y and Kim SS (2008) Internet users' information privacy-protective responses: a taxonomy and a nomological model. *MIS Quarterly* **32**(3), 503–529.

Straub DW (1989) Validating instruments in MIS research. *MIS Quarterly* **13**(2), 147–169.

Straub DW, Boudreau M-C and Gefen D (2004) Validation guidelines for is positivist research. *Communications of the Association for Information Systems* **13**(24), 380–427.

Sutanto J, Palme E, Tan C-H and Phang CW (2013) Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users *MIS Quarterly* **37**(4), 1141–1164.

Tang Z, Hu Y and Smith MD (2008) Gaining trust through online privacy protection: self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems* **24**(4), 153–173.

Tow WN-FH, Dell P and Venable J (2010) Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology* **25**(2), 126–136.

TRUSTe (2016) U.S. consumer privacy index 2016. https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/. Accessed on August 30, 2016.

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

Van Eerde W and Thierry H (1996) Vroom's expectancy models and work-related criteria: a meta-analysis. *Journal of Applied Psychology* **81**(5), 575–586.

Van Slyke C, Shim JT, Johnson R and Jiang JJ (2006) Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems* **7**(6), 415–444.

Venkatesh V and Davis FD (2000) A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science* **46**(2), 186–204.

Vitak J (2012) The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media* **56**(4), 451–470.

Vroom VH (1964) *Work and Motivation,* Wiley, New York.

Wakefield R (2013) The influence of user affect in online information disclosure. *Journal of Strategic Information Systems* **22**(2), 157–174.

Wall JD, Lowry PB and Barlow JB (2016) Organizational violations of externally governed privacy and security rules: explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems* **17**(1), 39–76.

Walther J, Van Der Heide B, Hamel L and Shulman H (2009) Self-generated versus other-generated statements and impressions in computer-mediated communication. *Communication Research* **36**(2), 229–253.

Warkentin M, Johnston AC and Shropshire J (2011) The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems* **20**(3), 267–284.

Weaver AC and Morrison BB (2008) Social networking. *Computer* **41**(2), 97–100.

Witte EH (2013) Small-group research and the crisis of social psychology: an introduction. In *Understanding Group Behavior: Small Group Processes and Interpersonal Relations* (Witte EH, Davis JH, Eds), pp 1–8, Psychology Press, New York.

Xu H (2007) The effects of self-construal and perceived control on privacy concerns. In *Proceedings of 28th Annual International Conference on Information Systems (ICIS), Montreal.*

Xu H, Dinev T, Smith HJ and Hart P (2011) Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* **12**(**12**), 798–824.

Xu H, Teo H-H, Tan BCY 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), 135–173.

Xu H, Teo HH and Tan BCY (2005) Predicting the adoption of location-based services: the roles of trust and privacy risk. In *Proceedings of 26th Annual International Conference on Information Systems (ICIS),* pp 897–910, Las Vegas, NV.

Xu H, Teo HH, Tan BCY 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), 1342–1363.

Yu J, Hu PJ-H and Tsang-Hsiang C (2015) Role of affect in self-disclosure on social network websites: a test of two competing models. *Journal of Management Information Systems* **32**(2), 239–277.

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), 53–89.

Appendix 1

Senior Scholars' Basket articles 2006–2016

We searched the eight journals in the Senior Scholars' Basket (AIS, 2016):

- *European Journal of Information Systems*
- *Information Systems Journal*
- *Information Systems Research*
- *Journal of AIS*
- *Journal of Information Technology*
- *Journal of MIS*
- *Journal of Strategic Information Systems*
- *MIS Quarterly*

We restricted our search to the years 2006–2016, which should include the "peer era" of privacy research, should it exist. We searched for articles that included the word "privacy" or the word "disclosure" in the title or subject terms list. We then examined each of those articles to ascertain whether it addressed questions associated with factors that may drive privacy concerns and/or outcomes that emanate from such concerns or if it considered some

