Journal of the Association for Information Systems (2019) **20**(4), 434-475
doi: 10.17705/1.jais.00540

RESEARCH PAPER

ISSN 1536-9323

Beyond Information: The Role of Territory in Privacy Management Behavior on Social Networking Sites

Shuaifu Lin[1], Deborah J. Armstrong[2]
[1]University of Central Arkansas, USA, slin8@uca.edu
[2]Florida State University, USA, djarmstrong@business.fsu.edu

Abstract

This study draws on communication privacy management theory to explore aspects of social networking sites (SNSs) that may influence individual privacy management behaviors and conceptualizes two behaviors for managing privacy on SNSs: private disclosure (for managing information privacy) and territory coordination (for managing territory privacy). Evidence from two studies of SNS members indicates that perceptions of trespassing over agreed-upon virtual boundaries within SNSs affects risk beliefs regarding information privacy and territory privacy differently. These distinct privacy risk beliefs, in turn, influence two privacy management behaviors. Theoretically, this study demonstrates that a more complete conceptualization of individual privacy management on SNSs should consider both information privacy *and* territory privacy; and that territory coordination is a more significant indicator of privacy management behaviors on SNSs than private disclosure. From a practical standpoint, this study provides guidance to SNS platform organizations on how to reduce individuals' privacy risk beliefs, encourage users to share private information, and potentially build larger online communities.

Keywords: Social Networking Site, Privacy Management Behavior, Territory Privacy, Information Privacy, Online Privacy.

Atreyi Kankanhalli was the accepting senior editor. This research article was submitted on January 27, 2017, and went through three revisions.

1 Introduction

The massive amount of personal information that has become available online and stored in the cloud has put individual privacy at the forefront of the discussion on the ability to safely store that information. Social networking sites (SNSs) such as Facebook and Twitter are types of virtual communities "that allow individuals to…construct a public or semipublic profile within a bounded system" (Boyd & Ellison, 2007, p. 211). SNSs are focused around sharing personal and/or private information (i.e., information about one's thoughts, values, and experiences that the individual can reasonably expect will not be made public) for the purpose of social interaction and relationship development (Benson, Saridakis, & Tennakoon, 2015).

Social profiling is the process of constructing a profile using an individual's voluntarily shared social data, and most often refers to the process of generating a profile with the assistance of technology (Cirit, Nikravesh, & Alptekin, 2005). While social profiling has been used to track terrorists (Andrews, 2002) and serial killers (Cater, 1997), its most current application

is employment-related. According to CareerBuilder's annual recruitment survey for 2017, 70% of employers use social networking sites to research and screen potential job candidates, up from 52% in 2015, 22% in 2008, and 11% in 2006 (Havenstein, 2008; Nauen, 2017; Nikravan, 2016). Social profiling is being used to select job applicants, but it can also be used to exclude applicants or deny access to people with the "wrong" social profile (Basulto, 2012). This trend reenergizes questions of online privacy, particularly within the social networking context.

There are over 275 million users on LinkedIn and Twitter, with approximately 2.2 billion users on Facebook. SNSs make their money from targeted advertising. Facebook made close to $8 billion in the first quarter of 2017 from digital advertisements. But, just ask the founders of MySpace—no users means no money. Thus, privacy within the context of SNSs should be a concern for individuals, employers and social networking service providers. To date, individual privacy management research on social networking sites has focused almost exclusively on the private information shared on these sites (e.g, Benson et al., 2015; Chakraborty, Vishik, & Rao, 2013; Chen, 2013; Gerlach, Widjaja, & Buxmann, 2015; Kisekka, Bagchi-Sen, & Raghav Rao, 2013; Li, Lin, & Wang, 2015; Shibchurn & Yan, 2015).

But information is just part of the privacy story. In Altman's (1975, p. 18) general theory of privacy, where privacy is defined as "the selective control of access to the self", the concept of "the self" also includes personal spaces or territories. Territories are bounded physical areas that individuals perceive as their own (Altman, 1975; Brown, Lawrence, & Robinson, 2005; Brown & Robinson, 2011), and within which they may place objects and information. For example, within one's home (a private physical territory) an individual may place objects such as furniture, bills, computers, and so on. These objects have information associated with them, and the associated information may be personal and/or private to the individual. For example, the rug (object) in one's dining room (territory) may be Persian and a treasured gift from late Aunt Mary (personal information). Thus, the notion of territory conveys the idea of ownership of a space, including the objects and information within that space. While the individual may invite others into the territory, trespassing into that space is not acceptable. In the physical world, trespassing can include something as innocuous as cutting through a neighbor's backyard, to hunting on private land, to breaking into an individual's home with malicious intent. In each of these scenarios, one's private space (e.g., territory) is being intruded upon.

So, what about an individual's private space on the Internet? Dinev et al. (2006, p. 393) relate private space and public space to perceptions of privacy, where privacy protection is strongly synonymous with the creation of a privacy zone. Within the context of Facebook, such a zone is established with the management of privacy settings. This enables users to determine who should have access to their profiles, and to define the level of access their network members have to their profiles. Having access to a profile on Facebook implies that a network member is able "to view and comment on any information posted on the profile and to tag the profile owner in contents (e.g. photos, videos, messages) shared by a network member" (Beldad, 2016, p. 22).

A place can be thought of as a container within which individuals have experiences and express themselves (Halford & Leonard, 2006) and "is formed by what people do within the boundaries of this container and by how they interact with others in it" (Saunders, Rutkowski, van Genuchten, Vogel, & Orrego, 2011, p. 1081). Related to this is the idea of a "third place". Oldenburg (1989) originally defined a third place as a physical location beyond home and work where people informally gather to socialize with each other (e.g., coffee shop). Researchers are beginning to explore online third places (Peachey, 2010; Soukup, 2006), and specifically third places within an online gaming context (e.g., Ducheneaut, Moore, & Nickell, 2007; Rao, 2008; Steinkuehler & Williams, 2006), an online music sharing context (Mechant & Evens, 2011), and an online academic learning environment (Aldosemani, Shepherd, Gashim, & Dousay, 2016).

An individual becomes attached to a specific place because "she has had activities that are meaningful within its boundaries" (Goel, Johnson, Junglas, & Ives, 2011, p. 751). Thus, an individual may have fond childhood memories of family vacations and become attached to a physical place (e.g., cabin in the mountains), or become attached to the virtual place where she announced her first pregnancy to her family (e.g., Facebook). On the Internet, a virtual place is a "bounded space imbued with meaning" (Saunders et al., 2011, p. 1080), and in essence, an SNS is a publicly accessible virtual place (Bateman, Pike, & Butler, 2011).

Within the framework of online places, in addition to public places, SNSs allow individuals to create semipublic places (i.e., third places) (Boyd & Ellison, 2007). Most SNSs allow individuals to set boundaries around their online places so they can interact differently with different groups of people and a few researchers have begun to explore SNS privacy settings (e.g., Beldad, 2016; Heirman, Walrave, Vermeulen, Ponnet, Vandebosch, Van Ouytsel, & Van Gool, 2016; Lankton, McKnight, & Tripp, 2017; Spottswood & Hancock, 2017). Drawing on Brown et al.'s (2005) theory of territory (also in Altman, 1975 and Brown & Robinson, 2011), we build on the idea of a third place and refer to these bounded online places as virtual territories. More precisely, a private virtual

territory on an SNS is a bounded location within cyberspace that an individual perceives as his/her own, where the individual can store and/or display objects and information, but also where the individual may control the level of access given to and interaction allowed with specific groups and/or subgroups of others. Examples of virtual territories on social networking sites include an individual's online photo album on Instagram, timeline (wall) on Facebook, or home on Twitter to name a few. For example, while an individual may feel comfortable announcing her first pregnancy to her family on Facebook by posting the ultrasound picture, she might not want some SNS members (e.g., her coworkers) to see the image. She also might not want some other SNS members to be able to leave comments. In this case, she controls the level of access to and interaction within her private virtual territory by establishing a boundary regarding who can and cannot access the image, comment on it, and/or link (tag) other members to it.

After the San Bernardino, California terrorist attack of 2015, Hilary Clinton made the following statement referencing virtual territories, "Resolve means depriving jihadists of *virtual territory*, just as we work to deprive them of actual territory.… They [the terrorists] are using websites, social media, chat rooms and other platforms to celebrate beheadings, recruit future terrorists and call for attacks" (qtd., Perlroth & Issac, 2015, emphasis added). Previous research has also hinted at the existence of a virtual territory as regards to privacy on the Internet. For example, within an e-commerce context, Hong and Thong (2013) assert that information privacy concerns contain two factors that they label interaction management and information management, thus broaching the territory/information distinction.

We assert that not only can individuals place information in a private virtual territory, they can also manage the privacy of that virtual territory. To manage virtual territory privacy, individuals control the level of access to and interaction within the territory (i.e., allowing/disallowing someone to see a post, to comment on the post, and/or to allow others to see or comment on the post). "Contrary to popular belief, privacy does not necessarily mean withdrawing from people. Instead, it involves controlling the amount and type of contact one has with others" (Pedersen, 1999, p. 397). When participating on a social networking site one is choosing to interact with others, while still maintaining control over one's territory and information within the SNS.

Previous studies have characterized privacy as comprising multiple dimensions (e.g., Burgoon, Parrott, Poire, Kelley, Walther, & Perry, 1989; Westin, 2003). Ball, Daniel, and Stride (2012) identified three distinct dimensions of workplace privacy and labeled them: personal information privacy, working environment privacy, and solitude privacy. Westin (1967) identified four dimensions (solitude, intimacy, anonymity, and reserve) in which the reserve can be equated to Westin's concept of privacy where one can control, or reserve, information as desired. While several dimensions of privacy have been proposed in the literature, a common thread is that they involve opening and/or closing boundaries in an attempt to optimize access by others or achieving the desired level of contact between the self and others in a given circumstance. For example, Taylor and Ferguson (1980, p. 237) found "a sturdy linkage between privacy and territoriality".

By inviting someone to access and interact with a Facebook post, individuals share with online social network members not only their private information, such as feelings, life stories, and objects (e.g., photos), but also their private virtual territory. Control-related issues have been identified as the top three predictors of Facebook usage intensity (Jordaan & Van Heerden, 2017). The recent high-profile privacy issues with Facebook have again highlighted concerns regarding personal information and control. A national online poll, conducted by Reuters less than one month after the Cambridge Analytica scandal indicated that only 23 percent of Facebook users believe they have "total control" over their information on the platform (Kahn & Ingram, 2018).

If individuals want high territory privacy, they could tightly control the level of access to and interaction within their virtual territory by making their specific Facebook "posts" accessible only to close friends, disabling comments, and disallowing invitations of other friends (tagging). But if individuals want low territory privacy, then they could more loosely control the level of access to and interaction within their territory by making some Facebook "posts" public, enabling comments, and allowing invitations (tagging). Therefore, to manage privacy on SNSs, individuals determine not only what information they want revealed (information privacy), but also control the level of access to and interaction within their private virtual territories (territory privacy). Stated another way, within the context of an SNS, information privacy considers the revelation of an individual's private information, and territory privacy considers the level of access to and interaction within an individual's private space.

Previous literature on online privacy has assumed all components of an online community contribute equally to participants' evaluation of their risk exposure (e.g., Chen, Lu, Guo, & Lin, 2013; Debatin, Lovejoy, Horn, & Hughes, 2009; Dinev & Hart, 2006) and privacy management behavior (e.g., Benson et al., 2015; Chen, 2013; Cheung, Lee, & Chan, 2015; Li et al., 2015). Because individuals may have differing views of their privacy risks, we argue that research

should consider both information and territory when considering individual privacy on SNSs. Thus, privacy management behavior should not be restricted to the behavior that determines the revelation of private information (i.e., private disclosure; Derlega, Metts, Petronio, & Margulis, 1993; Posey, Lowry, Roberts, & Ellis, 2010), but should also embrace individual behavior in order to regulate the level of access to and interaction within a private virtual territory (i.e., territory coordination; Petronio, 2002). Thus, we explore the following research question:

RQ: What factors influence how individuals manage their information privacy and territory privacy on SNSs?

This research makes two main theoretical contributions. First, this study introduces the construct of territory privacy and empirically examines it within the context of SNSs. We contribute to the literature by the discovery that information privacy and territory privacy are two essential and distinct components of an individual's perception of online privacy on an SNS. Second, although prior literature has hinted at individual behaviors to manage virtual territories (e.g., Child, Pearson, & Petronio, 2009; Jiang, Heng, & Choi, 2013), these behaviors have not been systematically conceptualized and studied. This study draws on internet privacy theory (Malhotra, Kim, & Agarwal, 2004) and communication privacy management theory (Petronio, 1991, 2002) to explore how individuals make decisions about managing privacy on SNSs, and examines two behaviors for managing privacy: private disclosure (managing the revelation of private information) and territory coordination (controlling the level of access to and interaction within virtual territories).

2 Background

2.1 Privacy in an Offline Context

We define personal information as information that can be used to identify a person (Culnan & Armstrong, 1999), while private information refers to the personal information that an individual may not make public, such as a childhood nickname or birthdate (Petronio, 2002). There is no absolute differentiation between what information is public, personal, or private, as individuals may perceive different degrees of sensitivity regarding the same information. Consistent with previous research on information privacy (e.g., Fernandez, 2008) and our research objective, we define *information privacy* as the freedom of an individual to determine the extent to which private information is communicated to others (Westin, 2003).

In the general privacy literature, privacy is concerned with how individuals regulate access to themselves (Margulis, 2003; Smith, Dinev, & Xu, 2011) and includes the regulation of boundaries to control access to the self. The bounded areas that individuals perceive as their own are defined as *territories*, and *territoriality* is "an individual's behavioral expression of feelings of ownership toward a physical or social object" (Brown et al., 2005, p. 578). In the offline context, the concept of territory privacy has been used to understand privacy concerns (see Brown, 2009; Fernandez, 2008; Ji & Lieber, 2010; Kimmons & Austin, 2012) and the resulting behaviors (design of rural settlements: Al-Nowaiser, 1987; protecting a home: Fernandez, 2008; introduction of wind turbines: Pedersen, Hallberg, & Waye, 2007).

To achieve the desired level of privacy, individuals regulate the level of access to their territory by regulating the territory's boundaries (Altman, 1975); for example, by erecting walls or fences, closing doors or windows, making signs, or arranging objects within the territory. Based on the work of Altman, individuals can regulate inputs from others in the form of interaction and outputs to others in the form of information. For example, a closed office door with a sign stating "Come in" indicates a different level of privacy than a sign stating "Do not disturb". If the individual locks the door, this may indicate that yet a different level of privacy is required. Further, a desk in the middle of a professor's office may imply a separation of a private-work zone for the professor and a semipublic zone for visitors. If an individual ignores the "Do not disturb" sign and walks into the unlocked office, or a visitor walks directly into the professor's private-work zone, most likely some discomfort or tension will arise between the two individuals as the visitor has trespassed into the individual's territory. Altman's privacy theory contends that controlling access to the self includes not only controlling what information about the self is communicated to others (*information* privacy), but also controlling the level of access to and interactions with the self (*territory* privacy). Each of these types of privacy are detailed within the SNS context.

2.2 Privacy in an SNS Context

In the SNS context, studies have identified several motives for disclosing information, such as the individuals' attitude toward the SNS (Chen & Sharma, 2015); concerns about social influence, reciprocity, and trust (Posey et al., 2010), and to the desire to "show off" to others (Waters & Ackerman, 2011). Bateman et al. (2011) found that the perceived publicness of an SNS negatively influenced individuals' self-disclosure intentions.

