Inf Technol Manag (2016) 17:341–360
DOI 10.1007/s10799-015-0246-0

The interpersonal privacy identity (IPI): development of a privacy as control model

Tabitha L. James[1] · Quinton Nottingham[1] · Stephane E. Collignon[1] · Merrill Warkentin[2] · Jennifer L. Ziegelmayer[3]

Published online: 23 July 2015

Abstract The Internet and social computing technology have revolutionized our ability to gather information as well as enabled new modes of communication and forms of self-expression. As the popularity of social computing technologies has increased, our society has begun to witness modifications in socialization behaviors. Social psychology theory suggests that technological changes can influence an individual's expectation of privacy, through adaptive behaviors resulting from use (Laufer and Wolfe in J Soc Issues 33(3): 22–42 (1977)). We adapt traditional privacy theory to explore the influence of developmental and environmental factors on the individual's inner privacy identity, which is comprised of the individual's belief in his or her right to control (1) personal information and (2) interactions with others, and is continuously shaped by privacy experiences. We then use the inner privacy identity to examine interpersonal behaviors in the online context. We find that individuals' belief in their right to control their information impacts their information disclosure practices when consequences are implied and that their belief in their right to control the interaction impacts their online information sharing practices. We do not find support for a relationship between the interaction management component of the IPI and online interaction behavior, which considered in the presence of the relationship between interaction management and online information sharing, suggests that interaction behavior is more complicated in the online context. Insights from the model developed in this study can inform future studies of situational privacy behaviors.

Keywords Privacy · Online behavior · Information control · Interaction control

✉ Tabitha L. James
tajames@vt.edu

Quinton Nottingham
notti@vt.edu

Stephane E. Collignon
stephane@vt.edu

Merrill Warkentin
m.warkentin@msstate.edu

Jennifer L. Ziegelmayer
jziegelmayer@qu.edu.qa

[1] Department of Business Information Technology, Pamplin College of Business, Virginia Tech, 1007 Pamplin Hall, Blacksburg, VA 24061, USA

[2] Management and Information Systems Department, College of Business, Mississippi State University, P.O. Box 9581, Mississippi State, MS 39762-9581, USA

[3] Department of Accounting and Information Systems, College of Business and Economics, Qatar University, P.O. Box 2713, Doha, Qatar

1 Introduction

A multi-disciplinary stream of literature shows the existence of a personal need for privacy [3, 8, 35, 58, 65], and research in information systems in particular has often focused on an individual's concern for privacy [59, 61]. However, as Aristotle said, human beings are "social animals." People need to participate in society, which typically entails the disclosure of some personal information [43, 65]. An individual's desire for privacy and his or her socially induced disclosure can be viewed as conflicting goals. This dilemma has led researchers toward the study of privacy regulation mechanisms based on the idea that privacy is a commodity [4, 10, 31, 49], a legal or human right,

a state of limited access or limited access to information [35, 65] or that control over what information is released to whom is crucial to maintaining a preferred level of privacy [21, 35, 39, 65]. This definitional categorization for privacy is given in Smith et al. [58]. It is the latter category with which we are concerned in this study.

When exploring the dynamics of *privacy as control*, it is important to consider the interplay between information and interaction management [35]. In order to benefit from societal participation, one may yield marginal control of personal information by disclosing some personal information and/or by extending our network of connections, thereby allowing personal information to be shared more broadly. Conversely, to maintain a more private posture, a person may limit his or her societal participation by restricting either the amount of information he or she discloses or the number of people or networks to which he or she discloses. The modern ubiquitous online environment, in which networks of information and communication technologies largely mediate individual identities, exacerbates the tension created by this dichotomous control environment.

Information Systems (IS) researchers have explored privacy's influence on online behaviors or behavioral intentions in different situational contexts. These studies have led to advances in our understanding of privacy management, especially with regards to e-commerce [9, 14, 16, 21, 22, 38, 41, 50, 60, 63]. While online consumerism was the first widespread commercial use of the Internet, social computing has become ubiquitous over the last decade. One form of social computing, online social networks (OSNs) such as Facebook, has been described as both more expansive and freer than its counterpart (offline social networks) [27]. As researchers explore the intricacies of participating in online society, they are experiencing somewhat paradoxical findings. Several studies have reported that people express a desire for privacy but actually reveal more than their stated preference [7, 11, 45]. It has also been shown that most users on Facebook seem to disregard the use of privacy controls in spite of a certain degree of privacy concern [1, 2]. These studies hint at a technological effect on privacy as some socialization has moved from an offline to an online environment.

The privacy as control approach differs from the more commonly studied concern for information privacy model [61]. We suggest that this view complements current IS research by providing an approach well suited to the dynamic and interactive nature of social computing. Whereas many privacy studies have rightly focused on e-commerce applications that by their nature involve relatively structured and defined interactions, social computing transfers the dynamic nature of interpersonal social relationships online. Laufer and Wolfe [35] suggest that although *information management* is an often-discussed element of privacy, *interaction management* is equally important, yet often overlooked. We argue that both of these elements are increasingly crucial to examining privacy behaviors in the social computing era. Similar to Laufer and Wolfe's [35, p. 33] conceptualization, we suggest that these two elements form an interpersonal dimension that "constitutes the core of the privacy phenomenon as it is experienced in daily life." Borrowing from this theory, we develop two constructs for information and interaction management and refer to these two constructs as forming the interpersonal privacy identity (IPI) of an individual. In other words, we suggest that the control an individual feels entitled to have over his or her information and interaction expresses his or her privacy concept. Our primary contribution is to operationalize the IPI constructs and explore their influence on contextual privacy behaviors. That is, we do not explore a specific situation (i.e. a particular website). Rather, we emphasize context (online) and examine the influence of the IPI on general online behaviors. Explorations of specific situations (e.g. OSNs, virtual communities, etc.) could follow, but are outside of the current scope of this study.

Laufer and Wolfe's [35] article is a conceptual piece in social psychology that theorizes about the interaction between three dimensions: interpersonal (which includes information and interaction management), self-ego, and environment. The discussion provided in Laufer and Wolfe [35] regarding the interplay between these three dimensions is high-level and complex. Thus, any model derived from their exposition will likely over-simplify the discussion. However, a model has been suggested and components of Laufer and Wolfe's theory have been utilized in the IS literature (most notably the concept of Calculus of Behavior). Lwin and Williams [37] offered a proposed model of the theory in the marketing literature on privacy, but it was not fully developed or tested. Dinev and Hart [21, 22] and Dinev et al. [23] introduced the idea of the calculus of behavior to IS research. These approaches provided us with a starting point. Our focus was on the development of the interpersonal elements, but similar to Lwin and Williams, we included the environment and self-ego dimensions in our proposed model. However, we excluded the calculus of behavior for the current study since it has already been well studied and is very situationally dependent in its operationalization [14, 22, 30, 66] in order to focus on the lesser-studied elements of the theory and generalize the context.

The remainder of the paper will be organized as follows: Sect. 2 will present the theoretical background, the proposed model, relevant literature, and the propositions. Section 3 will discuss the methods employed and the results. In Sect. 4, we will discuss our findings, their

implications and the limitations of the study. The paper will be concluded in Sect. 5.

2 Theoretical background and research model

2.1 Interpersonal privacy identity (IPI)

Researchers have used varying definitions and conceptualizations of privacy through the years. Privacy conceptualizations have been categorized by Smith et al. [58] to include privacy as (1) a commodity [4, 10, 31, 49], (2) a legal or human right, (3) a state of limited access [35, 65], or (4) privacy as control [21, 35, 39, 65]. The debate is still ongoing and the purpose of this study is not to debate the accuracy of the conceptualizations. We recommend Smith et al. [58] and Bélanger and Crossler [8] for concise overviews of the state of present knowledge concerning privacy research in IS. We position our paper primarily in the stream of research that examines information privacy through the perceived entitlement to control/manage what information is divulged and to whom (i.e. that the individual's belief in his or her right to control/manage information and interaction shapes the individual's privacy behaviors). This positioning falls within the conceptualization of privacy as control described in Smith et al. [58] and described in various forms by several scholars. For example, Margulis [39, p. 10] define privacy as representing "the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability".

The importance of being able to manage information and interaction is deeply rooted inside a person and influenced by the history of that individual from childhood [35, 65]. Therefore, the perception of what needs to be private varies from one individual to another and can vary over time for each individual. Laufer and Wolfe [35] expound on two dimensions, self-ego and environment, that interact with a third, the interpersonal dimension. They further suggest that the acting out of interpersonal relationships in everyday life revolves around two elements: interaction and information management [35]. In the current study, we operationalize these two elements and model them as forming an individual's set of privacy beliefs (i.e. the right to control what information is released and to whom), which we call the IPI, illustrated in the conceptual model of Fig. 1. We suggest that by gauging the perceived entitlement of an individual to manage his or her information and interaction, we can measure the significance of privacy to that individual at that point in time. Over an individual's lifetime, the IPI may evolve in response to experienced privacy situations. We propose that at any given point in time, the individual's IPI can be measured at the current state of evolution by examining his or her perceived right to manage his or her information and interaction management. Furthermore, we suggest that any time the individual is presented with a privacy situation or context, the IPI in its current form will influence his or her privacy related (information and interaction management) behaviors.