Table 8 Articles 2006–2016

Journal	*# in domain*	*Articles in domain*
European Journal of Information Systems	9	Bansal *et al* (2015), Dinev *et al* (2006, 2013), Hu *et al* (2015), Junglas *et al* (2008), Li & Unger (2012), Miltgen & Peyrat-Guillard (2014), Oetzel & Spiekermann (2014), Posey *et al* (2010)
Information Systems Journal	3	Conger *et al* (2013), Kehr *et al* (2015), Keith *et al* (2015)
Information Systems Research	7	Anderson & Agarwal (2011), Choi *et al* (2015), Dinev and Hart (2006), Dinev *et al* (2015), Jiang *et al* (2013), Tsai *et al* (2011), Xu *et al* (2012)
Journal of AIS	3	Sheng *et al* (2008), Van Slyke *et al* (2006), Xu *et al* (2011)
Journal of Information Technology	2	Krasnova *et al* (2010), Tow *et al* (2010)
Journal of MIS	6	Chellappa and Shivendu (2007), Hann *et al* (2007), Lowry *et al* (2011), Tang *et al* (2008), Xu *et al* (2009), Yu *et al* (2015)
Journal of Strategic Information Systems	3	Dinev *et al* (2008), Gerlach *et al* (2015), Wakefield (2013)
MIS Quarterly	9	Angst & Agarwal (2009), Awad & Krishnan (2006), Bélanger & Crossler (2011), Hong & Thong (2013), Hui *et al* (2007), Lee *et al* (2011), Smith *et al* (2011), Son & Kim (2008), Sutanto *et al* (2013)

form of privacy-related calculus, either explicit or implicit. Forty-two of the articles proved to be within that domain of interest; these articles are noted in Table 8.[4]

We then considered the foci of each article in this pool: Did the article focus on individuals' relationships to institutions and/or peers? The latter could have been reflected in either a consideration of subjects' concerns about peers having access to data associated with the subject or to communication with peers (either through an institutional system or via some other channel). Notably, only two of the articles in the pool considered such peer-associated relationships. Those two articles are highlighted in the text.

Appendix 2

Survey items

Privacy experience (scale strongly disagree → strongly agree)

PE1: I have frequently been the victim of an improper invasion of my information privacy by someone I know.

PE2: Only rarely is my information privacy invaded by someone I know.

PE3: I often feel that my information privacy has been being violated by someone I know.

PE4: My information privacy is invaded all the time by other people I know.

PE5: People I know often misuse my private information.

Privacy awareness (scale strongly disagree → strongly agree)

PA1: Almost every day, I hear something about the invasion of someone's information privacy by people they know.

PA2: I frequently hear about the invasion of someone's information privacy by people they know.

PA3: There is often news about how someone misuses information regarding a person she or he knows.

PA4: People often share information they should not about someone they know.

Privacy concerns (scale strongly disagree → strongly agree)

PC1: I am concerned that the information I share through the Internet with people I know could be misused by them.

PC2: I am concerned about sharing information through the Internet with people I know, because of what they might do with it.

PC3: I am concerned about sharing information through the Internet with people I know, because they could use it in a way I did not foresee.

PC4: I am concerned that when I share information through the Internet with people that I know, those people may share it with others whom I did not intend.

PC5: I am concerned that the information I share through the Internet with people I know could be misinterpreted by them.

Risk (scale not at all likely → very likely)

How likely is it that the information you provide to Facebook…

R1: Will be used by one of your Facebook friends to spy on you.

R2: Will be used against you by one of your Facebook friends.

R3: Will be used by a Facebook friend to embarrass you.

R4: Will be shared by one of your Facebook friends with someone you don't want (e.g., "ex," parents, teachers).

Trust (scale strongly disagree → strongly agree)

[4] Three articles addressing corporate privacy policies and/or compliance therewith were also identified in this search: Greenaway *et al* (2015), Wall *et al* (2016) and Warkentin *et al* (2011). These are not included in the table.

Generally, I trust that Facebook users to whom I have given access to information about me .
T1: Will not misuse my sincerity on Facebook.
T2: Will not embarrass me by using some information they learned about me through Facebook.
T3: Will not use the information they found about me in Facebook against me.
T4: Will not use the information about me in a wrong way.
T5: Are trustworthy.