Recall that an SNS allows an individual to create a public or semipublic space within a bounded system to place information into and to interact with others to develop social relationships (Boyd & Ellison, 2007). On SNSs, territories are social constructions that come

into being through the territorial behavior of individuals (Brown et al., 2005). A *private virtual territory* within an SNS context is a location in cyberspace where an individual can store and/or display objects and information, but also where the individual interacts with others for social purposes. We create meaning through interactions with others, and in doing so, socially construct our reality (Saunders et al., 2011). As Brown et al. (2005, p. 579) state, "As with all social constructions, an object only exists as a territory to the extent that it is reproduced in social interaction among relevant actors". Like in the physical world, individuals regulate access to their private virtual territory by regulating the boundaries of that territory. For example, on Facebook members of an individual's social network may (or may not) be able to view posts on an individual's "timeline", respond to (comment on) a post, "like" a post made by the individual, and/or invite (tag) others to see the post. Thus, social network members may (or may not) have access to the private virtual territory and may or may not be allowed to interact within the private virtual territory, depending on the level of privacy the individual desires.

Altman's privacy theory contends that privacy is an input process and an output process, as "people and groups attempt to regulate contacts *from* others and output they make *to* others" (Altman, 1975, p. 11). For the input process, people regulate privacy regarding what comes in from others; for the output process, people regulate privacy in terms of what goes out from the self. On SNSs, individuals manage the input process by regulating the level of access to and interaction within their private virtual territories (territory privacy), and individuals manage the output process by regulating the revelation of private information (information privacy). Following these discussions, we assert that it is appropriate (and needed) for research on individual privacy on SNSs to investigate territory privacy, in addition to information privacy. We assert that *individual privacy on social networking sites* is the freedom of an individual on a social networking site to determine to what extent and to whom (a) one's private information is revealed, and (b) one's private virtual territory is accessible.

2.3 Model and Hypotheses

The main purpose of the research model is to investigate, within the SNS context, how an individual manages information privacy and territory privacy. A portion of the research model—i.e., the nomological network of information privacy concerns, information trusting beliefs, and information privacy risk beliefs—has been examined in the e-commerce context by Malhotra et al. (2004). Our research builds on and extends previous work by using a communication privacy management lens, incorporating the concept of territory privacy management, and situating the model within an SNS context.

Communication privacy management (CPM) theory (Petronio, 1991, 2002) was originally developed to explain how an individual reveals or conceals private information to confidant(s). CPM theory uses the analogy of a boundary to explain individuals' privacy management behaviors. Boundary synchronicity/ harmony occurs when individuals and their confidants understand and comply with mutually agreed-upon privacy practices. Boundary turbulence occurs when an individual is concerned about information leakage through the boundary. The main contention of CPM theory is that when boundary synchronicity is disrupted (i.e., boundary turbulence occurs), individuals and their confidants exert privacy management behavior to regain boundary synchronicity.

Within the information systems (IS) literature CPM theory has been used to study information privacy management in a variety of contexts—such as electronic commerce [1] (e.g., Metzger, 2007), health information disclosures (e.g., Anderson & Agarwal, 2011), employee monitoring (e.g., Chang, Liu, & Lin, 2015), blogging (e.g., Child & Agyeman-Budu, 2010), individual privacy management strategies (e.g., Lankton et al., 2017), individual versus group privacy management practices (e.g., De Wolf, Willaert, & Pierson, 2014), and social networking (e.g., Bateman et al., 2011; Chen & Sharma, 2015; Posey et al., 2010; Waters & Ackerman, 2011).

Although CPM theory focuses on explaining the management of one's information-related privacy, the idea that privacy involves control over boundaries is highlighted here in the exploration of territory privacy. A *collective virtual territory* (CVT) is the area in an individual's private virtual territory into which the individual invites confidant(s) (i.e., social network members), thus establishing a confidant group. An individual establishes a CVT boundary by determining who is allowed to access a CVT, how they can access the CVT, and how they can interact in the CVT. When a collective virtual territory is established, the individual and his/her confidants are co-owners. For example, according to Child et al. (2009), establishing a Facebook page creates a CVT in which a specific community (i.e., confidant group) is given access to the territory. An individual may manage multiple

[1] Assuming information privacy as the focus within an e-commerce context is appropriate because the e-commerce environment only allows an individual to decide what information to share with an organization. Once the information is disclosed, the individual rarely has further control over the information.

CVTs on a social networking site such as a photo album (CVT_1) and a message board (CVT_2). See Figure 1 for a graphical representation of the territories under discussion. Each of the collective virtual territories (CVT_1, CVT_2, CVT_3, and CVT_4) denotes a different area within an individual's private virtual territory on a social networking platform.

Based on Malhotra et al.'s (2004) theory of internet privacy, the research model presented next is comprised of three primary components: privacy management, context-specific factors, and personal dispositions. The components of the model are detailed next working from right to left in Figure 2.

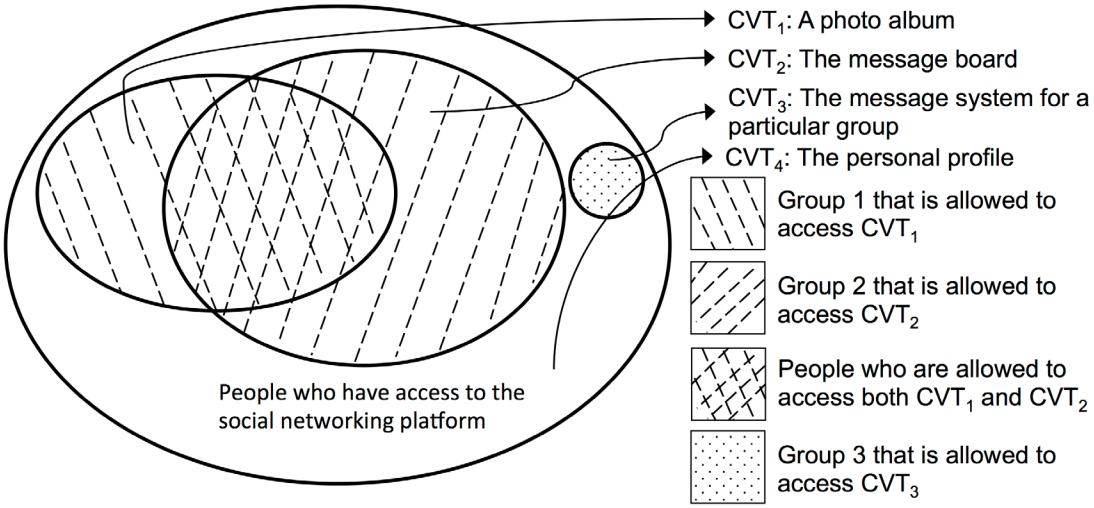

Figure 1. Virtual Territory

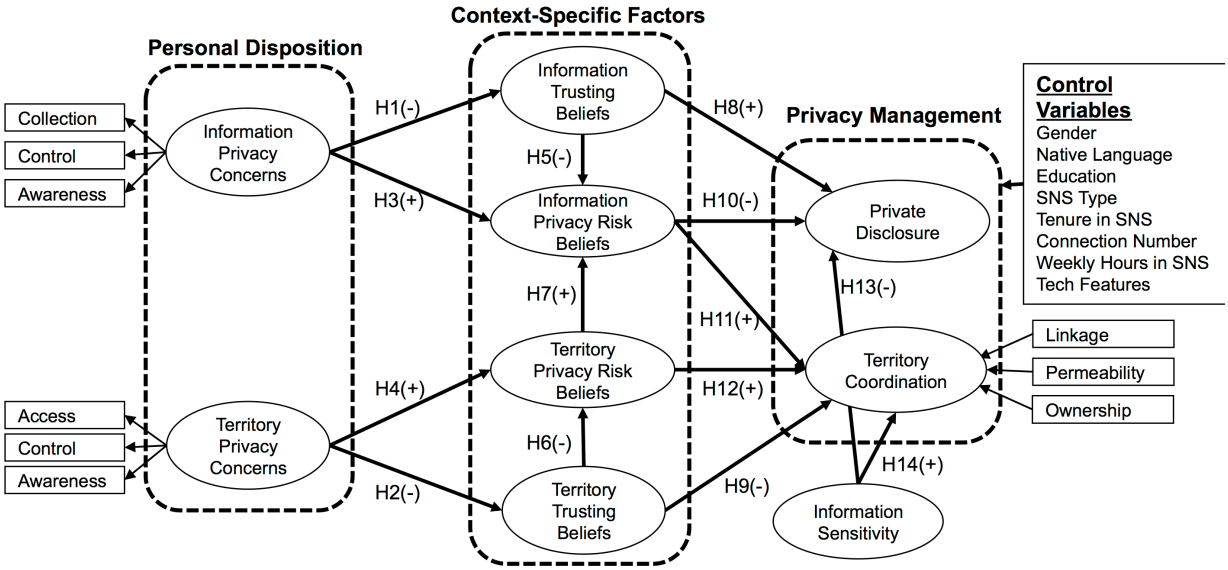

Figure 2. Research Model

In the research model (Figure 2), the first component, privacy management, is behavior that determines the level of revelation of private information and the regulation of the level of access to and interaction within a private virtual territory. Private disclosure occurs when individuals voluntarily and intentionally reveal information about themselves to others (Derlega et al., 1993; Petronio, 2002; Posey et al., 2010). Through private disclosure, an individual determines what private information is shared and what is concealed. Territory coordination occurs when individuals manage their private virtual territory. Through territory coordination, individuals determine who can and cannot access their various private virtual territories, and also how confidants can interact within their virtual territory. Individuals regulate the level of access to their private virtual territory by regulating the boundaries around their private virtual territory in various forms, including differentiating between people (e.g., who can have access), areas (e.g., which areas are accessible), and interactions (e.g., level of access). For example, some SNSs have tools (i.e., privacy settings) for determining who can see an individual's specific posts or personal information. Other SNS tools allow individuals to manage whether a post can be tagged (i.e., allow friends to invite others to see/respond to the post) and to review a tag before it appears. Yet other SNS tools allow individuals to manage who may connect to the individual, who may message the individual, who may post, and who may send app/event invites. In essence, to manage privacy on SNSs, an individual determines what private information is to be revealed (i.e., private disclosure; Derlega et al., 1993; Petronio, 2002; Posey et al., 2010), and who the individual wants to grant access to and interact with in the private virtual territory (i.e., territory coordination).

The second component in the research model—context-specific factors—represents a trust-risk appraisal that helps explain individuals' privacy management behavior. In their theory of internet privacy, Malhotra et al. (2004) included trusting beliefs and risk beliefs to explain an individual's revelation of private information in the e-commerce context. On SNSs, there is a level of perceived uncertainty related to privacy and participation in online social networks (the element of risk) and a level of one's willingness to be vulnerable (the element of trust). These factors can influence both types of privacy management behavior. Trust is the confidence that individuals will act as expected, and without that confidence, individuals might more stringently manage their privacy on SNSs (i.e., manage the risk). For example, Child, Petronio, Agyeman-Budu, & Westermann (2011) found that because of anticipated risks (i.e., information privacy risk beliefs), bloggers often regret disclosing certain information and sometimes remove posted information (i.e., private disclosure). Similarly, because of anticipated risks (i.e., territory privacy risk beliefs), an individual might remove someone from their "close friends" confidant group in their SNSs (i.e., territory coordination). In this research we assert that the higher the perceived vulnerability and privacy risk on a specific SNS, the higher the likelihood individuals will increase their privacy management behavior.

The third component in the research model is personal dispositions. Personal dispositions can be thought of as general tendencies or enduring characteristics of individuals (Ormerod, McKenzie, & Woods, 1995) that can influence a variety of outcomes. An individual's perception of a situation can be influenced by personal characteristics and past experiences (Hornsey, 2008). Malhotra et al. (2004) contend that personal dispositions (i.e., information privacy concerns) influence information trusting beliefs and information risk beliefs. In our research, information and territory privacy concerns capture individuals' anxiety, feelings, and/or disposition toward SNS privacy practices in general and are not specific to one SNS. While people may have different ideas about what is fair or appropriate concerning privacy practices, an individual's general tendency regarding concerns about privacy (i.e., information and territory privacy concerns) influences the individual's trust beliefs and risk beliefs in a specific SNS context.

We now turn to detailing the constructs and relationships between the constructs. We begin by developing the hypotheses for the distal antecedents, and then the proximal antecedents of privacy management behavior (moving from left to right in the model in Figure 2).

2.3.1 Privacy Concerns and Trusting Beliefs

Information privacy concerns refers to individuals' concerns about the information privacy practices of their SNS members. *Information trusting beliefs* is the degree to which an individual believes SNS confidant group members will behave in a dependable manner regarding his or her private information (Malhotra et al., 2004). Research on trust has suggested that one's perception of trust depends on perceptions of how others will behave (Good, 1988), or the trustworthiness of others (Mayer, Davis, & Schoorman, 1995). Research has also found that an individual with high information privacy concerns is less likely to trust others' information privacy practices in both an e-commerce context (Eastlick, Lotz, & Warrington, 2006; Fortes & Paulo, 2016; Malhotra et al., 2004; Van Slyke, Shim, Johnson, & Jiang, 2006), and an SNS context (Chang, Liu, & Shen, 2017). When an individual has the tendency to worry about information being leaked, the individual may perceive others as less trustworthy or honest regarding his or her private information in the specific SNS context (low information trusting beliefs). We confirm the

relationship in the SNS context so that we can compare the relationship with that of the territory privacy concerns / territory trusting beliefs relationship.

H1: On a social networking site, individuals' information privacy concerns will negatively influence their information trusting beliefs.

Territory privacy concerns refers to an individual's worries about SNS members' territory privacy practices. *Territory trusting beliefs* is the degree to which an individual believes his/her SNS confidant group members will behave in a dependable manner regarding his or her private virtual territory (i.e., confidants will not violate the individual's expectations regarding the virtual territory). An individual with high territory privacy concerns may anticipate that SNS confidant group members will share the private virtual territory with undependable others or act inappropriately in the private virtual territory. Therefore, the individual may be more suspicious and less trusting of SNS confidant group members. For example, Mary has concerns about controlling access to her private virtual territory because she does not know how to use the configuration tools to configure the visibility of her private virtual territory as she would like to. Because she cannot adequately control her territory, she strongly feels that her confidants also cannot be depended on to control the territory as she would like (i.e., they will make her private virtual territory public without her knowledge or permission). Thus, the degree to which an individual is concerned about the vulnerability of the territory (territory privacy concerns) influences the perception of confidant trustworthiness regarding the virtual territory (territory trusting beliefs).

H2: On a social networking site, individuals' territory privacy concerns will negatively influence their territory trusting beliefs.

2.3.2 Privacy Concerns and Privacy Risk Beliefs

Information privacy risk beliefs refers to an individual's perception of the likelihood of loss due to sharing private information with SNS confidant group members. Research has established a positive relationship between information privacy concerns and information privacy risk beliefs in an e-commerce context (Fortes & Paulo, 2016; Hong & Thong, 2013; Malhotra et al., 2004; Van Slyke et al., 2006) and an SNS context (Fogel & Nehmad, 2009; Liang, Liu, Lu, & Wong, 2015). On an SNS, when an individual has the tendency to worry about information being leaked, the individual may perceive greater risk of potential loss. We confirm this relationship in our context so that we can compare the information privacy concerns / information privacy risk beliefs relationship with the territory privacy concerns / territory privacy risk beliefs relationship.

H3: On a social networking site, individuals' information privacy concerns will positively influence their information privacy risk beliefs.

Theoretical frameworks of risk behavior have suggested that the tendency to worry about negative consequences may make an individual weigh the negative outcomes as more significant and thus possibly overestimate the probability of loss (Schneider & Lopes, 1986; Sitkin & Pablo, 1992). According to James et al. (2015), privacy concerns in online social networks include the desire to control information *and* interaction, leading to the "dual privacy decision" in which individuals choose what information to release and also who may have access to and interact within the virtual territory. Individuals with higher territory privacy concerns may worry about the negative consequences resulting from allowing access and interaction privileges within their private virtual territories.