Recent research has modeled the ability to control information as being an antecedent to perceived privacy in a specific situation [24]. This work applied concepts from Laufer and Wolfe [35] in a Web 2.0 setting. Their model emphasized an idea from Laufer and Wolfe [35, p. 39] that suggests: "the dimensions of the privacy phenomenon are conceptually distinct from control/choice, which is a mediating variable." Thus, Dinev et al. [24] defined information control in their context as "an individual's beliefs in one's ability to determine to what extent information about the self will be released onto the Web 2.0-related sites (p. 299)" and examined the influence of information control on perceived privacy. Our approach is similar in that we explore a conceptualization of privacy belief that includes the perceived entitlement to control information and interaction. We then identify a set of constructs that represent online privacy behaviors (as control choices over information and interaction) to ultimately examine the relationship between the privacy belief and the actual online practice. In addition, rather than looking at technical antecedents that influence the ultimate realization of the belief towards control over information and interaction, we examine developmental and environmental antecedents suggested in the conceptual Laufer and Wolfe [35] piece. An understanding of developmental and environmental antecedents' influence on the formation of the belief in the right to control information and interaction and the impact of this perception on actual behaviors can inform entities trying to disseminate safer privacy practices as to how best propagandize or advocate. Such practices have been suggested, along with technological changes, to be successful in adapting privacy concerns and behaviors [6, 35].

Laufer and Wolfe [35], as well as Westin [65], suggest that people manage their privacy at a situational level on a reward and cost basis. As Westin puts it: "The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself [or herself] to others […]" [65, p. 7]. This quote suggests that information privacy is managed by two conflicting privacy considerations: (1) the individual's perceived desire for privacy at the time the privacy experience is evaluated and (2) any factors that might override the individual's desire for privacy. This trade-off between desire for privacy and rewards

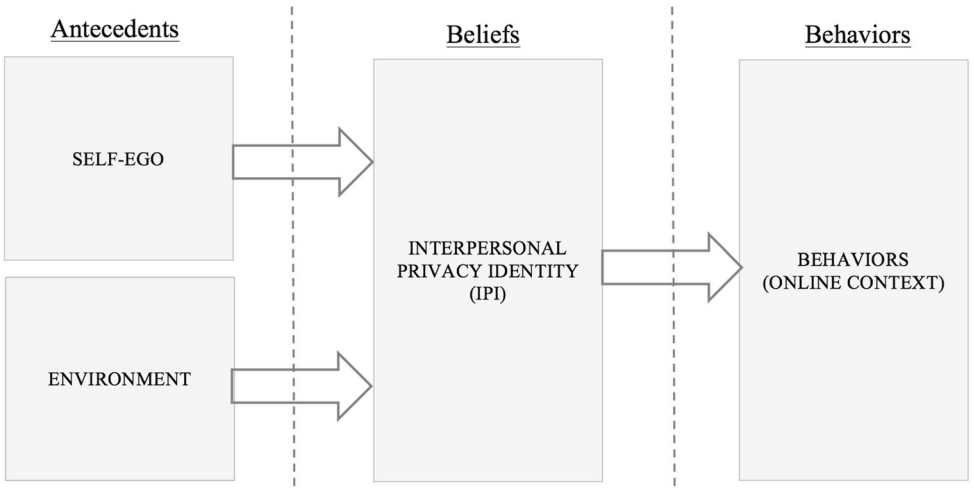

Fig. 1 Conceptual privacy model

is the concept of the Calculus of Behavior that is solely situational. Sometimes referred to as the privacy calculus, this concept is often modeled as the idea that there are certain desires that could cause an individual to override his or her privacy concept in a particular situation. For example, a store is offering a 10 % discount on an item in return for the person's email address. The discount may be so desirable that it overwhelms the individual's need for information control and results in the individual relinquishing his or her email address. The calculus variables, as typically modeled in IS [14, 22, 30, 66], focus on rewards specific to a particular situation (e.g. being able to receive the discount) that are not as easily defined in our general context. Future work could entail applying our model to a specific situation, in which case the current research model could be augmented with the IS privacy calculus constructs. The focus of our study is to examine the development of a model to explore an individual's IPI, thus, we examine only contextual variables (online behaviors) to test our proposed model rather than delve into a particular situation. However, Laufer and Wolfe [35] discuss the calculus of behavior phenomenon as part of a larger discussion on the ability or inability of an individual to foresee the consequences of his or her information disclosure. Thus, our model incorporates foreseeable consequence into our constructs but does not model the situational calculus constructs in the manner of previous IS research.

The interpersonal dimension consists of managing information and interaction. Privacy work in IS often focuses on the disclosure of information, but technological changes are creating the ability for people to manage their interaction with others online in more granular ways. Interaction management relates to the consideration of the others to which information is released. Each time an individual tells someone his or her piece of private information, the circle of people privy to that information increases. Maintaining this circle of people tightly so that private information stays in the circle is likely to become more difficult as the size of the circle grows. The concept of a circle (or circles) of people who are granted access to some of a person's private information is often referred to as designating privacy boundaries. We refer the reader to Altman and Taylor's Social Penetration Theory [4] and Derlega and Chaikin [19] for greater detail on the research relating to privacy boundaries.

In what follows, we first introduce the online behaviors examined in the current study and present the proposed relationships between the IPI constructs and the online behaviors. The antecedents to the IPI, based upon the self-ego and environment dimensions of Laufer and Wolfe's [35] theory, are then introduced. The relationships proposed between the antecedents and the IPI are discussed, and finally, the operationalized model is presented.

2.2 Information control belief and online behaviors

Information management relates to the self-disclosure or non-disclosure of personal information. Posey et al. [53], citing other researchers, define self-disclosure as "what individuals voluntarily and intentionally reveal about themselves to others—including thoughts, feelings and experiences [20, 47]." We propose that an individual forms a belief concerning his or her right to control the release of personal information. This belief informs the person's decision concerning whether to release a particular piece of information to another entity in any situation requiring such a decision. We refer to this component of the IPI as Information Control Belief and define it as snapshot of a person's belief in his or her right to control his or her information. For example, imagine that an individual is looking at his or her newsfeed on Facebook and sees an

article posted by a friend about a political candidate whose positions are not aligned with the individual. The decision the individual makes in regard to commenting on that article (i.e. whether the individual comments on the article and what information is contained in that comment) is informed by the significance he or she places on controlling his or her information.

It is difficult to define personal information, since what is considered personal may differ amongst people. For example, some people may feel that their marital status is personal information while others may reason that since marital status is part of the public record, it is public information. Exploring the release of specific pieces of information is outside the scope of the current study. However, Laufer and Wolfe [35] argue that the fundamental problem in evaluating whether to release information is that it is often difficult for individuals to know or to predict the consequences of releasing personal information. Therefore, to explore the breadth of Information Control Belief, we incorporated into the construct personal information in general and personal information with an associated consequence. The scale used to measure Information Control Belief is a modified version of an instrument developed in Pirim et al. [51] to measure an individual's perceived need for privacy.

When examining information control behaviors in an online context, we suggest that there is the consideration of the type of information that is being released, but that the online environment also allows for that information to take on different forms. For example, a person could update his or her Facebook status about an event he or she is attending, send a tweet about how well he or she is enjoying the event, and/or relate the story of the event on a lengthy blog entry. It could be argued that each one of these options exposes, in some manner, the individual's personal information to varying degrees. Therefore, our first information control behavior, which we will refer to as Information Sharing Behaviors in the Online Context, examines the extent of the release of personal information of an individual without regard to the application used to release. The construct represents the purely public (i.e. viewable to anyone) release of general information (information sharing) in the online context. The construct does not consider the reason for its release and more importantly does not infer consequences of these disclosures. We expect that individuals who feel strongly entitled to control their information would be reluctant to participate in online information sharing. *Au contraire*, people with a more relaxed perspective towards information control may engage in some amount of online information sharing.

Self-disclosure is not without consequence and the consequence is often hard to predict. Georg Simmel [57] coined the phrase "self-invasion" when people failed to protect their own privacy by divulging private information. To further complicate matters, people may choose to ignore future privacy risks for immediate rewards [1, 22]. This may help to explain why some individuals participate heavily in risky Internet practices and others do not. However, when the consequences are defined, we would expect individuals to try to avoid these consequences. Although we suggest that people who strongly believe they are entitled to control their information would be less likely to share information, they should be even less likely to do so when it is expected to have adverse consequences. Therefore, our Online Disclosure with Consequences construct captures the release of information with potential consequences attached to its release. Measuring disclosure of information with consequences is a way to distinguish types of private information. As we previously mentioned, we cannot infer what is or is not private as it varies with the individual and the situation. Therefore, we used type, similar to methods employed in other research in which the release of sensitive information was used, as a proxy for private information [44]. We do not differentiate between whether or not the perceived consequences have occurred; we only attach possible consequences to the release of information. In this manner, we can examine multiple levels of disclosure (i.e. general disclosure where possible consequences have to be inferred and disclosure where the consequences are provided).

Yet another way to manage information is to attempt to control the audience to which the information is released. In earlier versions of OSNs, the ability to control the scope of information release for online interactions was not terribly granular. Current OSN technologies are increasingly adding more fine-grained controls to manage privacy circles. For example, both Google+ and Facebook now allow the user to release information to a pre-specified audience. Under newer OSN controls, the user can decide to release a piece of information to a select few others. This, at least initially, limits the scope of the information release. These are relatively new controls and constitute a way to manage online privacy that has not been widely prevalent. Consequently, it may be too early for this impact to manifest but we will include it in the hypotheses since it is quickly becoming a feasible online privacy mechanism. We suggest that those individuals who strongly believe they are entitled to control their information will engage in highly inclusive interaction behaviors to a lesser extent than those that do not. This logic leads to the following set of hypotheses:

H1a An individual's belief in his or her right to control the disclosure of his or her information will be negatively related to online information sharing.

H1b An individual's belief in his or her right to control the disclosure of his or her information will be negatively related to online disclosure with consequences.

H1c An individual's belief in his or her right to control the disclosure of his or her information will be negatively related to online interaction behaviors.