Benefits (scale strongly disagree → strongly agree)

Bn1: Facebook helps me inform all my friends about my ongoing activities.
Bn2: Through Facebook I get connected to new people who share my interests.
Bn3: Facebook allows me to save time when I want to share something new with my friends.
Bn4: Facebook helps me to reconnect with my old friends.
Bn5: I find Facebook efficient in sharing information with my friends.
Bn6: Facebook helps me expand my network.

Information disclosure (scale not at all → to a great extent)

To what extent do you do each of the following on Facebook?
ID1: Keep your Facebook friends updated about what is going on in your life.
ID2: Share things you have to say with your Facebook friends.
ID3: Provide extra contact information to help others find you or add you as a friend.
ID4: Keep your information up to date for your Facebook friends.
ID5: Keep a detailed timeline for your Facebook friends to see.
ID6: Tell your Facebook friends a lot about yourself.
ID7: Enable your Facebook friends to find out your preferences in music, movies, books, etc.
ID8: Allow your Facebook friends to understand who you are.

Appendix 3

Table 9 Factor matrix

	PA	*PE*	*PC*	*R*	*T*	*Bn*	*ID*
Privacy awareness							
PA1	**.78**	.41	.37	.26	−.10	.03	.04
PA2	**.78**	.24	.37	.24	−.03	−.01	−.09
PA3	**.86**	.39	.42	.28	−.08	.01	−.01
PA4	**.83**	.28	.34	.28	−.08	.00	−.11
PA5	**.77**	.20	.36	.25	−.05	.03	−.15
Privacy experience							
PE1	.30	**.83**	.30	.29	−.19	.03	.02
PE2	.35	**.92**	.32	.30	−.23	−.08	−.01
PE3	.29	**.88**	.27	.27	−.24	−.09	−.01
PE4	.39	**.86**	.31	.23	−.21	−.08	−.01
Privacy concerns							
PC1	.38	.33	**.87**	.35	−.24	.01	−.09
PC2	.43	.36	**.92**	.39	−.25	.01	−.15
PC3	.44	.30	**.94**	.34	−.24	−.02	−.19
PC4	.43	.29	**.90**	.33	−.23	.04	−.15
PC5	.40	.27	**.88**	.34	−.24	−.03	−.18
Risk							
R1	.28	.24	.31	**.81**	−.24	−.02	−.16
R2	.30	.29	.34	**.94**	−.42	−.06	−.18
R3	.28	.30	.37	**.93**	−.43	−.03	−.16
R4	.31	.27	.35	**.88**	−.42	−.08	−.22
Trust							
T1	−.04	−.19	−.23	−.35	**.87**	.33	.41
T2	−.08	−.25	−.23	−.38	**.93**	.27	.35
T3	−.08	−.23	−.24	−.43	**.94**	.23	.30
T4	−.10	−.22	−.26	−.41	**.94**	.24	.34
T5	−.09	−.24	−.26	−.43	**.89**	.23	.35

	PA	*PE*	*PC*	*R*	*T*	*Bn*	*ID*
Benefits							
Bn1	−.01	−.10	−.01	−.07	.26	**.80**	.43
Bn2	−.04	−.11	−.03	−.06	.27	**.83**	.44
Bn3	−.02	−.05	.01	−.07	.29	**.84**	.47
Bn4	.08	.07	.00	−.01	.07	**.70**	.33
Bn5	−.02	−.06	.00	.00	.22	**.80**	.43
Bn6	.10	−.02	.04	−.04	.20	**.76**	.46
Information disclosure							
ID1	−.10	.08	−.18	−.19	.29	.40	**.84**
ID2	−.04	.09	−.15	−.12	.30	.34	**.82**
ID3	.02	−.03	−.06	−.12	.23	.42	**.73**
ID4	−.05	.01	−.11	−.15	.34	.47	**.80**
ID5	−.14	−.04	−.16	−.16	.28	.44	**.75**
ID6	−.01	−.03	−.08	−.13	.31	.55	**.77**
ID7	−.01	.06	−.13	−.14	.23	.31	**.69**
ID8	−.12	−.10	−.18	−.23	.39	.40	**.83**