From a CPM theory perspective, when individuals have territory privacy concerns, they worry about collective privacy practices, the vulnerabilities of their private virtual territory, and how confidant group members on their SNS will treat the collective virtual territory. For example, John may feel concerned about the fact that he does not know how to (or cannot) prohibit his college friends from tagging (i.e., inviting) others into his private virtual territory (high territory privacy concerns). This concern may further increase John's perception of potential loss of territory privacy (i.e., territory privacy risk beliefs).

Territory privacy risk beliefs refers to an individual's perception of the likelihood of loss from allowing SNS confidant group members to access and interact in one's private virtual territory. When individuals perceive ambiguity or have concerns about virtual territory privacy management practices, the individuals may believe that their private virtual territory is more vulnerable or at risk. For example, John has no idea of the consequences of a confidant allowing access to unknown others (allows tagging) and how the unknown others will behave in the virtual territory. Will the unknown others respect the virtual territory and act appropriately or will they be disrespectful (e.g., break the agreed-upon privacy management practice and further share access to the virtual territory)? Because John is worried about the practice of tagging (high territory privacy concerns), he may believe that his private virtual territory that is currently shared with his college friends will be unexpectedly trespassed into by some unknown other (high territory privacy risk beliefs). Thus, the higher the level of concern regarding the vulnerability of a

virtual territory, the higher the perceived probability of loss of territory privacy.

H4: On a social networking site, individuals' territory privacy concerns will positively influence their territory privacy risk beliefs.

2.3.3 Trusting Beliefs and Privacy Risk Beliefs

An individual with high information trusting beliefs accepts that SNS confidant group members are trustworthy and would not share private information with others. Research has found that within an e-commerce context an individual with high information trusting beliefs is less likely to expect a loss due to sharing private information (Jarvenpaa, Tractinsky, & Saarinen, 1999; Malhotra et al., 2004). The higher an individual's information trusting beliefs, the lower the individual's perceived information privacy risk. We confirm this negative relationship in the SNS context so that we can compare the relationship with the territory trusting beliefs / territory privacy risk beliefs relationship.

H5: On a social networking site, individuals' information trusting beliefs will negatively influence their information privacy risk beliefs.

As the individual and confidant group are co-owners of the virtual territory, they have established the privacy practices for this territory (i.e., drawn the boundary around the territory). According to CPM theory, when boundary synchronicity is expected, the individual trusts that a confidant will not deliberately or inadvertently allow access to the collectively held virtual territory to unauthorized others. An individual with high territory trusting beliefs generally believes that SNS confidant group members are dependable and trustworthy with respect to access to and interaction within the individual's private virtual territory. For example, John (virtual territory owner) believes Zack (a confidant) will not give access to John's online album to his spouse, because John and Zack have agreed that the album (i.e., private virtual territory) should never be shared. John trusts that Zack will not violate their agreement, so he believes the album is secure.

Theoretical frameworks of trust behavior have suggested that the tendency to trust others involves the trustor's willingness to become vulnerable (Moorman, Zaltman, & Deshpande, 1992). The willingness to increase one's vulnerability can be interpreted as one's propensity to take risks (Sitkin & Pablo, 1992). An individual with a high risk-taking propensity will weigh positive outcomes as more significant and will tend to underestimate the probability of loss (i.e., perceive lower risks) (Brockhaus, 1980; Sitkin & Pablo, 1992; Vlek & Stallen, 1980). Also, high trusting beliefs reduces the individual's perception of the likelihood of others engaging in opportunistic behavior (Jarvenpaa, Tractinsky, & Vitale, 2000; Mayer et al., 1995). Therefore, we argue that individuals who believe that SNS confidant group members will treat their private virtual territory in a trustworthy manner (e.g., not allow access to unknown or unauthorized others) are more likely to perceive lower privacy risks regarding their private virtual territory. Stated another way, the higher an individual's territory trusting beliefs, the lower the individual's perceived territory privacy risk.

H6: On a social networking site, individuals' territory trusting beliefs will negatively influence their territory privacy risk beliefs.

2.3.4 Territory Privacy Risk Beliefs and Information Privacy Risk Beliefs

On SNSs, individuals place private information and objects into their private virtual territory (e.g., upload pictures to their Facebook wall, posts about their New Year's resolution). When an agreement with a confidant about how to manage a private virtual territory is violated, the individual may feel that ownership of the territory, as well as the objects (uploaded picture) therein are at risk. Much like in the physical world, if your home is at risk of invasion, then the contents of your home are also at risk. In their study of Facebook, van Schaik, Jansen, Onibokun, Camp, & Kusev (2018) found that over 50% of the participants reported having taken precautions against potential violations of privacy through social network privacy settings. Therefore, we assert that the perceived level of security of the private virtual territory influences the perceived level security of the private information that resides within the territory. If individuals believe their territory is at risk, then they will likely perceive that the information housed within the territory is also at risk.

H7: On a social networking site, individuals' territory privacy risk beliefs will positively influence their information privacy risk beliefs.

2.3.5 Trusting Beliefs and Privacy Management Behavior

Recall that privacy management is the behavior engaged in by individuals to manage their information and territory on SNSs, and that private disclosure and territory coordination are two types of privacy management behaviors. *Private disclosure* refers to individuals' voluntary and intentional behavior of revealing private information to his/her SNS confidant group members (Derlega et al., 1993; Petronio, 2002; Posey et al., 2010), and *territory coordination* refers to individuals' voluntary and intentional behavior to manage the level of access to and interaction within their virtual territories.

Research has found that an individual with high information trusting beliefs is more likely to disclose private information in an e-commerce context (Malhotra et al., 2004; Van Slyke et al., 2006). Interestingly, in an SNS context Lo (2010) found a positive relationship between trust of the SNS and information disclosure, whereas McKnight, Lankton, and Tripp (2011) found a negative relationship between trust of the SNS and information disclosure. As the purpose of an SNS is to build social relationships, in this research, we view trust from the perspective that SNS members trust confidant group members not to misuse the information that has been shared. We therefore propose that individuals with higher trust in their SNS confidant group members will be willing to disclose more private information.

H8: On a social networking site, individuals' information trusting beliefs will positively influence their disclosure of private information.

Based on the theory of territoriality, Brown, Crossley, and Robinson (2014) found that a high trust work environment reduced the territorial behavior of individuals. As stated previously, an individual with high territory trusting beliefs believes SNS confidant group members will behave in a dependable manner regarding the individual's private virtual territory. Thus, the individual may reduce his/her territorial behavior. For example, if Selena trusts her SNS confidant group members in terms of how they will access and interact within her virtual territory, she might not feel the need to prevent them from tagging others. Also, from a CPM theory perspective, an individual with high territory trusting beliefs expects boundary synchronicity, and the individual, therefore, will not exert territory coordination behavior to change the current status. We therefore propose, similarly, that an individual with higher trust in SNS confidant group members regarding how they will access and behave in his or her private virtual territory will be less inclined to express territorial behaviors, such as highly coordinating the boundary of that territory (lower territory coordination).

H9: On a social networking site, individuals' territory trusting beliefs will negatively influence their territory coordination.

2.3.6 Privacy Risk Beliefs and Privacy Management Behavior

Research has found that an individual who perceives a high likelihood of loss due to sharing private information (i.e., high information privacy risk beliefs) is less likely to disclose private information in an e-commerce setting (Malhotra et al., 2004). Within an SNS setting this relationship has been supported (Hajli & Lin, 2016; Posey et al., 2010) and not supported (Cheung et al., 2015). We test this relationship in the SNS context so that we can compare the relationship with the territory privacy risk beliefs—territory coordination relationship.

H10: On a social networking site, individuals' perceived information privacy risk beliefs will negatively influence their disclosure of private information.

Research has found that individuals who perceive risks to their information are strongly disposed to engage in privacy management behaviors (Park, Campbell, & Kwak, 2012). In addition to the behavior of disclosing (or not disclosing) private information, an individual's privacy management behavior on an SNS includes managing the private virtual territory that contains the information. Recall that territory coordination involves individual behavior to regulate the level of access to and interaction within a private virtual territory. By engaging in territory coordination individuals protect their private virtual territory from infringement by others (Brown et al., 2005). Therefore, on SNSs, individuals engage in territory coordination behavior to prevent their private virtual territory from unwanted intrusion. If individuals perceive that the information has a high potential for loss, they might increase the protection of the information by building a stronger boundary around the private virtual territory. For example, in an offline context if an individual decides to keep valuable financial records at home, he or she might consider installing a security system to increase the protection of this information. In an online context, that individual might control how confidants can act/interact within his or her private virtual territory by eliminating their ability to tag posts. In this research we assert that the higher the perceived information privacy risk (i.e., high privacy risk beliefs), the higher the likelihood individuals will establish a more inaccessible boundary around their private virtual territory (high territory coordination).

H11: On a social networking site, individuals' perceived information privacy risk beliefs will positively influence their territory coordination.

The theory of territoriality proposed by Brown et al. (2005) suggests that individual territory privacy management behavior is influenced by territory privacy risk beliefs (Altman, 1975; Brown et al., 2005). The theory of territoriality states that when individuals perceive a greater likelihood of infringement into their territory, they will take action to prevent others from invading the territory (i.e., anticipatory defenses; Brown et al., 2005; Dyson-Hudson & Smith, 1978; Edney, 1975, 1976). From CPM theory, regarding a virtual private territory, high privacy risk evaluation means that the individual feels vulnerable when granting access to the private virtual territory. Individuals who perceive a high potential for loss due to sharing their private virtual territory with a confidant

group (i.e., territory privacy risk beliefs) are likely to increase their management of the private virtual territory (i.e., territory coordination). On SNSs, individuals who have high territory privacy risk beliefs may anticipate a high likelihood of loss resulting from allowing access to their private virtual territory, and thus may more tightly control their private virtual territory. For example, if Sandra perceives a high potential for "invasion" of her private virtual territory by unknown others, she may take preventative action such as adding a mechanism to review new members to ensure that only certain confidants have access to her territory.

H12: On a social networking site, individuals' perceived territory privacy risk beliefs will positively influence their territory coordination.

2.3.7 Information Sensitivity and Privacy Management Behavior

Sensitive information is information that is important to the individual and might result in negative consequences if revealed to certain individuals (Phelps, Nowak, & Ferrell, 2000). Previous research has found that more sensitive information negatively affects the disclosure of information online in an e-commerce context (e.g., Malhotra et al., 2004; McKnight et al., 2011; Yang & Wang, 2009), and an SNS context (James, Wallace, Warkentin, Kim, & Collignon, 2017). We confirm this finding to establish that in an SNS context individuals will be less likely to share information that they feel is sensitive so that we can compare the relationship with the information sensitivity / territory coordination relationship.

H13: On a social networking site, the level of information sensitivity will negatively influence individuals' private disclosure.

The more valuable something is, the more we protect it. We see this in everyday life, with car alarms, home security systems, and computer passwords. Sensitive information is important and valuable to the individual. The results of its misuse can be significant (e.g., embarrassing, financially costly), and thus, sensitive information is worthy of being protected. Within an SNS context, to protect sensitive information from being misused individuals may regulate the level of access to and interaction within their virtual territories. In essence, individuals may more tightly control the virtual territory boundary by controlling which SNS confidant group members may view, tag, and/or discuss what information. We further argue that the more sensitive the information, the more individuals may coordinate with their SNS confidant group members (i.e., more tightly control access) regarding their virtual territories.

H14: On a social networking site, the level of information sensitivity will positively influence individuals' territory coordination.

3 Research Method

We conducted two empirical studies to explore our model. Study 1 empirically validated the conceptual distinction between information and territory related to privacy on an SNS. Study 2 tested the research model and hypotheses.

3.1 Study 1

The objective of Study 1 was to develop a new scale to measure the concept of a virtual territory and empirically examine it as distinct from the concept of an SNS and the information contained on the SNS. To identify various forms of virtual territories, we first reviewed the relevant literature regarding territories (Altman, 1975; Brown et al., 2005; Brown & Robinson, 2011) and online social networks (Lewis, Kaufman, & Christakis, 2008; Steinfield, Ellison, & Lampe, 2008), and then conducted a qualitative inquiry through individual interviews with 20 undergraduate students from a southeastern university in the United States participating in a basic computer competency class (12 males and 8 females) who reported SNS use within the last 30 days. The interviews were conducted to determine the applicability of the focal constructs to the study context. Specifically, we wanted to identify whether individuals make a conceptual distinction between information and territory within the context of SNSs. The interviewees had a variety of majors (e.g., psychology, business, political science, etc.) with 50% of the participants from business disciplines. Interviewees highlighted the distinction between the information they place in their virtual territories and the territories themselves. We asked participants how they might define/describe the term virtual territory, as well as whether there are differences between information and territory and between information privacy and territory privacy. For example, when asked, "What is a virtual territory?" participants made statements like

> *Your Facebook wall could be considered your virtual territory, because it's your area. The use of the word wall is kind of a decent idea. Kind of like that commercial*[2] *that came out where that older woman she says you're not my friend anymore and pulls that*

[2] Esurance commercial "That's Not How This Works!" (https://www.youtube.com/watch?v=Aq_1l316ow8).

person's picture off the wall. The idea of a virtual wall is a [virtual] territory. (Zack)

Like your own personal, your own space or confinement within the internet. For instance, Instagram, my Instagram, that's like my virtual territory. (Brian)

My profile is my virtual territory because it's under my control. Like I have it set up so if someone tags me in a picture it doesn't automatically go to my page, I have to approve it. (Cassandra)

As a result of the literature review and qualitative data, a conceptual definition and pool of items were created to reflect a virtual territory within but distinct from SNSs. The pool included 4 items describing SNSs, 2 items describing private information, and 8 items describing a virtual territory. A structured questionnaire was developed based on the pool of items. All items used a seven-point Likert-type scale ranging from "strongly disagree" (1) to "strongly agree" (7). Appendix A, Table A1 contains the construct definitions and measurement items for each construct. The survey was administered to students in an introductory computer class at a large southeastern US university who reported SNS use within the previous 30 days. For this study we collected 156 completed questionnaires (five responses were dropped due to incomplete data). Men (49%) and women (51%) were almost equally represented and 93% of the participants were between 18 and 25 years of age. Participants reported an average of 5.4 years of SNS use.

To further explore the potential distinction between perceptions of privacy regarding online territories and online information, we performed an exploratory factor analysis using SPSS 21 on the items. Each of the items loaded higher than 0.70 on the appropriate factor and at the same time loaded less than 0.40 on other factors with the exception of one item (VT8). This item was removed from further analysis due to the low loading. Table 1 shows the result of the factor analysis and scale reliability.

We also performed a paired-samples t-test to compare the means of the variables (virtual territory mean = 5.23, social network mean = 5.57, private information mean = 5.95) and found a statistically significant difference (virtual territory and social network $t = 2.89$, $df = 155$, $p = 0.004$; virtual territory and private information $t = 7.11$, $df = 155$, $p = 0.000$; and social network and private information $t = 3.36$, $df = 155$, $p = 0.001$). The results indicate that the participants discriminated between the concepts of information, online social networks, and virtual territories. Given this finding, we proceeded to further explore the research question (*What factors influence how individuals manage their information privacy and territory privacy in SNSs?*) via an empirical test of the research model in Figure 2.

Table 1. Study 1 Factor Analysis and Scale Reliability

Item	Factor 1	Factor 2	Factor 3	Cronbach's alpha
INFO1	0.87			0.74
INFO2	0.89			
SNT1		0.85		0.90
SNT2		0.92		
SNT3		0.91		
SNT4		0.83		
VT1			0.83	0.92
VT2			0.85	
VT3			0.82	
VT4			0.85	
VT5			0.81	
VT6			0.82	
VT7			0.74	

3.2 Study 2

Since this research emphasizes explaining variance and developing causal relationships, we used a field study methodology and performed statistical analysis using structural equation modeling.