2.3 Interaction control belief and online behaviors

Laufer and Wolfe [35] state that "privacy as interaction management is actually a form of noninteraction with specified others." Interaction management refers to the amount of control an individual exercises over determining the size and scope of his or her circle(s) of confidants and the maintenance of those circle(s). The person's belief in his or her right to control his or her interactions with others, at least partially, informs how he or she will manage his or her interactions under a given context or in a particular situation (i.e. his or her management behaviors). For example, consider an individual who communicates with family and friends over Facebook. In a situation where a person the individual does not know sends a friend request, the decision to include that unknown person in his or her circle of friends is informed by the significance that individual places on managing his or her interaction. As a more complex example, imagine an individual considering posting a status update on Facebook containing a humorous story about his or her child. New OSN controls allow that individual to decide both whether to release that information (the story) and to what subset of individuals from the general Facebook audience. In the current study, we are measuring people's belief in their right to control their interaction, captured at the time they participated in the study. We refer to this part of the IPI as Interaction Control Belief and use this construct to capture an individual's belief in his or her right to manage his or her interactions. An individual's Interaction Control Belief is a facet of his or her overall privacy concept (or IPI) and, therefore, influences his or her behavior in a given situation but it is not itself situational. Rather it is simply a perception regarding his or her right to control (or manage) his or her interactions with others regardless of how those interactions are conducted. The scale used to measure Interaction Control Belief was rigorously developed for the current study, because no existing scale could be located to measure this construct.

When exploring online interaction management behaviors, one would expect that an individual who strongly believes he or she is entitled to control his or her interactions with others would be less likely to engage in what could be perceived as riskier online interactions. By online interactions, we mean Internet-mediated interactions with others. Since we are exploring general interaction behaviors in a particular context (online), rather than specific behaviors in a defined situation (e.g. interacting with a certain person on Twitter), we developed a construct that would explore the extent an individual interacts with different types of Internet users. These types of users are differentiated by the exposure that individual has to them outside of the online environment. We suggest that prior face-to-face contact with an individual increases the comfort of interacting with that person on the Internet because it does not extend a person's circle therefore, making that communication less risky. The inclusion of additional people within an individual's private circles necessitates this individual's trust that these people will be able to keep private information within the circle or that the privacy boundaries are closed [4, 15, 19, 49]. As explained by Westin [65], technology blurs our sense of privacy because it destroys the "practical boundaries of privacy." Communication through a media (e.g. online environment), whether it is in the work environment [17] or in the management of social relationships [33], has been shown to lack some social cues available in face-to-face communication. This may change how an individual perceives the richness of online relationships, especially if the media does not perfectly fit the purpose [18]. This may restrict an individual from forming close personal relationships online or at least from perceiving them as close. It could be suggested that these factors complicate that management of interaction in an online context. Moor [42] and Tavani [62] explain that limited control over information online pushes people to control their interactions with others in order to make sure that the right people access the right information. Our Interaction Behaviors in the Online Context construct examines behaviors that would extend or expose a person's privacy boundaries through online communication, which is arguably more complex to navigate due to the lack of physical exposure and depersonalization of the communication medium. Therefore, we suggest that someone who strongly believes he or she is entitled to control his or her interaction would be less likely to conduct such interaction behaviors in the online context.

As previously mentioned, OSN technologies are beginning to provide finer-grained disclosure controls that allow the user to decide what information to release and what the audience for that particular piece of information will be. Individuals wishing to manage their privacy in the evolving online environment can now choose several strategies. At one extreme, an individual could choose to release a piece of personal or sensitive information to a very small subset of others via the Internet. For example, a person could private message another person on Facebook a piece of gossip about a third party. At the other extreme, an individual could choose to release a piece of less personal or

sensitive information to everyone on the Internet. For example, a person could write a public blog entry that was a critique of an interesting movie they watched. Following this logic, we suggest that individuals that have a strong belief in their right to control their interactions with other people may carefully select which information they release to which others. Thus, it is possible that those individuals with who strongly believe they are entitled to control their interactions will be less likely to share information online. Again, the use of such fine-grained privacy controls may not yet be widespread enough to influence the results, but for completeness we suggest that as an individual's belief in his or her right to control his or her interactions increases, the information sharing and their online disclosure with consequences will decrease. This leads to the following hypothesis:

H2a An individual's belief in his or her right to control his or her interactions with others will be negatively related to online interaction behaviors.

H2b An individual's belief in his or her right to control his or her interactions with others will be negatively related to online information sharing.

H2c An individual's belief in his or her right to control his or her interactions with others will be negatively related to online disclosure with consequences.

3 Antecedents

The influence of an individual's self-concept and various environmental factors are discussed in depth in Laufer and Wolfe's conceptual work. Laufer and Wolfe [35] suggest that the privacy concept is expressed through information and interaction management practices for each privacy situation presented to an individual. That privacy concept is refined through these experiences, as well as through interaction with the self-ego and environment dimensions. Our interpretation models the privacy concept as belief in the right to control information and interaction, which in turn influences privacy (interaction and information management) behaviors. Lwin and Williams [37] proposed a model that incorporated environmental and self-ego factors as antecedents to a belief that people should be concerned about their privacy. We suggest that the multi-faceted approach of examining both information and interaction control beliefs as the privacy concept provides benefits for the exploration of privacy in the social computing era where applications offer management options that mimic these choices (for example: an increasingly diverse set of social computing technologies with various information disclosure prompts and OSN group options to manage levels of interaction such as Google+ circles or Facebook groups). Another contribution of the current research is in exploring the development of constructs for the antecedents; regardless of what privacy concept is used as a mediating variable. In much IS research, the antecedents to privacy control are technical in nature (e.g., computer anxiety) [32, 38, 59, 61]. Laufer and Wolfe's [35] theory allows us to explore social psychological factors influencing information privacy. Therefore, we follow Lwin and Williams' [37] use of the other two dimensions as antecedents to a privacy belief, but model the concept differently. Both models, ours and Lwin and Williams [37], are simplifications of the complexity related in Laufer and Wolfe's [35] robust conceptualization, but they advance the state of research in privacy as control by providing initial operational models of this seminal theory.

3.1 Self-ego

Laufer and Wolfe [35] argue that the developmental process, particularly in Western society, emphasizes the idea of autonomy. They explain that the development of the Self comes through the ability to separate oneself from the environment, which requires that one ultimately be capable of functioning alone. The ability to function independently eventually presents the choice of being alone voluntarily. The response to this choice is what determines one's autonomy. Autonomy implies the ideas of independence and control, even separation. Autonomy is how the Self influences privacy. Laufer and Wolfe refer to this dimension of privacy as self-ego.

In the current study, we define autonomy as an individual's need for independence. The personal style inventory (PSI) was developed to measure sociotropy and autonomy for use in the study of depression [55]. Robins et al. constructed an instrument that was composed of three factors for autonomy: perfectionism/self-criticism, need for control, and defensive separation. The need for control subscale for autonomy best matched Laufer and Wolfe's view of autonomy. This scale of the PSI study contains items related to the importance an individual places on his or her independence and the control over his or her activities. In the current study, we adopt the PSI items originally labeled "Need for Control". These items, along with the rest of our instrument, are listed in the results section below.

The concept of autonomy suggests the premise of functioning alone by choice. In other words, the aloneness or ability to accomplish things on one's own is viewed typically as a positive situation. Laufer and Wolfe suggest that privacy is often connected to independence as well as the idea of being able to do whatever one wanted to do. It can be argued that an individual with a high need for independence requires a higher level of privacy than an

individual who is less autonomous. In Malhotra et al. [38] and in Dinev and Hart [21] the notion of desire for control over privacy includes the notion of desire for autonomy, maybe implying that those two evolve in parallel. It is our expectation that one's level of autonomy will positively impact their concept of privacy. Stated another way, we expect to find that as autonomy increases, an individual's expectations with regard to controlling his or her interactions and information will increase. This leads us to the following two hypotheses:

H3a An individual's autonomy will be positively related to the individual's belief in his or her right to control the disclosure of his or her information.

H3b An individual's autonomy will be positively related to the individual's belief in his or her right to control his or her interactions with others.

3.2 Environment

Environment refers to all the external influences in one's surroundings. Laufer and Wolfe [35] divide these external influences into three-subcategories: cultural, socio-physical, and lifecycle. Cultural influences are those related to the traditions, customs, beliefs, and norms of a particular clustered group of people. The reality of the actual physical surroundings imposed on an individual defines the socio-physical element. The lifecycle element describes the makeup of one's environment depending on their stage of life, which can be described by the responsibilities of an individual at a particular time period. While all three can be considered environmental influences, they are distinct elements that independently influence an individual. All three can be argued to impact one's concept of privacy. Previous research has indicated that environment impacts privacy behaviors in particular situations. In Warkentin et al. [64] environment (called external cues) influences the capability to manage privacy and therefore behaviors. In the following subsections, we will examine each element of environment.

3.3 Cultural

A culture is a set of norms, traditions or customs of a particular group of people. This set of norms often derives from constraints on activities imposed by the landscape, religion, government, etc. but eventually come to describe a people. As such, cultural norms reflect "the perceived degree to which certain behaviors or practices are common in a given culture" [12].

Laufer and Wolfe [35] suggest that different cultures have different expressions of privacy and that the norms of a culture influence an individual's perception of his or her rights to privacy. Bélanger and Crossler [8] and Smith et al. [58] confirm through their study of the literature that privacy is impacted by societal norms (culture) and suggest that further research in this area would be beneficial. Notably, Laufer and Wolfe [35] describe technology's influence on a culture. Similar to the argument presented by Rule [56], they suggest that technology has a strong impact on how individuals in a society perceive privacy. This connection is often realized by privacy experiences, involving technology, that change the environment people (sometimes a generation) develop within. The influence of past privacy experiences involving technology are part of the environment that shapes the current status of the IPI. It could be argued that the current shift to a lifestyle that is led at least partially online for our younger generation is not only influencing the development of their privacy identity but also changing the culture in which they are developing. Although outside the scope of the current study, it could be suggested that the continuous pressure to share via social computing is encouraging a more open culture than existed previously, at least among younger generations.