3.2.1 Measure Development

For the constructs that had been previously developed and had valid and reliable measures (e.g., information privacy concerns, information trusting beliefs, and information privacy risk beliefs) (Malhotra et al. 2004), we adapted the measure to the SNS context. If no measure was available, we used the procedures suggested by Schwab (2005) to develop the measure. First, we clearly defined the construct based on the theory that informs the construct. Second, we developed the measures to be consistent with the construct definition. Third, to ensure the measure's content validity, we reviewed each item to make sure the items accurately captured the construct definition. Fourth, to ensure face validity, we invited three SNS members to review the wording of the items and the scales, and we reworded the items until consensus was reached. Fifth, we conducted a pilot test and then refined or added items based on the pilot test results. Appendix A, Table A2 contains the construct definitions, measurement items and sources for each construct.

There are three dimensions to information privacy concerns: collection, control, and awareness (Malhotra et al., 2004). We modified items in the collection dimension of information privacy concerns to reflect the nature of the information flow[3] on SNSs. The measure reflects the degree to which an individual is concerned about the private information divulged to confidants and was developed based on similar measures in the literature (Jiang et al., 2013; Wheeless & Grotz, 1976).

To measure territory privacy concerns, territory trusting beliefs, and territory privacy risk beliefs, we developed measures based on Altman's (1975) territory privacy theory, Malhotra et al.'s (2004) theory of internet privacy, Petronio's (2002) CPM theory, and our results from Study 1, using the procedure detailed previously. In Malhotra et al.'s (2004) theory of internet privacy, social contract theory is used to draw the three dimensions of information privacy concerns. Because territory privacy concerns, like information privacy concerns, captures how an individual perceives fairness in an exchange, we used social contract theory and Altman's notion of territory to develop the three dimensions of territory privacy concerns: access, control, and awareness. An individual perceives territory privacy practices to be fair (low territory privacy concerns) when confidants' "access" to the private virtual territory is perceived to be fair, when the individual has "control" over the private virtual territory, and when the individual is "aware" of the confidants' behavior intention within the private virtual territory.

In CPM theory, there are three types of territory coordination: linkage, permeability, and ownership (Petronio, 2002). Linkage coordination (five items) refers to managing who can access an individual's private virtual territory. For example, an individual may write a post and limit the "linkages" by inviting only family members to view and reply. Permeability coordination (five items) refers to managing how difficult a private virtual territory is for others to access. An individual can differentiate multiple virtual territories with different levels of accessibility. For example, through a password or other mechanisms, one may make a specific online photo album more difficult to access (less permeable) than other albums. Ownership coordination (seven items) refers to managing who has rights and privileges to control an individual's private virtual territory. Allowing others to have ownership means allowing them to have control over an area of an individual's private virtual territory. For example, individuals can determine whether or not to grant their confidants the right to invite (tag) other friends to see their online photos.

Among the measurement items for territory coordination, some items were adapted from Child et al. (2009), some were newly added, and some were dropped. There are two primary reasons for this approach. First, Child et al.'s (2009) measure reflects privacy management practices regarding the management of private information in a blog environment. Our study differentiates the behavior for managing private information (i.e., private disclosure) and the behavior for managing private virtual territories (i.e., territory coordination). Therefore, some items from Child et al. (2009), such as "I have limited the personal information posted on my blog", were dropped because they capture private disclosure rather than territory coordination. Other items, such as "I place my SNS members in different groups and share my virtual territory with different groups", were added because they reflect individual behavior to manage private virtual territories (i.e., territory coordination). A second reason for the modification is because Child et al.'s (2009) measure was developed specifically for a blogging context, and as such the wording of some items was adapted to the SNS context.

[3] The original items in the *collection* dimension reflects the fact that the organization collects private information from transactions in the B2C context. However, in SNSs the individual shares private information to confidants.

All items used a seven-point Likert-type scale ranging from "strongly disagree" (1) to "strongly agree" (7). Following the decision rules described by Jarvis, MacKenzie, and Podsakoff (2003) and MacKenzie et al. (2005), and consistent with previous research on online privacy management (Child et al., 2009; Malhotra et al., 2004), information trusting beliefs, territory trusting beliefs, information privacy risk beliefs, and territory privacy risk beliefs were modeled as first-order reflective constructs. We modeled information privacy concerns and territory privacy concerns as reflective first-order and reflective second-order constructs (Child et al., 2009; Malhotra et al., 2004).

A second-order latent construct has formative dimensions when: (1) all the dimensions together define the concept domain of the second-order latent construct, (2) changes in one dimension result in changes in the second-order latent construct, and (3) each dimension uniquely captures a concept domain of the second-order latent construct (Jarvis et al., 2003; MacKenzie et al., 2005). We modeled territory coordination as a reflective first-order and formative second-order construct as it met these criteria.

We included several factors as control variables, because while they are not included in the research model, it has been suggested in the literature that they have an influence on privacy-related attitudes and behaviors (Malhotra et al., 2004; Posey et al., 2010; Xu, Teo, Tan, & Agarwal, 2009). These variables include gender, native language, education, SNS[4], tenure in the SNS, number of connections, and weekly hours spent in SNS (see Appendix A for a description of these measures). In addition, considering some SNSs provide more tools for territory coordination than others, we included technological features as a control variable.

3.2.2 Data Collection

We designed the questionnaire with two different scenarios (i.e., low versus high information sensitivity) to investigate how individuals' privacy management behavior differs on the basis of the type of information shared. In scenario A (less sensitive information), participants were asked by their friends to share (on their SNS) photos taken at 2:00 p.m. in a local park, where they are sitting around a picnic table, eating bar-b-que and drinking tea. In scenario B (more sensitive information), participants were asked by their friends to share (on their SNS) photos taken at 2:00 a.m. in a local nightclub, where they are sitting around a table drinking (alcohol) and some were smoking/vaping. Participants were randomly assigned one of the two scenarios. Participants in both scenarios were presented with the same measurement items. This study collected data from undergraduate business students at a large southeastern university in the United States. The participants were "active" users,[5] since the individuals had visited an SNS within the last 30 days. We collected data using an online self-report survey instrument. Empirical evidence suggests that a separation of two to three weeks between the measurement of variables is an effective technique for reducing common method variance (Johnson, Rosen, & Djurdjevic, 2011, study 2). To minimize the possibility of common method variance, we collected the data in two stages (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003), with a minimum of 14 days between the two surveys.

In the first stage, participants responded to the questions measuring personal disposition factors and context-specific factors. When responding to questions regarding personal disposition factors such as information privacy concerns and territory privacy concerns, participants were asked to rate their level of agreement with the measurement items in general (not specific to any SNS or scenario). When answering questions regarding context-specific factors including information trusting beliefs, territory trusting beliefs, information privacy risk beliefs, and territory privacy risk beliefs, participants were asked to respond referencing a specific SNS. Participants were asked to think about the SNS that they used the most during the past 30 days. In the second stage, each participant was randomly assigned to one scenario (scenario A or scenario B) and responded to questions measuring private disclosure and territory coordination referencing the scenario provided.

4 Results

4.1 Sample Characteristics

The questionnaire was given to 265 participants. Overall, 246 participants completed the first-stage survey (a 93% response rate) and 195 participants took the second stage survey (79% of stage-one participants took the stage-two survey). As a result of data cleansing, 168 responses were valid for further analysis. See Table 2 for the demographics of the final sample.

[4] Our thanks to an anonymous reviewer for this suggestion.

[5] Facebook help page "What is a monthly active user?" (https://www.facebook.com/help/work/1101646006616660?helpref=uf_permalink).

Table 2. Demographics

Gender	Female = 52%	**Tenure in the SNS**	Less than 2 years = 9%
	Male = 48%		2-4 years = 22%
Age	18-25 = 97%		4-6 years = 36%
	26 or above = 3%		6 years or more = 33%
Native Language	English = 90%	**Number of Connections**	Less than 200 = 18%
	Spanish = 8%		201-400 = 23%
	Other = 2%		401-600 = 17%
Education	High School diploma = 45%		601-800 = 11%
	Associate's degree = 48%		801 or above = 30%
	Bachelor's degree = 7%	**Weekly Hours Spent in SNS**	Less than 2 hours = 14%
Social Networking Site	Facebook = 35%		3-6 hours = 30%
	Instagram = 29%		7-10 hours = 27%
	Snapchat = 21%		11-14hours = 14%
	Twitter = 8%		15-18 hours = 6%
	Other = 10%		19 or above = 9%

4.2 Measurement Model Assessment

The first stage of data analysis focused on the psychometric adequacy of the measurement model. The measures are reliable, as the composite reliabilities of all the constructs/dimensions ranged from 0.83 to 0.97 which are within the appropriate range (Bagozzi & Yi, 1988; Garver & Mentzer, 1999). See Table 3 for the composite reliability and Cronbach's alpha for each construct.

We conducted an exploratory factor analysis to obtain the preliminary evidence for convergent and discriminant validity (see Appendix A, Tables A3—A7 for factor loadings). For the second-order constructs, we grouped the measurement items under their respective second-order construct for the factor analysis, as demonstrated in Rai, Patnayakuni, and Seth's (2006) study. The results show that all of the item loadings were above 0.60 on the latent constructs/dimensions, and below 0.40 on the other constructs/dimensions (Hair, Anderson, Tatham, & Black, 1998). Also, the high eigenvalues (>1) of all latent constructs provides preliminary evidence for convergent validity.

We used the maximum likelihood estimation of structural equation modeling to confirm the psychometric adequacy of the measurement model. The measurement model fits the data well (χ^2 (df = 952, n= 168) = 1577.11, RMSEA = 0.06, CFI = 0.90, TLI = 0.89, SRMR = 0.08, PCFI = 0.82). The chi-square and the RMSEA indicate that our measurement model predicts the observed covariance matrix well. The CFI and TLI indicate that the measurement model fit the data well relative to the null model. The PCFI shows that the model is parsimonious and fits the data well.

We used two additional approaches to assess further evidence for convergent validity. First, measures show convergent validity when the standardized loadings are at least 0.70 or the average variance extracted (AVE) is greater than 0.50 (Fornell & Larcker, 1981). As observed in Table 3, both indicators suggest convergence in measurement (Bagozzi, 1981). Second, convergent validity is shown when items load significantly on their respective latent construct/dimension (Gefen & Straub, 2005). For second-order reflective constructs, measures show convergent validity when the path coefficient of a dimension loading onto its latent construct is significant (see Table 4). Thus, convergent validity is indicated for the measures.

We used three additional approaches to assess discriminant validity. First, measures showed discriminant validity when the square root of each AVE is larger than its correlation with any other latent constructs/dimensions (i.e., the Fornell-Larcker criterion; Chin, 1998a; Fornell & Larcker, 1981) (see Table 5). Second, the item-construct correlations (see Appendix B for the details) showed that the correlation of an item with its latent construct/dimension is greater than its correlations with other constructs/dimensions (Chin, 1998b; Gefen & Straub, 2005).

Table 3. AVEs, Construct Reliabilities, and Cronbach's Alpha

	AVE	Composite reliability	Cronbach's alpha
IPC_Collection	0.88	0.96	0.93
IPC_Control	0.68	0.87	0.77
IPC_Aware	0.90	0.97	0.96
TPC_Access	0.78	0.91	0.86
TPC_Control	0.62	0.83	0.69
TPC_Aware	0.83	0.94	0.90
ITB	0.82	0.95	0.94
TTB	0.78	0.93	0.91
IPRB	0.80	0.92	0.87
TPRB	0.86	0.95	0.92
PD	0.70	0.90	0.86
TC_Linkage	0.74	0.89	0.82
TC_Permeability	0.78	0.91	0.85
TC_Ownership	0.91	0.97	0.95
Technological Features	0.86	0.95	0.92

Table 4. Path Coefficients of Dimensions on Latent Constructs

Construct	Dimension	Type	Path coefficients		
			B	t-value	P
Information privacy concerns	Collection	Reflective first-order, reflective second-order	0.75	16.66	$p < 0.001$
	Control		0.77	14.97	$p < 0.001$
	Aware		0.88	43.58	$p < 0.001$
Territory privacy concerns	Access	Reflective first-order, reflective second-order	0.72	11.94	$p < 0.001$
	Control		0.76	16.61	$p < 0.001$
	Aware		0.83	33.96	$p < 0.001$
Territory coordination	Linkage	Reflective first-order, formative second-order	0.36	21.20	$p < 0.001$
	Ownership		0.38	20.10	$p < 0.001$
	Permeability		0.45	19.71	$p < 0.001$

Third, we conducted the fixed and freed method (Anderson & Gerbing, 1988; Jöreskog, 1971) to examine the discriminant validity for three pairs of constructs. The chi-square difference test suggested the measures for these constructs discriminate: information privacy concerns and territory privacy concerns ($\Delta\chi2= 18.50$, $p < 0.001$), information trusting beliefs and territory trusting beliefs ($\Delta\chi2= 7.80$, $p < 0.01$), and information privacy risk beliefs and territory privacy risk beliefs ($\Delta\chi2= 21.80$, $p < 0.001$).

Territory coordination is a construct with formative dimensions and reflective indicators (Type II constructs) (Jarvis et al., 2003; MacKenzie et al., 2005). For construct validity, we used item weights rather than item loadings as evidence of construct validity of formative constructs (Diamantopoulos & Winklhofer, 2001; Petter, Straub, & Rai, 2007). As the first-order dimensions had items as reflective indicators, significant item weights on their dimensions were not necessary. However, for the second-order dimensions, significant path coefficients indicated that the dimension explained a significant portion of variance in the latent construct. For evaluating the psychometric adequacy of formative constructs, convergent validity (Jarvis et al., 2003), composite reliabilities and Cronbach's alpha (Bollen, 1984; Chin, 1998b) were not required. The variance inflation factor (VIF) of the formative constructs ranged from 1.43 to 1.91 and were well below the 3.3 cut-off criterion (Diamantopoulos & Siguaw, 2006; Petter et al., 2007), suggesting the formative indicators were not highly correlated (Petter et al., 2007).

In addition to the two-phase data collection procedure, two statistical analyses suggested no evidence of the threat of common method bias. First, Harman's one-factor test showed the first factor accounted for only 21.9% of the total variance (a common methods bias problem presents if a single factor accounted for a large percentage of the variance). Second, we performed a marker variable test as suggested by Lindell and Whitney (2001). We used two variables that should have no relationship with the constructs of interest: (1) satisfaction with a car insurance company, and (2) the intention to take a long trip soon. The smallest correlation was 0.005, suggesting no correction was needed (based on Jayachandran, Sharma, Kaufman, & Raman, 2005; Richardson, Simmering, & Sturman, 2009). The results indicate that common method bias is unlikely to be a serious concern with this data.

4.3 Structural Model Assessment

We used partial least squares modeling (SmartPLS 2.0; Ringle, Wende, & Will, 2006) to evaluate the research model and test the hypotheses. To examine the hypotheses, we assessed the significance of the path coefficients through bootstrapping of 1500 subsamples (Chin, 1998a). Figure 3 graphically presents the results of the path analysis, and Table 6 presents the results of the hypothesis testing. The results indicate that the research model explained 24.1% of the variance in territory coordination, 18.2% of the variance in private disclosure, 40.2% of the variance in the information privacy risk beliefs, and 19.2% of the variance in the territory privacy risk beliefs.

Among the control variables, only the path coefficient from social networking sites to private disclosure ($\beta = 0.22$, $t = 2.30$, $p < 0.05$) was significant. This result suggests that participants that use different social networking sites may view private disclosure differently.

The findings show that individuals' territory privacy risk beliefs have no direct influence on territory coordination (H12, nonsignificant), and that with high territory privacy risk beliefs, individuals will perceive that the private information placed within the territory is at risk (H7). One plausible explanation for H12 being nonsignificant is that information privacy risk beliefs mediate the influence of territory privacy risk beliefs on territory coordination. Related to this, we performed a post hoc analysis to examine if/how territory coordination mediates the influence of information privacy risk beliefs on private disclosure (see Appendix C). We used two complementary approaches to examine the significance of the direct and indirect effects: the Sobel z-test (Sobel, 1982), and the significance test of the effect size ($f2$) following Cohen's (1988) and Chin, Marcolin, and Newsted's (2003) approach. Then, following Zhao, Lynch, and Chen's (2010) procedure, we examined the existence and type of mediation effects. Finally, we calculated the variance accounted for (VAF) (Helm, Eggert, & Garnefeld, 2010) to evaluate the magnitude of the mediation effects. The results confirm that information privacy risk beliefs fully mediate the influence of territory privacy risk beliefs on territory coordination (Sobel $Z=1.997$, $p < 0.05$, VAF = 25.2%). Appendix C presents all other mediation tests and procedures.

Another plausible explanation for H12 being nonsignificant might be that territory privacy risk beliefs have an influence on some but not all of the dimensions of territory coordination, which was obscured in the aggregation process. We performed a post hoc analysis to determine if territory risk beliefs directly influenced the dimensions of territory coordination. The results indicate that territory privacy risk beliefs did not significantly influence any of the individual territory coordination dimensions (linkage $\beta = 0.07$, p = nonsignificant; permeability $\beta = 0.13$, p = nonsignificant; ownership $\beta = 0.03$, p = nonsignificant), further confirming full mediation.

Table 5. Construct Correlations and AVEs

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1. Connect	1																					
2. Education	0.08	1																				
3. Gender	-0.13	0.03	1																			
4. Hours	0.14	0.06	-0.22	1																		
5. IPC: Aware	0.08	-0.03	-0.20	0.17	0.95																	
6. IPC: Collection	0.08	0.03	-0.13	0.01	0.43	0.94																
7. IPC: Control	-0.05	-0.04	-0.20	0.07	0.53	0.45	0.83															
8. IPRB	0.01	-0.06	-0.14	0.14	0.51	0.46	0.48	0.89														
9. ITB	0.02	0.00	0.00	0.15	0.00	0.04	0.01	-0.11	0.91													
10. Language	-0.01	0.10	0.12	0.02	-0.03	0.13	0.11	0.04	-0.03	1												
11. Linkage	-0.07	-0.03	-0.17	0.05	0.28	0.23	0.19	0.28	-0.05	0.00	0.86											
12. Ownership	-0.06	-0.01	-0.27	0.07	0.30	0.35	0.26	0.25	-0.03	0.04	0.48	0.95										
13. PD	0.03	-0.05	0.04	0.07	-0.24	-0.15	-0.20	-0.17	0.22	-0.13	-0.20	-0.22	0.84									
14. Permeability	-0.04	0.01	-0.11	0.07	0.31	0.28	0.18	0.24	-0.03	-0.04	0.65	0.52	-0.05	0.88								
15. SNS	-0.45	-0.10	-0.11	-0.01	-0.03	0.06	-0.11	-0.11	0.06	-0.06	-0.01	0.08	0.18	0.09	1							
16. Info Sentivity	0.09	0.06	-0.21	0.08	0.09	-0.01	-0.01	0.03	0.04	0.06	0.32	0.11	-0.23	0.22	-0.02	1						
17. TPC: Access	0.06	-0.06	-0.04	-0.03	0.27	0.27	0.42	0.32	0.00	-0.05	0.38	0.14	-0.18	0.16	-0.11	0.03	0.88					
18. TPC: Aware	0.21	-0.10	-0.09	0.24	0.53	0.39	0.32	0.30	0.12	0.03	0.24	0.25	-0.23	0.27	-0.01	0.14	0.33	0.91				
19. TPC: Control	0.00	-0.11	-0.17	0.21	0.45	0.62	0.32	0.28	0.21	0.10	0.24	0.38	-0.09	0.28	0.13	0.07	0.33	0.51	0.79			
20. TPRB	0.13	-0.11	0.11	0.14	0.17	0.08	0.31	0.31	0.04	0.04	0.18	0.11	0.01	0.19	-0.10	0.10	0.48	0.32	0.19	0.93		
21. TTB	0.05	-0.05	-0.04	0.20	0.19	0.27	0.10	0.23	0.38	0.03	0.09	0.12	0.02	0.11	0.07	-0.02	0.22	0.23	0.34	0.10	0.88	
22. Tech Feature	0.08	0.20	-0.22	0.09	0.02	0.04	-0.04	-0.10	-0.05	0.08	0.15	0.09	-0.05	0.07	0.05	0.03	-0.13	0.06	0.02	-0.14	-0.03	0.93
23. Tenure	0.44	0.19	-0.09	0.15	0.16	0.13	0.17	0.17	-0.01	0.12	-0.11	-0.07	-0.02	-0.06	-0.38	-0.05	0.10	0.06	0.03	0.06	0.06	0.05

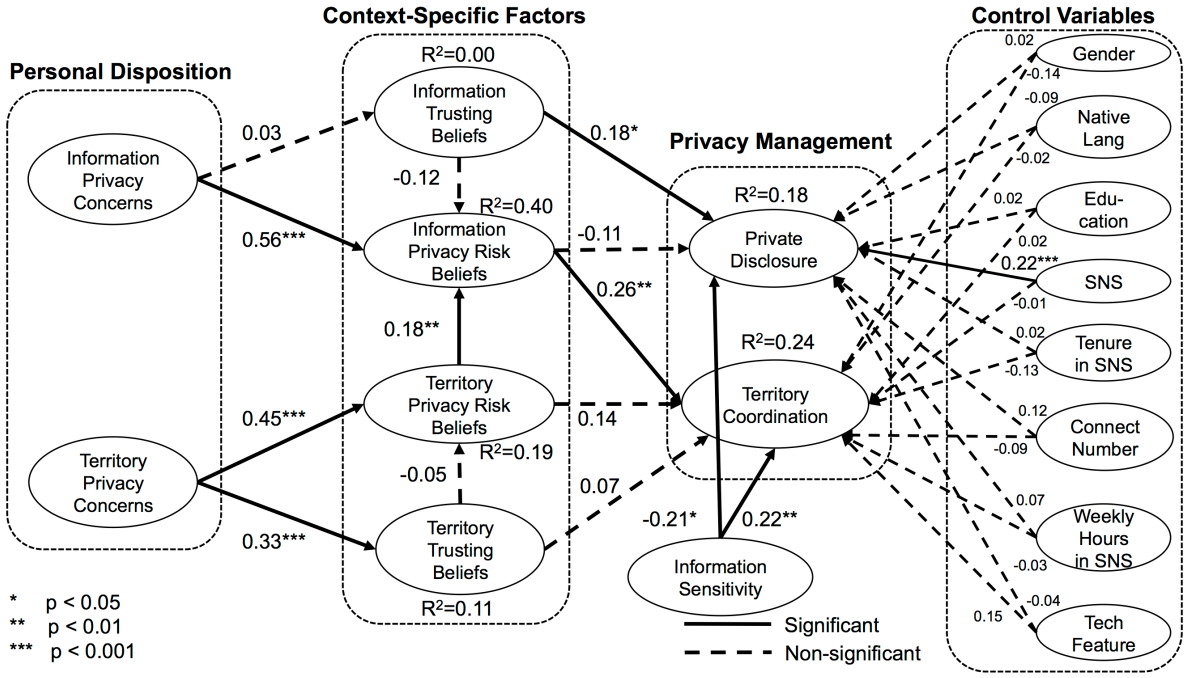

Figure 3. Results of Path Analysis

Table 6. Summary of Hypotheses Testing

Hypothesis	Relationships between constructs (direction of relationship)	Results	Support
H1	Information privacy concerns → Information trusting beliefs (-)	β = 0.03 t = 0.28	Not supported
H2	Territory privacy concerns → Territory trusting beliefs (-)	β = 0.33 t = 5.16	Not Supported*
H3	Information privacy concerns → Information privacy risk beliefs (+)	β = 0.56 t = 9.44	Supported (p < 0.001)
H4	Territory privacy concerns → Territory privacy risk beliefs (+)	β = 0.45 t = 6.62	Supported (p < 0.001)
H5	Information trusting beliefs → Information privacy risk beliefs (-)	β = -0.12 t = 1.56	Not supported
H6	Territory trusting beliefs → Territory privacy risk beliefs (-)	β = -0.05 t = 0.64	Not supported
H7	Territory privacy risk beliefs → Information privacy risk beliefs (+)	β = 0.18 t = 2.71	Supported (p < 0.01)
H8	Information trusting beliefs → Private disclosure (+)	β = 0.18 t = 2.43	Supported (p < 0.05)
H9	Territory trusting beliefs → Territory coordination (-)	β = 0.07 t = 0.93	Not supported
H10	Information privacy risk beliefs → Private disclosure (-)	β = -0.11 t = 1.20	Not supported
H11	Information privacy risk beliefs → Territory coordination (+)	β = 0.26 t = 3.04	Supported (p < 0.01)
H12	Territory privacy risk beliefs → Territory coordination (+)	β = 0.14 t = 1.82	Not supported
H13	Information sensitivity → Private disclosure (-)	β = -0.21 t = 2.45	Supported (p < 0.05)
H14	Information sensitivity → Territory coordination (+)	β = 0.22 t = 2.73	Supported (p < 0.01)

Note: * The relationship was significant, but in the opposite direction of the hypothesis.

5 Discussion

The underlying premise of this research is that in order to manage privacy on SNSs, individuals should determine what information to reveal (information privacy), *as well as* whom they allow access to and with whom they interact in their private virtual territories (territory privacy). Based on this premise we explored factors that influence how individuals manage their information privacy and territory privacy on SNSs.

Regarding the causal relationships in the information privacy theoretical framework (between information privacy concerns, information trusting beliefs, information privacy risk beliefs, and private disclosure), the findings of this study are mixed. Consistent with prior research (e.g., Hong & Thong, 2013; Malhotra et al., 2004), H3 and H8 were supported, but counter to previous findings (e.g., Malhotra et al., 2004; Shibchurn & Yan, 2015) H1, H5 and H10 were not supported. These findings indicate that in an SNS context trust may not play the same role in information disclosure as in an e-commerce context; and that the inclusion of the territory privacy construct may influence the relationships within the private disclosure framework. The findings also suggest that in the theoretical framework of territory privacy, territory privacy concerns and territory privacy risk beliefs have a significant relationship (H4).

When viewed holistically, the model tells a particularly interesting story. The findings indicate that both information and territory privacy concerns are key distal antecedents of privacy management behavior within an SNS context as they strongly and significantly influence the respective risk beliefs. In addition, both information and territory risk beliefs play significant roles in determining privacy management behavior, and specifically territory coordination.

Also, the relationship between information privacy risk beliefs and territory coordination was supported, but not the relationship between territory privacy risk beliefs and territory coordination. A post hoc analysis indicated that information privacy risk beliefs fully mediated the impact of territory privacy risk beliefs on territory coordination. Thus, the perception of potential loss due to allowing SNS members access to one's private virtual territory alone is not sufficient motivation for individuals to increase their territory coordination unless they perceive that the information within the private virtual territory is also at risk.

Finally, as hypothesized, the sensitivity of the information significantly influenced the level of private disclosure (-) and territory coordination (+). This finding is consistent with previous research in both an e-commerce setting (e.g., Mothersbaugh, Foxx, Beatty, & Wang, 2012) and an SNS setting (e.g., Cheung et al., 2015; Hajli & Lin, 2016). Given this consistent finding, we speculate that an individual may disclose less in public virtual territories and more in private virtual territories because the individual can better control the level of access to and interaction within the private virtual territory.

5.1 Implications

The findings suggest two main implications for theory. First, the findings reveal that to have a comprehensive understanding of online privacy issues concerning SNSs, researchers should consider both information privacy and territory privacy. Previous privacy-related IS research has examined the antecedents of information privacy (e.g., Dinev & Hart, 2004; Malhotra et al., 2004), and hinted at multiple dimensions of privacy (e.g., Malhotra et al., 2004; Smith, Milburg, & Burke, 1996) but has not systematically investigated different types of privacy (e.g., information and territory). The findings from this study tell us that the antecedents and outcomes of information privacy and territory privacy are different. In other words, the level of territory privacy cannot simply be inferred by the assessment of information privacy, and vice versa. The findings show that the level of information privacy risk beliefs is determined not only by information privacy concerns, but also by territory privacy risk beliefs. Given that information privacy risk beliefs fully mediate the effect of territory privacy risk beliefs on territory coordination, researchers should consider how the perceived risks regarding the virtual territory influence the perceived risks of the information and territory boundary coordination efforts. While there can be different types of privacy, these findings suggest that the level of one type of privacy risk cannot be summarily inferred from another. Future research should explore the extent of the differences in antecedents of the two types of privacy risk beliefs in multiple SNS contexts. Future research on privacy on SNSs might study how information privacy risk beliefs and territory privacy risk beliefs may influence SNS participation. For example, would information privacy risk beliefs and territory privacy risk beliefs influence SNS participation in the same way?

Second, this study suggests that in the SNS context, territory coordination is a more evident indicator of individuals' privacy management behavior than is private disclosure. Prior research of privacy mainly adopted private disclosure (or similar concepts) as the behavioral outcome and used it as the indicator of individual privacy management behavior. However, our study suggests that in the SNS context, territory coordination is a significant behavioral outcome of information privacy risk beliefs, whereas private disclosure is not. These results imply that individuals on SNSs may rely more on territory coordination as the

privacy management behavior than on private disclosure. Future research should revisit how individuals in a variety of contexts manage their privacy and how territory privacy management behavior and information privacy management behavior influence participation.

In addition to theoretical contributions, there are also implications for practice. This study found that addressing individuals' territory privacy concerns may help SNS platform organizations mitigate individual evaluations of territory privacy risk (and ultimately information privacy risk). As the findings indicate, if an individual has high territory privacy concerns, the individual will also have high territory privacy risk beliefs. To mitigate access concerns, SNS platform organizations could implement a variety of mechanisms to encourage individuals to share their virtual territories. For example, Facebook provides mobile applications to encourage users to share photos (i.e., private information) and interact with others in the photo comment area (i.e., private virtual territory). To mitigate control concerns, organizations could provide (or improve) tools for individuals to manage the accessibility of the private virtual territory to SNS members. To mitigate awareness concerns, organizations could use tools such as online help to guide individuals to the default territory privacy practices settings of SNS members and different territory privacy practices that are available to SNS members. These settings may help SNS platform providers decrease the perceived risks to users' private virtual territories, (and ultimately of sharing private information), potentially increasing participation and satisfaction with SNSs and potentially increasing revenue.

The second implication for practice, especially for organizations that host social networking platforms (e.g., Twitter, Facebook), is about how to facilitate territory coordination and encourage individuals to share private information. For these organizations, the business model is simple—the more users, the more revenue (e.g., Facebook made an average of $7.37 in revenue per user in 2018).[6] Research suggests that every additional connection (direct or indirect) within one's online social network raises a user's barrier to leave the network (Algesheimer & Von Wangenheim, 2006; Xu, Lu, Goh, Jiang, & Zhu, 2009). Network members' activity is highly relevant for advertising effectiveness, member loyalty, and a member's willingness to pay for services in the online social network (Cheung & Lee, 2010; Ganley & Lampe, 2009; Krasnova, Hildebrand, & Günther, 2009; Oestreicher-Singer & Zalmanson, 2009; Xu, Zhang, Xue, & Yeo, 2008). Therefore, organizations that host social networking platforms might use the findings from this study to increase the number of users and increase user retention by encouraging users to manage their privacy more effectively and provide tools and/or techniques to support individuals in effectively protecting their private virtual territory.