Cultures are often described on a continuum from collectivistic to individualistic. Collectivistic cultures are viewed as having a common focus in which the people work together for the good of the group rather than the good of the individual. Collectivistic cultures tend to place more weight on advice from respected members of the community, often demonstrate less competitiveness, and emphasize sharing for the collective good. These characteristics are not the focus in an individualistic society in which thinking for oneself and individual success are often encouraged. Existing studies of privacy expectancy and information disclosure approach the idea of culture through the individualism/collectivism prism [36, 53]. In a workplace environment, Luo et al. [36] hypothesized a positive relationship between individualism and privacy expectancy and a negative relationship between collectivism and privacy expectancy. In Posey et al. [53], perceived collectivism increased the disclosure of information whereas individualism was found to be non-significant. Therefore, we suggest that in a collectivistic culture in which more emphasis is placed on sharing information, common decision-making, and togetherness, one will have lowered expectation of being able to manage one's interaction and information. Conversely, we would expect that the more individualistic (less collectivistic) a culture is, the more the expectation to control their interaction and information will increase. This leads us to the following hypotheses:

H4a A collectivistic culture will be negatively related to an individual's belief in his or her right to control the disclosure of his or her information.

H4b A collectivistic culture will be negatively related to an individual's belief in his or her right to control his or her interactions with others.

In the present study, we develop a shortened version of Bierbrauer, Meyer, and Wolfradt's [12] cultural orientation scale (COS) to measure the degree to which an individual's culture is collectivistic. This scale is very focused on the role of family on individuals' behaviors, which may be viewed as restrictive but is consistent with Laufer and Wolfe's emphasis on the role of childhood experiences in the shaping of an individual's privacy concept.

3.4 Socio-physical

Another major environmental influence is the makeup of an individual's physical surroundings and the level of privacy associated with those surroundings. The concept of being physically separated from others has been examined in IS privacy research. Rensel et al. [54] found that physical environment impacted the use of commercial websites in public facilities and was moderated by a need for privacy. This lends credence to the idea that physical seclusion has a connection to privacy. Furthermore, the ability to obtain physical separation from others is the traditional view of privacy. We will use the socio-physical element of the model to examine the degree of physical seclusion available to an individual for the majority of their life experience and define seclusion as being physically separated from the presence of others.

Laufer and Wolfe [35] approached the element of spatial environment notably by contrasting urban surroundings to rural surroundings. It can be argued that as the physical surroundings of an individual become more urban it becomes harder to obtain physical separation. Therefore, in an urban environment, obtaining privacy (in terms of being away from others) is harder to accomplish than in rural areas. According to Laufer and Wolfe [35], in a rural environment the home is considered a non-private space and individuals may need to leave the home to obtain privacy. However, in an urban environment people would learn to manage privacy at home by separating the space into private areas. In other words, due to a lack of options to be alone (which would suggest more privacy experiences overall), urban dwellers would be forced to learn to manage their interactions and information in order to obtain privacy. We suggest that this will increase their need to control their information and interactions. For rural dwellers, managing their location can accommodate their desire to be physically alone. As obtaining physical seclusion is arguably easier in a rural setting, the need for an individual to control his or her information and interactions should decrease. Thus, the more interaction they experience with others in their vicinity (i.e. the less physical seclusion people experience), the stronger their belief in their right to control their information and interactions. This leads us to the following hypotheses:

H5a The level of seclusion of the socio-physical environment will be negatively related to an individual's belief in his or her right to control the disclosure of his or her information.

H5b The level of seclusion of the socio-physical environment will be negatively related to an individual's belief in his or her right to control his or her interactions with others.

Marshall [40] developed a scale for measuring privacy preferences that includes six subscales: non-involvement with neighbors, seclusion of the home, solitude, privacy with intimates, anonymity, and reserve. Most of the items in this scale deal with the idea of being able to obtain physical separation from others, the importance of such separation to an individual, and the level of interaction desired. The ability to obtain physical separation from others is the traditional view of privacy [65]: "the right to be left alone"). Hence, we initially used items from Marshall [40] for this construct. However, in pretests, these items did not load cleanly. This finding is also supported in Pedersen [48]. We believe that this is due in part to the age of the instrument and the phrasing of the items. Thus, we used Marshall's non-involvement with neighbors scale as a foundation for ours, which Marshall found to load similarly for both students and adults.

3.5 Lifecycle

The lifecycle element is based on the idea that throughout an individual's lifespan his or her privacy conditions change. Laufer and Wolfe [35] describe a cycle that begins as a child when little privacy is available or desired due to the high dependency on another human being for survival. As individuals age, their independence, and therefore their ability to obtain privacy, increases. Eventually, at the end of the lifecycle, one may return to a heavy dependence on others, and may be afforded less privacy even though it may still be desired.

This general cycle goes from high dependence on others, to low dependence on others, back to high dependence on others. However, as an individual's dependence on others decreases through some stage of his or her lifecycle, others' dependence on the individual often increases. An individual may go through stages in their lifecycle in which they have various dependents: a spouse, children, aging parents, friends, and employees. It can be argued that as dependents increase, an individual's

responsibilities increase, and often his or her ability (or time) to be alone decreases. We therefore posit that responsibility could be used as a proxy for this cycle of life and dependency.

As an individual moves through life he or she exercises very little responsibility as a baby and that level of responsibility increases if/when he or she gets married, has children and/or takes on higher positions of leadership within his or her career. We would expect that increased responsibility is generally indicative of the more vigorous stages of life and thus the stages of our lifecycle in which one has the greatest expectations for control over privacy. Westin [65] explains that one of the functions of privacy is "emotional release", which certainly is more necessary as responsibilities increase. Thus, we can argue that as an individual's level of responsibility increases, he or she will develop a stronger belief in his or her right to control his or her interactions and information. This leads to the following two hypotheses:

H6a Responsibility will be positively related to an individual's belief in his or her right to control the disclosure of his or her information.

H6b Responsibility will be positively related to an individual's belief in his or her right to control his or her interactions with others.

To measure responsibility, we used a subscale measuring exercised responsibility from Hakstian et al. [29]. The level of responsibility exercised by an individual can be argued to increase with age and position. By using responsibility to measure the lifecycle element, we eliminate the need to use categorical variables for age, marital status, career stage and number of various dependents. While it would certainly be possible to use the categorical data, determining lifecycle categories has long been a topic of some debate [34] and the authors could find no widely accepted classification.

In Fig. 2, we propose a model based on Laufer and Wolfe's [35] theory to determine an individual's concept of privacy. We then use this model to examine behaviors in the online context. The purpose of the study is to present the operationalized model as well as examine the impact of the individual's privacy concept on an individual's actual online information and interaction behaviors. The insight gained from this study may help improve researchers' insight into why some individuals are more willing to release personal information in an environment that is publicly accessible. This insight may aid the development of privacy policies, privacy education, identity theft prevention technique, security technologies, and technology acceptance.

4 Methods and results

4.1 Scale development and survey administration

We conducted several pilot tests of the survey in 2007 and 2008. For the first pilot, conducted in the fall of 2007, the survey was administered to undergraduate business students from two universities in the southeastern region of the United States and resulted in a sample size of 183. A second pilot test was performed in the spring of 2008 using 165 undergraduate business students from one southeastern university. The results of the exploratory factor analyses (EFAs) after each of the first two pilots suggested modifications to the survey that were subsequently performed. For the third pilot, the survey was administered again in the spring of 2008 to undergraduate business students at a southeastern university, resulting in a usable sample of 386. The results from the third pilot indicated a stable instrument that was used for the final data collection.

The Qualtrics online platform (www.qualtrics.com) was used to administer the final survey. Participation was voluntary and anonymity was ensured. The construct measurement items were randomized using Qualtrics in order to reduce common method variance [52]. The full data collection was performed in the fall of 2014 on both the Mechanical Turk platform provided by Amazon, as well as employing a group of undergraduate business students from a large southeastern university. A total of 168 responses were collected from Mechanical Turk and 593 from the undergraduate student pool. Of those, 48 students and 14 Mechanical Turk workers did not finish the survey, and thus their partial responses were discarded. "Attention trap" questions were used in the survey to ensure that the respondents were cognitively engaged in the activity [46]. A total of 161 respondents did not pass the "attention trap" questions, indicating that they were not cognitively engaged, and were therefore removed from the final sample. The usable sample included 441 responses from the undergraduate student pool and 97 obtained from Mechanical Turk—for a grand total of 587 usable responses.

The final survey respondent profile is given in Table 1. The demographic information provided by the respondents reveals a sample with about 100 more males than females. There is variation in age, with most of the sample being between 18 and 29 years of age. The majority of the sample was under 50 years of age, but the use of data collected from Mechanical Turk added some variety in age as well as ethnicity. The majority of the sample reported being born in and/or a permanent resident of the U.S. There was also a fairly large number (61 and 56) reporting being born in or being a permanent resident of India or Pakistan.