The third implication for practice indicates that the three types of territory coordination behavior (linkage, permeability, ownership) also have implications for organizations that host social networking platforms. A survey of SNS users has observed the trend that individuals are becoming more active in managing their virtual territories on SNSs (Madden, 2012). The researcher found that the majority of individuals on SNSs (78%) set their profile to private or partially private so that only friends (or friends of friends) can see it. Moreover, among the individuals who already restrict the level of access to their SNS profile, a notable portion of them manage their friends in multiple groups so as to limit what specific individuals can and cannot see.

Our conceptualization of territory coordination suggests three types of tools and/or techniques that an SNS platform organization could provide for individuals to facilitate the management of private virtual territories. For example, to support linkage coordination, some SNSs allow individuals to determine to whom a message box or a photo album (private virtual territory) is accessible. SNS platforms could add finer-grained selection tools so that SNS members could control exactly who can and cannot access subsets of their virtual territories. To support permeability coordination, SNS platform organizations could provide finer-grained tools for individuals to configure the accessibility of the private virtual territory, so that individuals can manage their private virtual territories with different boundaries, such as a nonaccess virtual territory boundary and several collective virtual territory boundaries. For example, a simulation tool that enables individuals to see what their friends may see, or a visualization tool such as a dashboard of virtual territory accessibility, might help individuals manage boundary permeability. To support ownership coordination, some SNSs allow individuals to delete unwanted comments from SNS members. Also, SNSs could introduce a badge mechanism through which individuals can authorize administrative privileges to friends using various badges. By providing these tools, SNS platform organizations might facilitate greater levels of comfort among individuals sharing their virtual territories with others.

[6] According to https://www.statista.com/statistics/251328/facebooks-average-revenue-per-user-by-region/.

5.2 Limitations and Future Research

Care must be taken when generalizing the findings beyond the boundary of the study context (SNS). Given the fact that there are several types of virtual communities, the findings of this study should be generalized outside the SNS context with caution. Individuals participating in other types of virtual communities may have privacy perceptions and privacy management behavior patterns that are different from those using SNSs. Future research could examine whether the findings in this study are generalizable to additional SNS platforms and virtual communities (e.g., virtual worlds, StackOverflow, or SourceForge).

In addition, this research assumed that virtual territories are nested within virtual communities (i.e., we asked survey respondents to answer the survey questions with one focal SNS in mind). An alternative view is that a private virtual territory is a combination of smaller territories scattered across various virtual communities, especially given the fact that many of these communities are technologically intertwined. Thus, our assumption may be a limitation of the study. Future research could focus on detailing the perceived relationship between virtual territories and virtual communities. Related to this issue is the potential temporal aspect of privacy management on SNSs. In answer to the question, does one form of privacy precede another (i.e., does territory privacy occur before or after information privacy)? We see examples of territory privacy occurring first (e.g., establish territory boundaries when creating a social network profile), information privacy occurring first (e.g., do not disclose private information in an open SNS), and both occurring simultaneously (e.g., establish a new virtual territory on the SNS for a specific confidant group in which limited private information is shared). Future research could explore the nature of the relationship between these two forms of online privacy (including any temporal relationship).

A characteristic of the sample to consider is the native language of the participants. Although efforts were made to include a range of participants representing different cultural groups, 90% of the participants were native English speakers. Therefore, the applicability of the findings to other cultural groups may be limited. As such, we cannot clearly derive from this study whether and how people from different cultural backgrounds may manage their territory privacy on SNSs. Future research could expand this study to include non-US-based samples. Finally, we took steps to control for common method variance in the research design and in the data analysis to ensure that common method bias was not a concern in the data. However, a longitudinal research design could further validate the casual relationships found here.

6 Conclusion

This study proposed several aspects of SNSs that may influence an individuals' evaluation of privacy risks, which in turn influences individual privacy management behavior (including private disclosure and territory coordination). Theoretically, this study demonstrates that a more complete conceptualization of privacy in SNS should consider both information privacy *and* territory privacy, and that private disclosure and territory coordination are complementary privacy management behaviors. From a practical standpoint, this study provides guidance to SNS platform organizations on potential ways to encourage users to share private information as a mechanism to increase their community population and potentially increase revenue.

References

Al-Nowaiser, M. (1987). The conceptual role of the built environment on environmental experience in central Saudi Arabia. *Journal of Architectural and Planning Research, 4*(3), 181-198.

Aldosemani, T. I., Shepherd, C. E., Gashim, I., & Dousay, T. (2016). Developing third places to foster sense of community in online instruction. *British Journal of Educational Technology, 47*(6), 1020-1031.

Algesheimer, R., & Von Wangenheim, F. (2006). A network based approach to customer equity management. *Journal of Relationship Marketing, 5*(1), 39-57.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423.

Andrews, E. L. (2002, April 20). German media report potential ties between Tunisian blast and Al Qaeda, *New York Times*. Retrieved from http://www.nytimes.com/2002/04/20/international/europe/german-media-report-potential-ties-between-tunisian.html

Bagozzi, R. P. (1981). Evaluating structural equation models with unobservable variables and measurement error: A comment. *Journal of Marketing Research, 18*(3), 375-381.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74-94.

Ball, K., Daniel, E. M., & Stride, C. (2012). Dimensions of employee privacy: An empirical study. *Information Technology & People, 25*(4), 376-394.

Basulto, D. (2012, May 3). Is social profiling discrimination? *The Washington Post*. Retrieved from https://www.washingtonpost.com/blogs/innovations/post/is-social-profiling-the-new-racism/2012/05/03/gIQAXQQDzT_blog.html?utm_term=.c09ab28b82b9

Bateman, P. J., Pike, J. C., & Butler, B. S. (2011). To disclose or not: Publicness in social networking sites. *Information Technology & People, 24*(1), 78-100.

Beldad, A. (2016). Sealing one's online wall off from outsiders: Determinants of the use of Facebook's privacy settings among young Dutch users. *International Journal of Technology and Human Interaction, 12*(1), 21-34.

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People, 28*(3), 426-441.

Bollen, K. (1984). Multiple indicators: Internal consistency of no necessary relationships? *Quality and Quantity, 18*, 377-385.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230.

Brockhaus, R. H. (1980). Risk-taking propensity of entrepreneurs. *Academy of Management Journal, 23*(3), 509-520.

Brown, G. (2009). Claiming a corner at work: Measuring employee territoriality in their workspaces. *Journal of Environmental Psychology, 29*(1), 44-52.

Brown, G., Crossley, C., & Robinson, S. L. (2014). Psychological ownership, territorial behavior, and being perceived as a team contributor: The critical role of trust in the work environment. *Personnel Psychology, 67*(2), 463-485.

Brown, G., Lawrence, T. B., & Robinson, S. L. (2005). Territoriality in organizations. *Academy of Management Review, 30*(3), 577-594.

Brown, G., & Robinson, S. L. (2011). Reactions to territorial infringement. *Organization Science, 22*(1), 210-224.

Burgoon, J. K., Parrott, R., Poire, B. A. L., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships, 6*(3).

Cater, J. G. (1997). Social construction of the serial killer. *Gazette, 59*(1), 2-21.

Chakraborty, R., Vishik, C., & Rao, H. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems 55*(4), 948-956.

Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems, 115*(1), 88-106.

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior, 69*(C), 207-217.

Chen, R. (2013). Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems, 55*(3), 661-668.

Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: The case of Facebook users. *European Journal of Information Systems, 24*(1), 93-106.

Chen, X., Lu, T., Guo, L., & Lin, X. (2013). Research on influence factors and behavioral willing of user privacy concern on social network platform. *Information Technology Journal, 12*(16), 3759-3763.

Cheung, C., & Lee, M. K. O. (2010). A theoretical model of intentional social action in online social networks. *Decision Support Systems, 49*(1), 24-30.

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Research, 25*(2), 279-299.

Child, J. T., & Agyeman-Budu, E. A. (2010). Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior, 26*(5), 957-963.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology, 60*(10), 2079-2094.

Child, J. T., Petronio, S., Agyeman-Budu, E. A., & Westermann, D. A. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior, 27*(5), 2017-2027.

Chin, W. W. (1998a). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), 7-16.

Chin, W. W. (1998b). The partial least square approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Mahwah, New Jersey: Erlbaum.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research, 14*(2), 189-217.

Cirit, F. O., Nikravesh, M., & Alptekin, S. E. (2005). Consumer profiling using fuzzy query and social network techniques. In M. Nikravesh & L. A. Zadeh (Eds.), *Soft computing for information processing and analysis* (pp. 285-294). Berlin: Springer.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Hillside, NJ: Erlbaum.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115.

De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior, 35*, 444-454.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-disclosure*. Newbury Park, CA: SAGE.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management, 17*(4), 263-282.

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formation indicators: An alternative to scale development. *Journal of Marketing Research, 38*, 259-277.

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. *European Journal of Information Systems, 15*(4), 389-402.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents measurement validity and

a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

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

Ducheneaut, N., Moore, R. J., & Nickell, E. (2007). Virtual third places: A case study of sociability in massively multiplayer games. *Computer Supported Cooperative Work, 16*(1-12), 129-166.

Dyson-Hudson, R., & Smith, E. A. (1978). Human territoriality: An ecological reassessment. *American Anthropologist, 80*(1), 21-41.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877-886.

Edney, J. J. (1975). Territoriality and control: A field experiment. *Journal of Personality and Social Psychology, 31*(6), 1108-1115.

Edney, J. J. (1976). Human territories: Comments on functional properties. *Environment and Behavior, 8*(1), 31-47.

Fernandez, K. V. (2008). Protecting the portals of home. In A. Y. Lee & D. Soman (Eds.), *Advances in consumer research* (Vol. 35, pp. 774-775). Duluth, MN: Association for Consumer Research.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobserved variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Fortes, N., & Paulo, R. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics, 22*(3), 167-176.

Ganley, D., & Lampe, C. (2009). The ties that bind: Social network principles in online communities. *Decision Support Systems, 47*(3), 266.

Garver, M. S., & Mentzer, J. T. (1999). Logistics research methods: Employing structural equation modeling to test for construct validity. *Journal of Business Logistics, 20*(1), 33-57.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*, 91-109.

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

Goel, L., Johnson, N., Junglas, I., & Ives, B. (2011). From space to place: Predicting users' intentions to return to virtual worlds. *MIS Quarterly, 35*(3), 749-771.

Good, D. (1988). Individuals, interpersonal relations, and trust. In D. G. Gambetta (Ed.), *Trust* (pp. 131-185). New York, NY: Blackwell.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate data analysis with readings* (5th ed.). Englewood Cliffs, NJ: Prentice Hall.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*(1), 111-123.

Halford, S., & Leonard, P. (2006). Place, space and time: Contextualizing workplace subjectivity. *Organization Studies, 27*(5), 657-676.

Havenstein, H. (2008). One in five employers uses social networks in the hiring process. Retrieved from http://www.computerworld.com/s/article/9114560/One_in_five_employers_uses_social_networks_in_hiring_process

Heirman, W., Walrave, M., Vermeulen, A., Ponnet, K., Vandebosch, H., Van Ouytsel, J., & Van Gool, E. (2016). An open book on Facebook? Examining the interdependence of adolescents' privacy regulation strategies. *Behaviour & Information Technology, 35*(9), 706-719.

Helm, S., Eggert, A., & Garnefeld, I. (2010). Modeling the impact of corporate reputation on customer satisfaction and loyalty using partial least squares. In V. E. Vinzi, W. W. Chin, J. Henseler & H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods, and applications* (pp. 515-534). Berlin: Springer.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275-298.

Hornsey, M. J. (2008). Social identity theory and self-categorization theory: A historical review. *Social and Personality Psychology Compass, 2*(1), 204-222.

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management, 54*(7), Information & Management

James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management, 52*(8), 893-908.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2).

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology and Management, 1*(1-2), 45-71.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199-218.

Jayachandran, S., Sharma, S., Kaufman, P., & Raman, P. (2005). The role of relational information processes and technology use in customer relationship management. *Journal of Marketing, 69*(4), 177-192.

Ji, P., & Lieber, P. S. (2010). Am I safe? Exploring relationships between primary territories and online privacy. *Journal of Internet Commerce, 9*(1), 3-22.

Jiang, Z. J., Heng, C. S., & Choi, B. C. F. (2013). Research note: Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research, 24*(3), 579-595.

Johnson, R. E., Rosen, C. C., & Djurdjevic, E. (2011). Assessing the impact of common method variance on higher order multidimensional constructs. *Journal of Applied Psychology, 96*(4), 744-761.

Jordaan, Y., & Van Heerden, G. (2017). Online privacy-predictors of Facebook usage intensity. *Computers in Human Behavior, 70*, 90-96.

Jöreskog, K. G. (1971). Statistical analysis of sets of congeneric tests. *Psychometrika, 36*(2), 109-133.

Kahn, C., & Ingram, D. (2018). Three-quarters Facebook users as active or more since privacy scandal: Reuters/lpsos poll. Retrieved from https://www.reuters.com/article/us-facebook-privacy-poll/three-quarters-facebook-users-as-active-or-more-since-privacy-scandal-reuters-ipsos-poll-idUSKBN1I7081/

Kimmons, J. V., & Austin, T. (2012). Territory and privacy in academic workspaces. *Business Studies Journal, 4*, 59-69.

Kisekka, V., Bagchi-Sen, S., & Raghav Rao, H. (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. *Computers in Human Behavior, 29*(6), 2722-2729.

Krasnova, H., Hildebrand, T., & Günther, O. (2009). *Investigating the value of privacy in online social networks: Conjoint analysis.* Paper presented at the 30th International Conference on Information Systems, Phoenix, AZ.

Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior, 76*, 149-163.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*(1), 79-100.

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management 52*(7), 882-891.

Liang, K., Liu, J. K., Lu, R., & Wong, D. S. (2015). Privacy concerns for photo sharing in online social networks. *IEEE Internet Computing, 19*(2), 58-63.

Lindell, M., & Whitney, D. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114-121.

Lo, J. (2010). *Privacy concern, locus of control, and salience in a trust-risk model of information disclosure on social networking sites*. Paper presented at the 16th Americas Conference on Information Systems, Lima, Peru.

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of Applied Psychology, 90*(4), 710-730.

Madden, M. (2012). Privacy management on social media sites. Pew Research Center. Retrieved from http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/

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

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411-429.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

McKnight, D. H., Lankton, N., & Tripp, J. (2011). *Social networking information disclosure and continuance intention: A disconnect*. Paper presented at the 44th Hawaii International Conference on System Sciences, Manoa, HI.

Mechant, P., & Evens, T. (2011). Interaction in web-based communities: A case study of Last.fm. *International Journal of Web Based Communities, 7*(2), 234-249.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335-361.

Moorman, C., Zaltman, G., & Deshpande, R. (1992). Relationships between providers and users of marketing research: The dynamics of trust within and between organizations. *Journal of Marketing Research, 29*(3), 314-328.

Mothersbaugh, D. L., Foxx, W. K. I., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76-98.

Nauen, R. (2017). Number of employers using social media to screen candidates at all-time high, finds latest careerbuilder study. Retrieved from http://press.careerbuilder.com/2017-06-15-Number-of-Employers-Using-Social-Media-to-Screen-Candidates-at-All-Time-High-Finds-Latest-CareerBuilder-Study

Nikravan, L. (2016). Number of employers using social media to screen candidates has increased 500 percent over the last decade. Retrieved from http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?ed=12%2F31%2F2016&id=pr945&sd=4%2F28%2F2016

Oestreicher-Singer, G., & Zalmanson, L. (2009). *"Paying for content or paying for community?" The effect of social involvement on subscribing to media web sites.* Paper presented at the 30th International Conference on Information Systems, Phoenix, AZ.

Oldenburg, R. (1989). *The great good place: Cafes, coffee shops, community centers, beauty parlors, general stores, bars, hangouts and how they get you through the day*. New York, NY: Marlowe.

Ormerod, M. B., McKenzie, J., & Woods, A. (1995). Final report on research relating to the concept of five separate dimensions of personality—or six including intelligence. *Personality and Individual Differences, 18*, 451-461.

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior, 28*(3), 1019-1027.

Peachey, A. (2010). The third place in Second Life: Real life community in virtual worlds. In A. Peachey, J. Gillen, D. Livingstone, & S. Smith-Robbins (Eds.), *Human-computer interaction series: Researching learning in virtual worlds* (pp. 91-110). London: Springer.

Pedersen, D. M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology, 19*(4), 397-405.

Pedersen, E., Hallberg, L. R., & Waye, K. P. (2007). Living in the vicinity of wind turbines: A grounded theory study. *Qualitative Research in Psychology, 4*(1-2), 49-63.

Perlroth, N., & Issac, M. (2015, December 8). Terrorists mock bid to end use of social media. *New York Times*.

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory, 1*(4), 311-335.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623-656.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy Marketing, 19*(1), 27-41.

Podsakoff, P., MacKenzie, S., Lee, J., & Podsakoff, N. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181-195.

Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm performance impacts of digitally enabled supply chain integration capabilities. *MIS Quarterly, 30*(2), 225-246.

Rao, V. (2008). *Facebook Applications and playful mood: the construction of Facebook as a "third place"*. Paper presented at the MindTrek 12th International Conference on Entertainment and Media in the Ubiquitous Era, Tampere, Finland.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods, 12*(4), 762-800.

Ringle, C. M., Wende, S., & Will, A. (2006). SmartPLS 2.0.M3. Retrieved from http://www.smartpls.com

Saunders, C., Rutkowski, A.-F., van Genuchten, M., Vogel, D. R., & Orrego, J. M. (2011). Virtual space and place: Theory and test. *MIS Quarterly, 35*(4), 1078-1098.

Schneider, S. L., & Lopes, L. L. (1986). Reflection in preferences under risk: Who and when may suggest why. *Journal of Experimental Psychology: Human Perception and Performance, 12*(4), 535-548.

Schwab, D. P. (2005). *Research methods for organizational studies* (2nd ed.). Mahwah, NJ: Erlbaum.

Shibchurn, J., & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic-extrinsic motivation perspective. *Computers in Human Behavior, 44*, 103-117.

Sitkin, S., & Pablo, A. (1992). Reconceptualizing the determinants of risk behavior. *Academy of Management Review, 17*(1), 9-38.

Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Smith, H., Milburg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation model. In S. Leinhardt (Ed.), *Sociological methodology* (pp. 290-312). San Francisco, CA: Jossey-Bass.

Soukup, C. (2006). Computer-mediated communication as a virtual third place: Building Oldenburg's great good places on the World Wide Web. *New Media & Society, 8*(3), 421-440.

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication, 22*(2), 55-70.

Steinfield, C., Ellison, N. B., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology, 29*(6), 434-445.

Steinkuehler, C., & Williams, D. (2006). Where everybody knows your (screen) name: Online games as "third places". *Journal of Computer Mediated Communication, 11*(4), 885-905.

Taylor, R. B., & Ferguson, G. (1980). Solitude and intimacy: Linking territoriality and privacy experiences. *Journal of Nonverbal Behavior, 4*(4), 227-239.

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior, 78*, 283-297.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*, 415-444.

Vlek, C., & Stallen, P. J. (1980). Rational and personal aspects of risk. *Acta Psychologica, 45*(1-3), 273-300.

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*(1), 101-115.

Westin, A. (1967). *Privacy and freedom*. New York, NY: Athenaeum.

Westin, A. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure.

Human Communication Research, 2(4), 338-346.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135-173.

Xu, Y., Lu, X., Goh, K. Y., Jiang, Z., & Zhu, X. (2009). *The impact of online social network on consumer loyalty: An empirical study of an online dining community.* Paper presented at the 30th International Conference on Information Systems, Phoenix, AZ.

Xu, Y., Zhang, C., Xue, L., & Yeo, L. L. (2008). *Product adoption in online social network.* Paper presented at the 29th International Conference on Information Systems, Paris, France.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *The Database for Advances in Information Systems, 40*(1), 38-51.

Zhao, X., Lynch, J. G. J., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research, 37*(2), 197-206.

Appendix A: Survey Instrument, Measures, and Factor Validity

We used an online self-report survey instrument to collect data. The instructions and questions for Study 1 are presented in Table A1. All items used a seven-point Likert-type scale ranging from "strongly disagree" (1) to "strongly agree" (7).

Table A1. Study 1: Survey Instructions and Questions

The purpose of this survey is to learn about managing privacy in online social networks. **Note that many questions are similar, so please read each question carefully.** Please select the answer that corresponds to how much do you agree or disagree with the following statements:	
Item #	**Question**
INFO 1	Private information is sensitive information that you tell only under certain circumstances.
INFO 2	Private information is sensitive information that you tell only to certain people.
SNT1	An online social network refers to a group of people who interact on the Internet.
SNT2	An online social network refers to a group of people who interact on the Internet about a specific topic (e.g. snowboarding).
SNT3	An online social network refers to a group of people who interact on the Internet for a specific purpose (e.g. political action).
SNT4	An online forum focused on sports is an example of an online social network.
VT1	Your virtual territory is the area on a social networking site that you feel is your own.
VT2	Your virtual territory is the space on a social networking site that you feel is yours.
VT3	You can have multiple virtual territories on a social networking site.
VT4	You can have multiple areas on a social networking site that you feel are your own.
VT5	Your main page on Facebook is an example of a virtual territory in an online social network.
VT6	An Instagram account is an example of a virtual territory in an online social network.
VT7	Your Facebook wall ("Timeline" page) that displays all the items associated with your name is an example of a virtual territory in an online social network.

Table A2 presents the construct definitions and the measures for Study 2. Tables A3-A7 present the measurement items and the results of the factor analysis. All items used a seven-point Likert-type scale ranging from "strongly disagree" (1) to "strongly agree" (7).

Table A2. Study 2: Summary of Constructs and Measures

Construct and definition	No. of Items	Measure
Information Privacy Concerns: An individual's worries about SNS members' information privacy practices. **Collection dimension:** The degree to which an individual is concerned about the private information disclosed to SNS members (i.e., confidants) relative to the benefits received. **Control dimension:** The degree to which an individual is concerned about her freedom to approve, modify, or delete his or her private information. **Awareness dimension:** The degree to which an individual is concerned about his or her knowledge of the SNS members' information privacy practices.	10	Adapted from Malhotra et al. (2004)
Territory Privacy Concerns: An individual's worries about SNS members' territory privacy practices. **Access dimension:** The degree to which an individual is concerned about the vulnerability of the private virtual territory made accessible to SNS members relative to the value of the benefits received. **Control dimension:** The degree to which an individual is concerned about his or her freedom to configure access to his or her private virtual territory. **Awareness dimension:** The degree to which an individual is concerned about his or her knowledge of the SNS members' territory privacy practices.	9	Developed
Information Trusting Beliefs: The degree to which an individual believes that his or her SNS members will behave in a dependable manner regarding the individual's private information.	4	Adapted from Malhotra et al. (2004)
Territory Trusting Beliefs: The degree to which an individual believes that his or her members will behave in a dependable manner regarding the individual's virtual territory.	4	Developed
Information Privacy Risk Beliefs: An individual's perception of the likelihood of loss due to sharing private information with his or her SNS members.	4	Adapted from Malhotra et al. (2004)
Territory Privacy Risk Beliefs: An individual's perception of the likelihood of loss due to allowing his or her SNS members to access and interact in one's virtual territory.	4	Developed
Private Disclosure: An individual's voluntarily and intentionally revealing private information to his or her SNS members.	4	Adapted from Jiang et al. (2013)

Territory Coordination: An individual's behavior to manage virtual territory accessibility with his or her SNS members. **Linkage coordination:** An individual's behavior to manage who can access an individual's private virtual territory. **Permeability coordination:** An individual's behavior to manage how difficult a private virtual territory is for others to access. **Ownership coordination:** An individual's behavior to manage who has rights and privileges to control an individual's private virtual territory.	10	Developed
Technological Features: The degree to which an individual perceives that technical tools/features exist to support territory coordination.	3	Developed

Table A3. Study 2: Information Privacy Concerns Items and Factor Loadings

Construct: dimension	Question	Item#	Collect	Control	Aware
Information privacy concerns (IPC): Collection	It bothers me when I need to disclose private information about myself to social networking site members.	IPC1	.898	.153	.174
	I sometimes think twice before disclosing private information about me on my social networking site.	IPC2	Drop		
	It bothers me to disclose private information about me to so many social networking site members.	IPC3	.912	.175	.174
	It bothers me to disclose too much private information about me on my social networking site.	IPC4	.892	.181	.228
	I'm concerned that I disclose too much private information about me on my social networking site.	IPC5	Drop		
Information privacy concerns (IPC): Control	Privacy in the social networking site is really a matter of my right to exercise control over decisions about how my private information is shared on my social networking site.	IPC6	.320	.725	.088
	Control of my private information lies at the heart of privacy in the social networking site.	IPC7	.003	.821	.266
	I believe that privacy in the social networking site is invaded when control over private information about me is lost or unwillingly reduced.	IPC8	.242	.767	.336
	It is very important to me that I am knowledgeable about how social networking site members view my private information.	IPC9	Drop		
Information privacy concerns (IPC): Awareness	Social networking site members who want to further share my private information should inform me how they will discuss it.	IPC10	.144	.161	.913
	Social networking site members should make it clear and conspicuous to me about the way my private information is discussed.	IPC11	.234	.252	.871
	It is very important to me that I am knowledgeable about how social networking site members treat my private information.	IPC12	Drop		
	Social networking site members who want to further share my private information should inform me how they will share it.	IPC13	.154	.195	.931
	Social networking site members should make it clear and obvious to me how my private information is shared.	IPC14	.219	.265	.887

Table A4. Study 2: Territory Privacy Concerns Items and Factor Loadings

Construct: dimension	Question	Item #	Access	Control	Aware
Territory privacy concerns (TPC): Access	It bothers me when I consider making my virtual territory accessible to social networking site members.	TPC1	.847	.128	.101
	I sometimes think twice before making my virtual territory accessible to social networking site members.	TPC2	Drop		
	It bothers me to make my virtual territory accessible to so many social networking site members.	TPC3	.888	.109	.173
	It bothers me to make too much of my virtual territory accessible to social networking site members.	TPC4	.844	.144	.115
	I'm concerned that I make too much of my virtual territory accessible to social networking site members.	TPC5	Drop		
Territory privacy concerns (TPC): Control	Privacy is really a matter of my right to exercise control over decisions about what social networking site members DISCLOSE in my virtual territory.	TPC6	.232	.675	.147
	Control of my virtual territory lies at the heart of privacy on my social networking site.	TPC7	.061	.847	.136
	I believe that privacy in the social networking site is invaded when control over my virtual territory is lost or unwillingly reduced.	TPC8	.094	.704	.373
Territory privacy concerns (TPC): Awareness	It is very important to me that I am knowledgeable about what social networking site members will DISCLOSE in my virtual territory.	TPC9	Drop		
	It is very important to me that I am knowledgeable about how social networking site members will INTERACT WITH OTHERS in my virtual territory.	TPC10	Drop		
	Social networking site members should make it clear and conspicuous to me what they will DISCLOSE in my virtual territory.	TPC11	.201	.191	.874
	Social networking site members should make it clear and conspicuous to me how they will INTERACT WITH OTHERS in my virtual territory.	TPC12	.084	.196	.896
	Privacy is really a matter of my right to exercise control over decisions about how social networking site members INTERACT WITH OTHERS in my virtual territory.	TPC13	Drop		
	Social networking site members should make it clear and conspicuous to me what they will DO in my virtual territory.	TPC14	.144	.243	.849
	Social networking site members should make it clear and conspicuous to me how they will SHARE my virtual territory.	TPC15	Drop		

Table A5. Study 2: Territory Coordination Items and Factor Loadings

Construct: dimension	Question	Item#	Link-age	Permea-bility	Owner-ship
Territory coordination (TC): Linkage coordination	I would share my virtual territory with online social network members with hesitation.	TC1	Drop		
	I would try to figure out who is trustworthy when deciding whom I allow to access to my virtual territory.	TC2	.797	.200	.364
	I would try to discourage other friends from visiting my virtual territory.	TC3	.726	.329	-.032
	I would try to figure out if social networking site members are trustworthy when deciding whether I should make my virtual territory accessible.	TC4	.810	.274	.337
	I would make my virtual territory accessible to a few selected people.	TC5	Drop		
Territory coordination (TC): Permeability coordination	I would make some areas of my virtual territory very private, while making others not as private.	TC6	.249	.579	.440
	Not all areas of my virtual territory would be accessible to all social networking site members.	TC7	Drop		
	I would make it difficult for some people to have access to some of the areas of my virtual territory.	TC8	Drop		
	To manage my virtual territory, I would put social networking site members in different groups.	TC9	.259	.889	.194
	Each group on my social networking site would have its own level of accessibility to my virtual territory.	TC10	.345	.858	.196
Territory coordination (TC): Ownership coordination	When online social network members invite their friends to VIEW my virtual territory (through tags or links), I may disable the invitations (tags) that I do not like.	TC11	Drop		
	When online social network members invite their friends to INTERACT in my virtual territory (through tags or links), I may disable the invitations (tags) that I do not like.	TC12	Drop		
	I would try to prevent online social network members from linking (tagging) their friends that I do not want in my virtual territory.	TC13	Drop		
	I may delete online social network members' comments I do not like from my virtual territory.	TC14	.288	.093	.734
	Online social network members should not post things in my virtual territory that may embarrass me.	TC15	.155	.239	.873
	I would try to prevent online social network members from posting things in my virtual territory that may embarrass me.	TC16	.134	.193	.915
	I would try to prevent online social network members from doing things in my virtual territory that may embarrass me.	TC17	.113	.220	.902

Table A6. Study 2: Items and Factor Loadings for TPRB, TTB, IPRB, ITB, and Technological Features

Construct	Questions	Item#	TPRB	TTB	IPRB	ITB	PD	TF
Territory privacy risk beliefs	It is risky to allow social networking site members to visit my virtual territory	TPRB1	Drop					
	It is risky to allow social networking site members to interact with me in my virtual territory.	TPRB2	Drop					
	It is risky to allow social networking site members to interact with others in my virtual territory.	TPRB3	Drop					
	There is a high potential for loss associated with allowing social networking site members to interact with me in my virtual territory.	TPRB4	Drop					
	There is a high potential for loss associated with allowing social networking site members to visit my virtual territory.	TPRB5	.826	.039	.229	.060	.015	-.045
	There is too much uncertainty associated with allowing social networking site members to visit my virtual territory.	TPRB6	.920	.028	.106	.035	-.022	-.062
	To allow social networking site members to visit my virtual territory involves many unexpected problems.	TPRB7	Drop					
	There is a high potential for loss associated with allowing social networking site members to interact with others in my virtual territory.	TPRB8	Drop					
	There is too much uncertainty associated with allowing social networking site members to interact with me in my virtual territory.	TPRB9	.926	.039	.108	-.002	.009	-.046
	There is too much uncertainty associated with allowing social networking site members to interact with others in my virtual territory.	TPRB 10	Drop					
	To allow social networking site members to interact with me in my virtual territory involves many unexpected problems.	TPRB 11	Drop					
	To allow social networking site members to interact with others in my virtual territory involves many unexpected problems.	TPRB 12	.855	-.011	.182	-.035	-.016	-.077
Territory trusting beliefs	I trust that social networking site members would keep my best interests in mind when posting things in my virtual territory.	TTB1	Drop					
	Online social network members are in general predictable regarding posting things in my virtual territory.	TTB2	-.013	.870	-.008	.118	.035	.019
	Online social network members are in general consistent regarding posting things in my virtual territory.	TTB3	.002	.869	.128	.201	.007	-.036