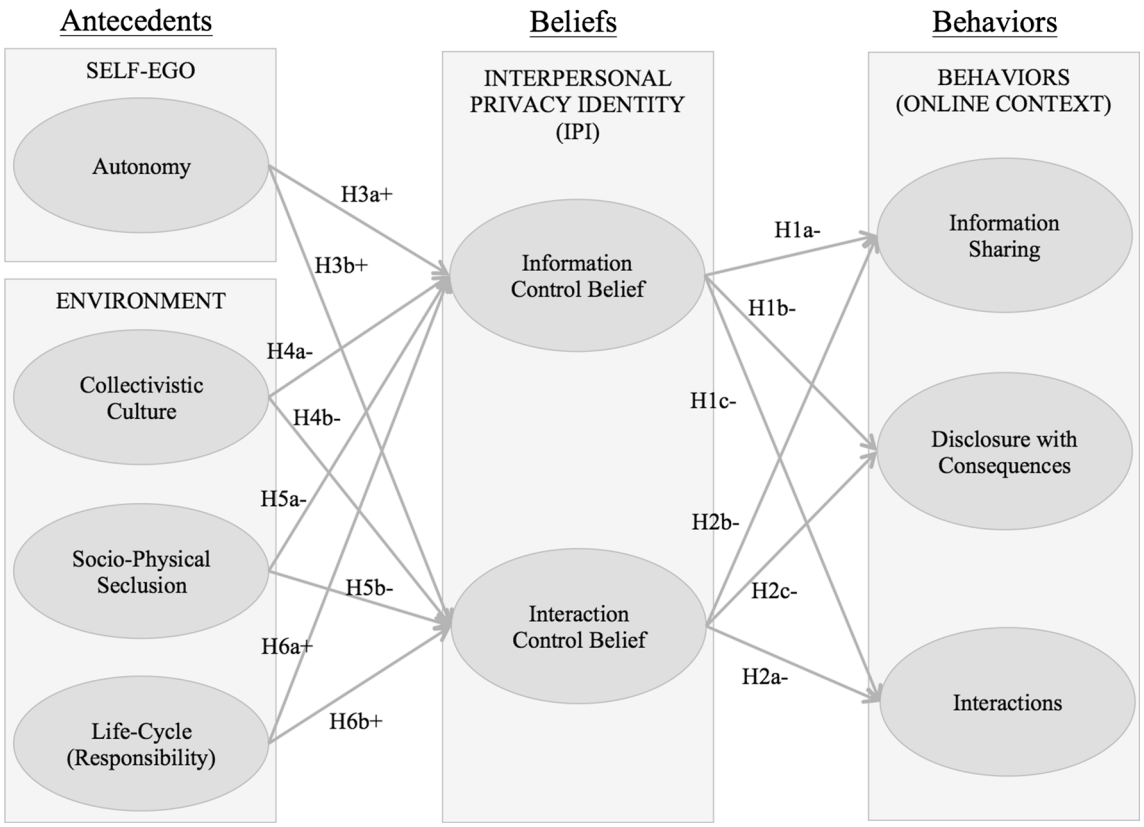

Fig. 2 Operational privacy model

Table 1 Demographic information

Sex		Age		Country of	Birth	Permanent residence	Race		Computer proficiency	
Male	320	<20	205	U.S.	441	465	White/Caucasian	362	Advanced	198
Female	218	20–29	271	Europe	10	4	Black/African American	16	Intermediate	320
		30–39	40	Asia	20	7	Asian	125	Novice	20
		40–49	11	Central America and Caribbean	4	2	Pacific Islander	2		
		50–59	3	India and Pakistan	61	56	Latino	14		
		60–69	7	New Zealand	1		Native American Indian	8		
		70–79	1	United Arab Emirates	1	1	Middle-Eastern	1		
							Other	10		

Approximately 62 % of the sample reported White/Caucasian as their ethnicity, with approximately 22 % identifying as Asian. The majority of the respondents categorized themselves as having intermediate computer proficiency or better.

Table 2 contains the items from the final survey along with the means and standard deviations for each item. A 5-point Likert-type scale was used with 1 being "Strongly Agree" and 5 being "Strongly Disagree." Presentation of the response scale has been shown to impact on how respondents answer and it is common in psychological research to present the scale with the most positive descriptor first [13]. The descriptive statistics highlight a few interesting points related to the sample used. On the physical seclusion items, relatively high means are observed which denotes that most of the sample has

Table 2 Items and descriptive statistics

Items	Mean	SD
Autonomy items		
A1. I resent it when people try to direct my behavior or activities	2.56	1.022
A2. I am very upset when other people or circumstances interfere with my plans	2.53	1.055
A3. I become upset more than most people I know when limits are placed on my personal independence or freedom	2.76	1.172
A4. I feel controlled when others have a say in my plans	2.95	1.107
Collectivistic culture items		
C5. I think that people in my culture share their ideas and newly acquired knowledge with their parents	2.32	0.939
C6. I think that people in my culture listen to the advice of their parents or close relatives when choosing a career	2.21	0.975
C7. I think that people in my culture take advice on how to spend their money	2.63	1.093
C8. I think that people in my culture consult their family before making an important decision	2.00	0.914
C9. I think that people in my culture discuss job or study related problems with their parents	2.01	0.908
Physical seclusion items		
S10. My friends have felt that they can drop in at my house any time they like	3.47	1.268
S11. For most of my life. I have lived in a neighborhood where people do things together now and then	3.53	1.214
S12. For most of my life, I have gotten to Know my neighbors	3.62	1.201
S13. For most of my life. I have talked to my neighbors	3.67	1.231
S14. I have been friends with some of my neighbors	4.04	1.066
Responsibility items		
R15. I often moke suggestions	1.88	0.844
R16. I have often been a group leader	2.15	1.064
R17. I enjoy takirg charge of things	1.98	0.977
R18. I have held many positions of responsibility in the past in my job(s) and extracurricular activities	1.97	0.973
R19. I like to take responsibility for making decisions	1.75	0.854
Interaction control belief items		
IT20. I have the right to control who I interact with	1.59	0.824
IT21. Control over who I interact with is very important to me	1.92	0.963
IT22. I have the right not to talk to someone	1.60	0.853
IT23. I have the right to avoid people who are rude	1.59	0.835
IT24. I have the right to avoid people I don't like	1.68	0.887
IT25. I pick and choose who I associate with	1.71	0.821
Information control belief items		
IF26. I have the right not to release sensitive information to any entity	1.66	0.902
IF27. I have the right to avoid having personal information released that I think could be financially damaging	1.57	0.876
IF28. I have the right to avoid having personal Information released that I think could be socially damaging to me	1.55	0.838
IF29. I have the right to avoid having personal information about me released that may go against social morals and attitudes	1.64	0.844
IF30. I have the right to have personal information that has been released by me used only in the manner that I intended	1.73	0.923
Online interaction behaviors items		
OI31.1 have communicated with people on the Internet that I have not physically met	2.42	1.388
OI32.1 have communicated with people on the Internet that I feel I do not personally know well	2.57	1.320
OI33. I have communicated with people on the Internet that I have not physically met but who are friends with someone in my social circle	2.57	1.365
OI34.1 have communicated with people on the Internet that I do not personally know but who have been recommended by one of my friends	3.04	1.377
Online information sharing behaviors items		
IS35. I have put personal information on the Internet so that anyone can see/access it	2.95	1.359
IS36. I have had a blog on the Internet so that anyone can see/access it	3.91	1.440
IS37. I have posted personal stories about myself on the Internet so that anyone can see/access them	3.39	1.343
Online disclosure with consequences items		
DC38. I have posted information on the Internet that could he socially damaging to me	3.63	1.290

Table 2 continued

Items	Mean	SD
DC39. I have posted information on the Internet that could be financially damaging to me	4.22	1.042
DC40. I have posted information on the Internet that could jeopardize my employment (or future employment)	3.87	1.234
DC41. I have posted information on the Internet that may be insulting to someone else	3.30	1.324
DC42. I have posted information on the Internet that may go against someone's moral values	3.09	1.390

experienced an urban socio-physical environment. This is consistent with the demographic information collected, which shows a majority of the participants listing urban areas as their permanent address. The responsibility items all have a mean close to 2 (slightly agree). This suggests that the respondents, on average, perceive themselves to have some level of responsibility. Although the sample contains a larger proportion of college age adults, expanding the data collection to Mechanical Turk added some variation in the stage of lifecycle. In fact, 47 respondents reported having children and the large majority of the sample (434) living with other people.

The respondents exhibited a strong belief in their right to control both their information and interactions. Interestingly, the interaction behaviors in the online context items had means mostly on the agree side of the scale (though with pretty large standard deviations). This indicates that many are likely to engage in riskier online interaction. The means for the information sharing behaviors in the online context are primarily between neutral (2.95) and slightly disagree (3.91). Similarly to the findings for interaction behaviors, the fact that the means for sharing personal information on the Internet are not terribly high suggests that the respondents are sharing some personal information online. Surprisingly, the online disclosure with consequences items mostly had means between 3 (neutral) and 4 (slightly disagree), with the exception of financially damaging information. Overall, they were a bit more adamant about not having released information that could be financially damaging than any of the other possible consequences. This could be due to identity theft (misuse of financial information) being one of the most publicized negative consequences of Internet use [6].

4.2 Reliability, convergent validity and discriminant validity

The privacy model employed in this article has nine (9) latent variables: Autonomy, Collectivistic Culture, Socio-Physical Seclusion, Life-Cycle (Responsibility), Interaction Control Belief, Information Control Belief, Online Interaction Behaviors, Online Information Sharing Behaviors, and Online Disclosure with Consequences. Table 3 contains Cronbach's α, composite reliability (CR), and average variance extracted (AVE) for each of the latent variables of the model.

The Cronbach's α for six of the nine latent variables in this study meet or exceed 0.70. The Cronbach's α's for Autonomy (0.6573) and Collectivistic Culture (0.6809) were slightly below the 0.70 recommended level. Given that these are established scales and the composite reliability is above the recommended value, we opted to make no further modifications. The Cronbach's α for Information Sharing Behaviors (0.5862) is also lower than might be desired, but the AVE is above the recommended 0.5 and the composite reliability was greater than the AVE, suggesting adequate reliability.

The CR for all constructs exceeds the 0.70 recommended value, which is evidence of their reliability. The AVEs for all but autonomy (0.4871) and collectivistic culture (0.4117) are at or above the 0.50 recommendation. These are slightly below the cutoff recommended by Fornell and Larker [25]. However, given the values for composite reliability and Cronbach's α, we feel the scales have adequate reliability. Table 3 also provides the construct correlation matrix with the square root of the AVE shown along the diagonal. None of the correlations are greater than the square root of the AVE above them, which suggests no discriminant validity issues.

The structural model was tested in SmartPLS Version 2.0.M3 (http://www.smartpls.de). The results of the confirmatory factor analysis (CFA) obtained from SmartPLS are given in Table 4. Most of the items have high factor loadings (>0.70). For a sample of our size, loadings greater than 0.30 are acceptable [28] and all loadings exceed this threshold. Furthermore, all the t-values are significant (>1.96). This combined with the values obtained for AVE indicate good convergent validity.

4.3 Structural model

The proposed model contained 9 latent variables. The usable sample from the final data collection was n = 587. The path model was tested in SmartPLS Version 2.0.M3 (http://www.smartpls.de). SmartPLS tests the model, by allowing the relationships among multiple independent and dependent constructs to be modeled simultaneously, using Partial Least Squares (PLS) regression [5, 26]. Figure 3

Table 3 Confirmatory factor analysis statistics

Latent factor	Cronbach's α	Composite reliability	AVE	A	C	S	R	IT	IF	OI	IS	DC
Autonomy (A)	0.6573	0.7903	0.4871	0.698								
Culture (C)	0.6809	0.7635	0.4117	0.112	0.642							
Socio-physical seclusion (S)	0.8161	0.8677	0.5766	0.012	0.215	0.759						
Responsibility (lifecycle) (R)	0.7932	0.8541	0.5405	0.125	0.231	−0.270	0.735					
Interaction control belief (IM)	0.8267	0.8737	0.5364	0.247	0.196	−0.195	0.277	0.732				
Information control belief (IT)	0.8212	0.8745	0.5837	0.158	0.278	−0.189	0.297	0.443	0.764			
Online interaction behaviors (OI)	0.8462	0.8637	0.6181	0.027	−0.008		0.129	0.090	0.081	0.786		
Online information sharing behaviors (IS)	0.5862	0.7628	0.5224	0.080	−0.078	0.069	0.045	−0.120	−0.100	0.333	0.723	
Online disclosure with consequences (DC)	0.8213	0.8262	0.4995	0.034	−0.159	0.080	−0.063	−0.208	−0.222	0.201	0.466	0.707

shows the operationalized model and contains the path coefficients, p values, and R^2 values for the proposed model. Most of the hypothesized relationships were supported at the level of $p < 0.01$ or below. SmartPLS outputs the path coefficients, t-scores (from which the p values can be calculated), and the R^2 values for the endogenous variables. The path coefficients and t-scores for each hypothesis are also provided in Table 5.

5 Discussion, contribution and limitations

Table 5 summarizes the results of the hypotheses tests—ten of fourteen were supported at a significant level. This study contributes to the existing IS privacy literature in three ways. First, by adapting theory from social psychology, we are able to explore a robust privacy concept (beliefs), comprised of an individual's belief in the right to control information disclosure and interaction with others. An individual's developmental and environmental conditions throughout his or her life contribute to the formation of this privacy concept and it is further refined by privacy situations experienced over time. The multi-faceted internal privacy concept (IPI), based on Laufer and Wolfe's [35] influential work, allows for the exploration of privacy at a finer-grained level than many privacy studies and provides an operational form very relevant to the social computing era.

Second, rather than using technological or data driven antecedents to the development of a privacy concern, the current study investigates developmental and environmental conditions an individual can operate within over a lifetime that could shape his or her concept of privacy. Both approaches are equally necessary, as they both emphasize a different perspective. It would also be valid to combine elements of both approaches in future studies. Our proposed model shows that the IPI is indeed influenced by the antecedents.

Considering the results obtained from the first half of the model, we found that autonomy, level of seclusion, and responsibility impacted both elements of the IPI in the direction postulated. Autonomy is one's internal presentation of independence. So it is reasonable to suggest that the more autonomous an individual is the more he or she expects to control his or her interactions with others and what he or she discloses. So, as anticipated, the relationships between autonomy and both interaction and information control beliefs were both significant and positive as hypothesized in H3a and H3b. These results follow a similar logic to those in the literature [16, 21, 38] where control and autonomy are found within the same concept (e.g. privacy concerns).

The impact of culture on both interaction and information control beliefs is significant but opposite to our assumptions. H4a and H4b are therefore not confirmed but we seem to have discovered a reversed relationship. The results indicate that the more collectivistic the individual, the more control is expected. Bélanger and Crossler [8] and Smith et al. [58] suggest that the link between individualism/collectivism and privacy has not yet been consistently identified in the literature. Prior literature has found theoretical or empirical support for a relationship between collectivism/individualism and privacy or information disclosure [36, 53]. Posey et al. [53] report that the more

Table 4 Confirmatory factor analysis

Item	Component									*t* value
	1	2	3	4	5	6	7	8	9	
Autonomy										
A1	0.727									15.99
A2	0.766									17.84
A3	0.685									13.12
A4	0.603									9.65
Collectivistic culture										
C5		0.470								5.24
C6		0.655								9.65
C7		0.358								3.58
C8		0.836								24.13
C9		0.763								17.11
Socio-physical seclusion										
S10			0.485							7.36
S11			0.689							14.82
S12			0.829							30.77
S13			0.840							32.62
S14			0.883							41.82
Responsibility (lifecycle)										
R15				0.749						23.28
R16				0.712						17.17
R17				0.813						34.86
R18				0.651						14.05
R19				0.742						21.90
Interaction control desire										
IT20					0.740					25.42
IT21					0.639					15.12
IT22					0.748					23.81
IT23					0.743					20.92
IT24					0.786					29.32
IT25					0.730					23.13
Information control desire										
IF26						0.714				18.94
IF27						0.775				27.28
IF28						0.842				46.19
IF29						0.798				32.65
IF30						0.681				18.32
Online interaction behaviors										
OI31							0.898			3.61
OI32							0.832			3.48
OI33							0.792			3.65
OI34							0.589			2.38
Online information sharing behaviors										
IS35								0.602		3.18
IS36								0.849		8.09
IS37								0.696		4.47

Table 4 continued

Item	Component									*t* value
	1	2	3	4	5	6	7	8	9	
Online disclosure with consequences										
DC38									0.761	7.56
DC39									0.913	20.84
DC40									0.743	9.57
DC41									0.515	3.45
DC42									0.518	3.51

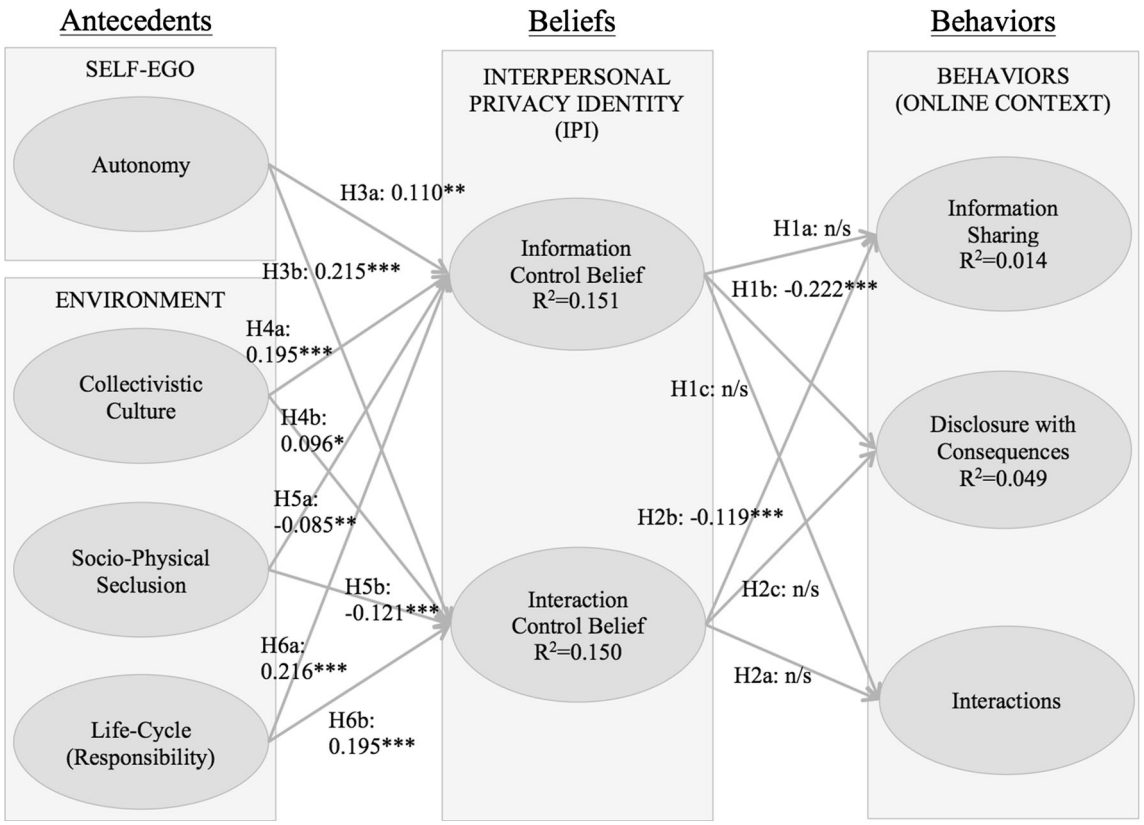

Fig. 3 Operationalized privacy model to examine online behaviors

collectivistic a culture the greater the information disclosed. Our original premise was similar to Posey et al.'s suggestion, namely that people in collectivistic cultures are encouraged to interact and share with others more than in individualistic cultures, and therefore, their belief in their right to control their information and interactions would be diminished. However, an alternative explanation could be that even though the quantity of information release is greater and/or the number of interactions larger, it does not mean that there is less of an expectation towards being entitled to control information and interaction. The requirement to socialize more could increase the exposure to privacy situations and through exposure increase the belief in the right for information and interaction control. Furthermore, in a collectivistic culture, the consequences of inappropriate information disclosure or interactions are not limited to the individual but are shared among the group. This may lead to hyper-vigilance out of concern for the group's control beliefs. Hence, there may be differing beliefs regarding information disclosure and interaction within the group (potentially encouraged) versus outside the group (potentially discouraged).

We find support for the position that the physical environment an individual is exposed to has an impact on privacy. Our results show a significant relationship between seclusion and the belief in information and

Table 5 Summary of hypotheses and results

No.	Hypotheses	Coefficient	*t* score	Results
H1a	An individual's belief in his or her right to control the disclosure of his or her information will be negatively related to online information sharing	–	–	Not significant
H1b	An individual's belief in his or her right to control the disclosure of his or her information will be negatively related to online disclosure with consequences	−0.222	6.138	Significant
H1c	An individual's belief in his or her right to control the disclosure of his or her information will be negatively related to online interaction behaviors	–	–	Not Significant
H2a	An individual's belief in his or her right to control his or her interactions with others will be negatively related to online interaction behaviors	–	–	Not Significant
H2b	An individual's belief in his or her right to control his or her interactions with others will be negatively related to online information sharing	−0.119	2.963	Significant
H2c	An individual's belief in his or her right to control his or her interactions with others will be negatively related to online disclosure with consequences	–	–	Not Significant
H3a	An individual's autonomy will be positively related to the individual's belief in his or her right to control the disclosure of his or her information	0.110	2.670	Significant
H3b	An individual's autonomy will be positively related to the individual's belief in his or her right to control his or her interactions with others	0.215	5.142	Significant
H4a	A collectivistic culture will be negatively related to an individual's belief in his or her right to control the disclosure of his or her information	0.195	4.416	Significant (but +)
H4b	A collectivistic culture will be negatively related to an individual's belief in his or her right to control his or her interactions with others	0.096	2.172	Significant (but +)
H5a	The level of seclusion of the socio-physical environment will be negatively related to an individual's belief in his or her right to control the disclosure of his or her information	−0.085	2.009	Significant
H5b	The level of seclusion of the socio-physical environment will be negatively related to an individual's belief in his or her right to control his or her interactions with others	−0.121	3.002	Significant
H6a	Responsibility will be positively related to an individual's belief in his or her right to control the disclosure of his or her information	0.216	4.616	Significant
H6b	Responsibility will be positively related to an individual's belief in his or her right to control his or her interactions with others	0.195	4.198	Significant

interaction control. Therefore, H5a and H5b are confirmed. The relationship between socio-physical seclusion and information control belief suggests that the more exposure individuals have with others in their neighboring vicinity over their lifetime (which would suggest a more urban environment with plentiful neighbors or a less secluded primary environment) the more entitled individuals believe themselves to be over the control of their information. This lends support to our argument that urban dwellers are more often exposed to privacy situations and therefore develop an internal representation that perceives control of their information to be important.

The findings regarding the last antecedent, life-cycle, are also as expected. We confirm H6a and H6b—that people with more responsibilities tend to have a stronger sense of entitlement towards their control over information and interaction. We argued that people with greater responsibilities, children, spouse, etc., would have a strong belief in their right to control their information and interactions with others. We used responsibility as a proxy for life-cycle. One can argue that responsibility increases as more dependents are acquired (spouse, children, aging family members, etc.) and positions of leadership in career paths are obtained. These additional responsibilities could quite possibly lead to changes in the expectations one has with regard to information and interaction control. We indeed found that those individuals with a high level of perceived responsibility did have a greater belief in their right to manage both their interaction and information.

Our third contribution was to explore the influence of the multi-faceted privacy concept on information and interaction behaviors in the online context. Socialization via the Internet has become extremely popular. Privacy management is arguably quite different in this communication medium. Furthermore, Laufer and Wolfe suggest that technology can modify general privacy beliefs and expectations of a society. An examination of privacy behaviors in this general context, is therefore, quite appropriate.

In the current study, we focus on behaviors that reflect the component nature of the IPI by creating two constructs to explore behaviors that map to the facets of the IPI: interaction behaviors in the online context and two constructs for information behaviors in the online context that explore general online information sharing behaviors and the release of information with possible consequences. Our

results indicate support for two of our six relationships. H1b and H2b are statistically significant relationships with substantial path coefficients. Therefore, a person with a strong belief in his or her right to control his or her private information will tend to be more cautious about disclosing information that could have future consequences. Additionally, a person with a strong belief in his or her right to control his or her interaction will be less likely to disseminate information in the online medium. This second finding is interesting in that it could be indicative of more sophisticated online privacy management strategies, such as limiting the audience of particular information. Future research into the particulars of this relationship, perhaps in specific situations such as OSNs or blogs, may be an interesting avenue to explore.

However, H2a and H1c are not supported. Therefore, neither interaction nor information control beliefs impacted the interaction behaviors in the online context. While this is a surprising result, there are several possible explanations for it that are interesting avenues to explore in future research. Our sample could have experienced fewer negative privacy experiences with regard to managing interactions. Fewer privacy experiences with IPI shaping consequences may cause individuals to have a harder time attaching a risk to interaction behaviors online. In developing the construct, our argument was that exploring interaction behaviors using types of participants grouped by lack of previous physical contact would imply risk. However, it is possible that the psychological distance created in online interactions may give the subjects a false sense of safety. Hence, the subjects may feel that they are managing their interactions because they do not take place "in real life". Lastly, while there has been a considerable amount of attention paid to managing one's online information in the popular media, interaction management has not been given quite as much attention (other than possibly with very young children) and controls to let users have fine-grained control over their interaction management are relatively new. On social media sites, users have been able to decide to be friends or not be friends with people, but it has only been fairly recently that more fine-grained control has been provided in terms of interaction and information management (circles, enhancements to privacy controls, friend classifications, etc.). As the use of such controls becomes more common, it will be interesting to explore how the emphasis on interaction changes behaviors in this context over time.

H1a and H2c were also not supported. A lack of support for H1a is surprising and a bit worrisome. This finding indicates that there is no defined relationship between belief in one's right to manage information and sharing information online. Future work should investigate whether this is due to a more fine-grained approach to what is or is not shared online, if it is just the case that people are often sharing information no matter what their IPI (e.g. perhaps due to the situational privacy calculus—information disclosed in a particular situation due to social pressure or the draw of some kind of incentive such as feedback or rewards), or because the consequences of the online environment have been laid out well enough that people have reduced the amount of personal information shared online. That H2c is not supported is less surprising and probably relates to a lack of sharing information with consequences in general rather than worrying about the scope of its release.

6 Conclusions and directions for future research

In this study, we implement an operational model of privacy built using theory proposed in Laufer and Wolfe [35]. We examine the influence of autonomy, culture, socio-physical seclusion, and responsibility on an individual's IPI. The IPI consists of two elements: an individual's belief in his or her right to control his or her interactions and information. We then develop constructs to examine behaviors reflecting privacy management in the online context. Specifically we look at individuals' interaction and information sharing behaviors in the online context and online disclosure with consequences behaviors.

The majority of our hypotheses are significant and interpretable, which suggests that exploring a privacy concept composed of the belief in one's right to control interaction and information offers encouraging perspectives for further research. The structure of the IPI is an alternative approach to exploring individual privacy beliefs and its use may be especially attractive in investigating social computing platforms and interactions.

Specifically, we found support for the influence of autonomy, level of seclusion, and responsibility on both facets of an individual's concept of privacy. Although the relationship was not in the direction postulated, the relationships between culture and both components of the IPI were significant. We also found that an individual's interaction control belief impacts his or her information sharing behaviors in the online context. It is also shown that as an individual's information control belief increases, the individual is more likely to consider possible consequences to the disclosure of information on the Internet. The research we conduct in this study develops a comprehensive model for privacy. Considering the complexity of the concept of privacy, we believe that the model could be further refined and improved through future work.

Since the addition of the interaction control belief construct is a novel addition to testing privacy, but can be argued to be increasing in practical importance, it would be interesting to further examine interaction behaviors. Perhaps the identification of what information should remain private is easier than the identification of who should be included in the circle of confidants. Also, as Westin [65] explains, people adapt their behaviors to accommodate the others. It could be argued that interaction is more difficult to manage (a more complicated facet) due to social complexities inherent to the process.

Bélanger and Crossler [8] and Smith et al. [58] suggest that the link between collectivism and privacy is not yet consistently identified in the literature. Our findings do not resolve that issue since we find a relationship opposite to our expectations. Nevertheless, the relationship found is significant and may point to more collectivistic individuals having more management oriented belief systems.

The study was somewhat limited by a lack of diversity in the sample. Specifically, future work may want to add more diversity in the sample with regards to culture or vary the dimensions of culture examined in order to more fully explore the culture construct.

Another interesting area of future investigation would be to explore the operationalized model or the use of the dual-faceted IPI in particular situations (e.g. Amazon, Facebook, etc.). For example, examining the decision of releasing a funny story about one's child on Facebook with regard to both interaction management (to which friends) and information management (releasing the full story, an edited story lacking detail, or not releasing it at all). In models that exchange our more general contextual (online behaviors) constructs with constructs for situational behaviors, the calculus of behavior could be modeled and perhaps draw additional insights tailored towards very specific privacy situations (e.g. overriding the belief in the right to manage information and/or interaction and releasing the story on Facebook in order to socialize). The use of situational constructs could lead to interesting future studies that explore the development of new dependent variables. Refinement of our current contextual variables could also be the subject of future work, including expansion of the contextual exploration, item development and refinement, and adaptation of scales.

References

1. Acquisti A (2004) Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM conference on electronic commerce, pp 21–29. ACM
2. Acquisti A, Gross R (2006) Imagined communities: awareness, information sharing, and privacy on the Facebook. In: Privacy enhancing technologies, lecture notes in computer science, vol 4258. Springer, Berlin, pp 36–58
3. Altman I (1975) The environment and social behavior. Brooks/Cole, Monterey
4. Altman I, Taylor DA (1973) Social penetration: the development of interpersonal relationships. Holt, Rinehart & Winston, Oxford
5. Anderson JC, Gerbing DW (1988) Structural equation modeling in practice: a review and recommended two-step approach. Psychol Bull 103(3):411–423
6. Anton AI, Earp JB, Young JD (2010) How internet users' privacy concerns have evolved since 2002. IEEE Secur Priv 8(1):21–27
7. Barnes SB (2006) A privacy paradox: social networking in the United States. First Monday 11(9):11–15
8. Bélanger F, Crossler RE (2011) Privacy in the digital age: a review of information privacy research in information systems. MIS Q 35(4):1017–1042
9. Bélanger F, Hiller JS, Smith WJ (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. J Strateg Inf Syst 11(3):245–270
10. Bennett CJ (1995) The political economy of privacy: a review of the literature. Center for Social and Legal Research, Hackensack
11. Berendt B, Gunther O, Spiekermann S (2005) Privacy in e-commerce: stated preferences vs. actual behavior. Commun ACM 48(4):101–106
12. Bierbrauer G, Meyer H, Wolfradt U (1994) Measurement of normative and evaluative aspects in individualistic and collectivistic orientations: The Cultural Orientation Scale (COS). In: Kim U, Triandis HC, Cigdem K, Choi S-C, Yoon G (eds) Individualism and collectivism: theory, method, and applications. Cross-cultural research and methodology series, vol 18. Sage Publications Inc, Thousand Oaks, pp 189–199
13. Chan JC (1991) Response-order effects in Likert-type scales. Educ Psychol Meas 51:531–540
14. Chellappa RK, Sin R (2005) Personalization versus privacy: an empirical examination of the online consumer's dilemma. Inf Technol Manag 6(2):181–202
15. Child JT, Pearson JC, Petronio S (2009) Blogging, communication, and privacy management: development of the blogging privacy management measure. J Am Soc Inform Sci Technol 60(10):2079–2094
16. Culnan M, Armstrong P (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organ Sci 10(1):104–115
17. Daft RL, Lengel RH, Trevino LK (1987) Message equivocality, media selection, and manager performance: implications for information systems. MIS Q 11(3):355–366
18. Dennis AR, Fuller RM, Valacich JS (2008) Media, tasks, and communication processes: a theory of media synchronicity. MIS Q 32(3):575–600
19. Derlega VJ, Chaikin AL (1977) Privacy and self-disclosure in social relationships. J Soc Issues 33(3):102–115
20. Derlega VJ, Metts S, Petronio S, Margulis ST (1993) Self-disclosure. Sage Publications Inc, Newbury Park
21. Dinev T, Hart P (2004) Internet privacy concerns and their antecedents—measurement validity and a regression model. Behav Inf Technol 23(6):413–422
22. Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. Inf Syst Res 17(1):61–80
23. Dinev T, Bellotto M, Hart P, Russo V, Serra I, Colautti C (2006) Privacy calculus model in e-commerce—a study of Italy and the United States. Eur J Inf Syst 15(4):389–402
24. Dinev T, Xu H, Smith JH, Hart P (2013) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. Eur J Inf Syst 22(3):295–316

25. Fornell C, Larker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. J Mark Res 18:39–50
26. Gefen D, Straub DW, Boudreau M-C (2000) Structural equation modeling and regression: guidelines for research practice. Commun Assoc Inf Syst 1(7):1–78
27. Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM workshop on privacy in the electronic society, pp. 71–80. ACM
28. Hair JF, Black WC, Babin BJ, Anderson RE, Tatham RL (2006) Multivariate data analysis. Pearson Prentice Hall, Upper Saddle River
29. Hakstian A, Suedfeld P, Ballard E, Rank D (1986) The ascription of responsibility questionnaire: development and empirical extensions. J Pers Assess 50(2):229–247
30. Hann I-H, Hui K-L, Lee SYT, Png IPL (2008) Overcoming online information privacy concerns: an information-processing theory approach. J Manag Inf Syst 24(2):13–42
31. Hui KL, Teo HH, Lee SYT (2007) The value of privacy assurance: an exploratory field experiment. MIS Q 31(1):19–33
32. Junglas IA, Johnson NA, Spitzmüller C (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur J Inf Syst 17(4):387–402
33. Kraut R, Patterson M, Lundmark V, Kiesler S, Mukophadhyay T, Scherlis W (1998) Internet paradox: a social technology that reduces social involvement and psychological well-being? Am Psychol 53(9):1017–1031
34. Lansing J, Kish L (1957) Family life cycle as an independent variable. Am Sociol Rev 22(5):512–519
35. Laufer R, Wolfe M (1977) Privacy as a concept and a social issue: a multidimensional developmental theory. J Soc Issues 33(3):22–42
36. Luo X, Warkentin M, Johnston AC (2009) The impact of national culture on workplace privacy expectations in the context of information security assurance. In: AMCIS 2009 Proceedings
37. Lwin M, Williams J (2003) A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. Mark Lett 14(4):257–272
38. Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf Syst Res 15(4):336–355
39. Margulis ST (1977) Conceptions of privacy: current status and next steps. J Soc Issues 33(3):5–21
40. Marshall N (1974) Dimensions of privacy preferences. Multivar Behav Res 9(3):255–272
41. Milne GR, Rohm A (2000) Consumer privacy and name removal across direct marketing channels: exploring opt-in and opt-out alternatives. J Pub Policy Mark 19(2):238–249
42. Moor JH (1997) Towards a theory of privacy in the information age. Comput Soc 27(3):27–32
43. Murphy RF (1964) Social distance and the veil. Am Anthropol 66(6):1257–1274
44. Nosko A (2011) To tell or not to tell: predictors of disclosure and privacy settings usage in an online social networking site (facebook). Theses and Dissertations (Comprehensive). Paper 1116
45. Norberg PA, Horne DR, Horne DA (2007) The privacy paradox: personal information disclosure intentions versus behaviors. J Consum Aff 41(1):100–126
46. Oppenheimer DM, Meyvis T, Davidenko N (2009) Instructional manipulation checks: detecting satisficing to increase statistical power. J Exp Soc Psychol 45(4):867–872
47. Pearce WB, Sharp SM (1973) Self-disclosing communication. J Commun 23(4):409–425
48. Pedersen D (1996) A factorial comparison of privacy questionnaires. Soc Behav Personal 24(3):249–262
49. Petronio SS (2002) Boundaries of privacy: dialectics of disclosure. State University of New York Press, Albany
50. Phelps J, Nowak G, Ferrell E (2000) Privacy concerns and consumer willingness to provide personal information. J Pub Policy Mark 19(1):27–41
51. Pirim T, James TL, Boswell K, Reithel B, Barkhi R (2008) An empirical investigation of an individual's perceived need for privacy and security. Int J Inf Secur Priv 2(1):42–53
52. Podsakoff PM, MacKensie SB, Lee J-Y, Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol 88(5):879–903
53. Posey C, Lowry PB, Roberts TL, Ellis TS (2010) Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. Eur J Inf Syst 19(2):181–195
54. Rensel AD, Abbas JM, Rao HR (2006) Private transactions in public places: an exploration of the impact of the computer environment on public transactional Web site use. J Assoc Inf Syst 7(1):19–50
55. Robins C, Ladd J, Welkowitz J, Blaney P, Diaz R, Kutcher G (1994) The personal style inventory: preliminary validation studies of new measures of sociotropy and autonomy. J Psychopathol Behav Assess 16(4):277–300
56. Rule JB (1974) Private lives and public surveillance: social control in the computer age. Schocken Books, New York, p 382
57. Simmel G (1950) The sociology of Georg Simmel: translated, edited and with an introduction by Kurt H. Wolff. The Free Press, New York
58. Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MIS Q 35(4):989–1016
59. Smith H, Milberg S, Burke S (1996) Information privacy: measuring individuals' concerns about organizational practices. MIS Q 20(2):167–196
60. Son JY, Kim SS (2008) Internet users' information privacy-protective responses: a taxonomy and a nomological model. MIS Q 32(3):503–529
61. Stewart K, Segars A (2002) An empirical examination of the concern for information privacy instrument. Inf Syst Res 13(1):36–49
62. Tavani HT (2007) Philosophical theories of privacy: implications for an adequate online privacy policy. Metaphilosophy 38(1):1–22
63. Van Slyke C, Shim JT, Johnson R, Jiang J (2006) Concern for information privacy and online consumer purchasing. J Assoc Inf Syst 7(6):415–444
64. Warkentin M, Johnston AC, Shropshire J (2011) The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur J Inf Syst 20(3):267–284
65. Westin A (1967) Privacy and freedom. Atheneum Publishers, New York
66. Xu H, Teo HH, Tan BCY, Agarwal R (2010) The role of push-pull technology in privacy calculus: the case of location-based services. J Manag Inf Syst 26(3):137–176