Table A6. Study 2: Items and Factor Loadings for TPRB, TTB, IPRB, ITB, and Technological Features

Construct	Questions	Item#	TPRB	TTB	IPRB	ITB	PD	TF
	Social networking site members are, in general, honest with me about how they will behave when posting things in my virtual territory.	TTB4	Drop					
	I trust that social networking site members would keep my best interests in mind when interacting with others in my virtual territory.	TTB5	Drop					
	Online social network members are in general predictable regarding how they interact with others in my virtual territory.	TTB6	.044	.881	.076	.176	.024	-.059
	Online social network members are in general consistent regarding how they interact with others in my virtual territory.	TTB7	.071	.834	.192	.231	-.010	.053
	Social networking site members are in general honest with me about how they will behave when interacting with others in my virtual territory.	TTB8	Drop					
Information privacy risk beliefs	It is risky to give my private information to online social network members.	IPRB1	.015	.157	.832	-.016	-.006	-.073
	There is a high potential for loss associated with giving my private information to online social network members.	IPRB2	.170	.119	.879	-.061	-.091	-.056
	There is too much uncertainty associated with giving my private information to online social network members.	IPRB3	.209	.056	.859	-.056	-.109	-.011
	Sharing my private information in an online social network involves many unexpected problems.	IPRB4	.316	.024	.811	-.093	-.048	.037
Information trusting beliefs	I trust that social networking site members would keep my best interests in mind when dealing with my private information.	ITB1	Drop					
	Social networking site members are in general honest with me regarding how they will discuss my private information.	ITB2	-.003	.184	-.119	.866	.101	-.013
	Social networking site members are in general honest with me regarding how they will share my private information.	ITB3	.046	.183	-.094	.900	.126	.013
	Social networking site members are in general predictable regarding how they will discuss my private information.	ITB4	.019	.181	.011	.892	.067	-.032
	Social networking site members are in general predictable with me regarding how they will share my private information.	ITB5	-.008	.172	-.025	.899	.071	-.064
	Social networking site members are in general consistent with me regarding how they will discuss my private information.	ITB6	Drop					
	Social networking site members are in general consistent with me regarding how they will share my private information.	ITB7	Drop					

Table A6. Study 2: Items and Factor Loadings for TPRB, TTB, IPRB, ITB, and Technological Features

Construct	Questions	Item#	TPRB	TTB	IPRB	ITB	PD	TF
Private disclosure	I would reveal personal thoughts about the photos in my virtual territory.	PD1	-.099	.048	.094	.104	.866	-.054
	I would reveal personal feelings about the photos in my virtual territory.	PD2	-.061	.023	.019	.092	.864	-.041
	I would reveal personal experiences about the photos in my virtual territory.	PD3	Drop					
	I would reveal sensitive information about the photos in my virtual territory.	PD4	.142	-.048	-.205	.082	.767	.011
	I would reveal a lot of information about the photos in my virtual territory.	PD5	.096	.001	-.186	.098	.780	.008
Technological features	There are sufficient tools/features for me to control who can access my virtual territory.	TF1	-.154	-.068	-.061	-.027	-.004	.912
	There are sufficient tools/features for me to control which part of my virtual territory is accessible to various social networking site members.	TF2	-.090	-.026	-.039	-.037	-.042	.941
	There are sufficient tools/features for me to control what social networking site members can do in my virtual territory.	TF3	.028	.068	.000	-.021	-.018	.913

Table A7. Study 2: Items for Control Variables

Gender: male; female; other.

Native language: Native language? Arabic; Chinese; English; French; Hindi; Korean; Malay; Portuguese; Spanish; Other, please specify _____.

Education: Highest level of education attained? Some school, no degree; high school diploma; associates degree; bachelor's degree; graduate degree.

SNS type: Social networking site that you have visited/participated with the most in the past 30 days? Facebook; Instagram; Twitter; Forum; Blog; LinkedIn; Tumblr; Snapchat; other online social network, please specify _____.

Tenure in SNS: Years you have participated in your focal online social network? Less than 1 year; 1-2 years; 2-3 years; 3-4 years; 4-5 years; 5-6 years; 6-7 years; 7 or more.

Connection number: Number of connections (e.g., friends, followers, etc.) in the focal online social network? Less than 100; 101-200; 201-300; 301-400; 401-500; 501-600; 601-700; 701-800; 801-1,000; More than 1,000.

Weekly hours in SNS: Hours per week, on average, in the focal online social network? < 1 hour per week; 1-2 hours per week; 3-4 hours per week; 5-6 hours per week; 7-8 hours per week; 9-10 hours per week; 11-14 hours per week; 15-18 hours per week; 19-24 hours per week; 25-30 hours per week; 30-40 hours per week; > 40 hours per week.

Technological features:

(TF1) There are sufficient tools/features for me to control who can access my virtual territory.

(TF2) There are sufficient tools/features for me to control which part of my virtual territory is accessible to various social networking site members.

(TF3) There are sufficient tools/features for me to control what social networking site members can do in my virtual territory.

Appendix B: Item-Construct Correlation

Table B1. Item-Construct Correlation

	IPC Collect	IPC Ctrl	IPC Aware	ITB	IPRB	TPC Access	TPC Ctrl	TPC Aware	TTB	TPRB	PD	Link-age	Permea-bility	Owner-ship
IPC1	.931	.395	.375	-.004	.412	.410	.304	.315	.073	.301	-.164	.204	.201	.253
IPC3	.948	.417	.385	.052	.447	.403	.279	.280	.044	.291	-.190	.195	.161	.231
IPC4	.939	.434	.432	.026	.475	.364	.303	.305	.107	.280	-.149	.140	.163	.243
IPC6	.416	.772	.340	.102	.358	.227	.505	.341	.185	.106	-.075	.152	.145	.250
IPC7	.243	.824	.431	-.038	.365	.223	.491	.333	.181	.079	-.093	.228	.326	.299
IPC8	.437	.882	.533	.022	.407	.228	.542	.308	.255	.030	-.143	.194	.235	.317
IPC10	.352	.447	.935	.016	.432	.233	.422	.476	.156	.169	-.188	.252	.279	.256
IPC11	.440	.532	.938	.036	.504	.255	.382	.512	.145	.158	-.219	.255	.278	.296
IPC13	.374	.484	.961	.000	.470	.257	.446	.480	.169	.172	-.187	.223	.268	.255
IPC14	.437	.543	.951	.002	.497	.277	.433	.530	.200	.133	-.220	.301	.329	.327
ITB2	-.040	.040	-.011	.905	-.134	-.031	.210	.104	.340	.013	.207	-.003	-.026	-.059
ITB3	.010	.042	.000	.936	-.111	-.003	.197	.118	.355	.061	.224	-.059	-.038	.020
ITB4	.054	.022	.084	.904	-.025	.036	.198	.167	.364	.056	.162	-.032	.011	-.037
ITB5	.080	.015	-.016	.913	-.054	.036	.176	.068	.353	.029	.176	-.104	-.043	-.045
IPRB1	.412	.391	.432	-.039	.862	.264	.245	.219	.234	.173	-.080	.170	.180	.254
IPRB2	.374	.419	.444	-.096	.925	.239	.231	.253	.205	.304	-.166	.221	.249	.177
IPRB3	.485	.411	.474	-.106	.893	.354	.262	.333	.149	.327	-.176	.334	.208	.232
IPRB4	.368	.291	.325	-.137	.772	.251	.168	.277	.111	.387	-.088	.254	.255	.117
TPC1	.325	.163	.174	.041	.155	.862	.279	.266	.215	.484	-.061	.278	.110	.101
TPC3	.345	.255	.261	-.027	.261	.913	.300	.321	.135	.433	-.188	.416	.179	.163
TPC4	.434	.300	.277	.012	.428	.865	.300	.275	.180	.353	-.216	.316	.147	.111
TPC6	.145	.352	.304	.074	.227	.309	.725	.349	.260	.144	-.038	.235	.139	.212
TPC7	.227	.454	.250	.242	.128	.219	.819	.351	.244	.134	.021	.201	.317	.286
TPC8	.359	.642	.490	.182	.295	.263	.814	.495	.253	.164	-.158	.139	.206	.387
TPC11	.287	.369	.472	.072	.289	.346	.458	.918	.160	.319	-.208	.194	.222	.238
TPC12	.264	.331	.469	.124	.257	.246	.450	.920	.185	.301	-.139	.218	.287	.225
TPC14	.324	.378	.503	.146	.276	.302	.483	.896	.259	.252	-.255	.241	.238	.228
TTB2	-.047	.142	.078	.301	.095	.068	.176	.124	.859	.001	.057	.100	.105	.051
TTB3	.105	.270	.150	.354	.217	.225	.336	.242	.907	.073	.025	.065	.056	.063
TTB6	.048	.153	.147	.345	.182	.141	.253	.163	.897	.091	.046	.072	.072	.137
TTB7	.161	.316	.243	.366	.271	.260	.359	.246	.892	.143	.003	.080	.143	.153
TPRB5	.291	.107	.188	.062	.332	.433	.183	.304	.099	.883	.002	.175	.194	.095
TPRB6	.276	.072	.121	.044	.255	.458	.183	.299	.074	.946	-.007	.170	.177	.104
TPRB9	.294	.057	.156	.015	.255	.445	.155	.285	.075	.948	.010	.151	.173	.114
TPRB12	.233	.114	.145	-.029	.303	.358	.162	.272	.029	.774	-.006	.197	.202	.085

Table B1. Item-Construct Correlation

	IPC Collect	IPC Ctrl	IPC Aware	ITB	IPRB	TPC Access	TPC Ctrl	TPC Aware	TTB	TPRB	PD	Link-age	Permea-bility	Owner-ship
PD1	-.042	-.024	-.028	.188	-.028	-.128	-.015	-.165	.088	-.039	.829	-.150	-.019	-.090
PD2	-.041	.020	-.027	.179	-.082	-.129	.051	-.123	.053	-.022	.830	-.131	.006	.004
PD3	-.030	-.002	-.098	.085	-.066	-.152	.037	-.124	.036	-.041	.699	-.196	-.058	-.025
PD4	-.255	-.226	-.343	.160	-.215	-.121	-.134	-.211	-.029	.047	.849	-.147	-.059	-.283
PD5	-.239	-.175	-.293	.185	-.193	-.212	-.138	-.233	.017	.014	.858	-.218	-.064	-.262
TC2	.198	.196	.292	-.067	.237	.305	.209	.196	.067	.151	-.223	.897	.567	.481
TC3	.086	.084	.073	-.040	.173	.277	.141	.142	.064	.173	-.007	.737	.473	.212
TC4	.194	.294	.303	-.031	.279	.398	.259	.265	.095	.141	-.235	.927	.619	.486
TC6	.108	.226	.291	-.072	.187	.090	.205	.229	.079	.001	-.117	.524	.785	.527
TC9	.176	.263	.241	.014	.200	.159	.252	.229	.089	.267	.013	.564	.917	.429
TC10	.201	.265	.279	-.019	.240	.183	.286	.263	.109	.228	-.018	.622	.933	.420
TC14	.240	.264	.277	.030	.194	.140	.298	.245	.127	.061	-.175	.449	.421	.660
TC15	.281	.380	.369	-.019	.257	.173	.431	.276	.149	.140	-.197	.461	.506	.933
TC16	.254	.338	.265	-.044	.217	.135	.335	.247	.084	.084	-.201	.450	.478	.967
TC17	.202	.283	.224	-.030	.229	.100	.317	.200	.096	.100	-.160	.438	.490	.956

Appendix C: Mediation Test

Table C1 presents the results of the effect size test, the Sobel test, the mediation types, and the VAF of mediation effects for the post hoc analysis. The Sobel test is a z-statistic based on the path coefficients and the standard errors of two paths: the path from the independent variable to the mediator and the path from the mediator to the dependent variable (Sobel, 1982). The F statistic is calculated as $f^2 \times$ (n-k-1), with (1, (n-k)) degrees of freedom, where n = sample size, k = number of constructs, and f^2 = (R^2 for path included - R^2 for path excluded) / (1 - R^2 for path included) (Chin, Marcolin, & Newsted, 2003). VAF is computed as (indirect path coefficient $\alpha \times$ indirect path coefficient β) / (indirect path coefficient $\alpha \times$ indirect path coefficient β + direct path efficient) (Helm, Eggert, & Garnefeld, 2010).

Table C1. Summary of Mediation Tests

	Path	Path coefficient		Effect size			Sobel		Mediation type	VAF
		β	P value	f^2	F	P value	Z	P value		
IPC-ITB-PD	IPC-ITB	0.025	NS	0.037	5.883	p < 0.05	0.267	NS	No Mediation	0.009
	ITB-PD	0.196	p < 0.01							
	IPC-PD	-0.269	p < 0.01	0.057	9.063	p < 0.01				
IPC-IPRB-PD	IPC-IPRB	0.558	p < 0.001	0.000	0.000	NS	0.238	NS	No Mediation	0.046
	IPRB-PD	0.023	NS							
	IPC-PD	-0.269	p < 0.01	0.057	9.063	NS				
IPC-IPRB-TC	IPC-IPRB	0.558	p < 0.001	0.008	1.272	NS	1.038	NS	No Mediation	0.160
	IPRB-TC	0.102	NS							
	IPRB-TC	0.298	p < 0.001	0.070	11.130	p < 0.001				
IPC-ITB-IPRB	IPC-ITB	0.025	NS	0.023	3.657	NS	0.276	NS	No Mediation	0.005
	ITB-IPRB	-0.120	NS							
	IPC-IPRB	0.558	p < 0.001	0.483	76.797	p < 0.001				
ITB-IPRB-PD	ITB-IPRB	-0.120	NS	0.012	1.908	NS	0.946	NS	No Mediation	0.067
	IPRB-PD	-0.105	NS							
	ITB-PD	0.175	p < 0.05	0.033	5.247	p < 0.05				
ITB-IPRB-TC	ITB-IPRB	-0.120	NS	0.057	9.063	p < 0.01	1.351	NS	No Mediation	0.301
	IPRB-TC	0.245	p < 0.01							
	ITB-TC	-0.068	NS	0.004	0.636	NS				
IPRB-TC-PD	IPRB-TC	0.260	p < 0.01	0.009	1.431	NS	0.776	NS	No Mediation	0.182
	TC-PD	-0.090	NS							
	IPRB-PD	-0.105	NS	0.012	1.908	NS				
TPC-TTB-TC	TPC-TTB	0.334	p < 0.001	0.001	0.159	NS	0.033	NS	No Mediation	0.002
	TTB-TC	-0.002	NS							
	TPC-TC	0.321	p < 0.001	0.097	15.423	p < 0.001				
TPC-TPRB-TC	TPC-TPRB	0.451	p < 0.001	0.000	0.000	NS	0.459	NS	No Mediation	0.046
	TPRB-TC	0.034	NS							
	TPC-TC	0.321	p < 0.001	0.097	15.423	p < 0.001				
TPC-TTB-TPRB	TPC-TTB	0.333	p < 0.001	0.002	0.318	NS	0.636	NS	No Mediation	0.035
	TTB-TPRB	-0.049	NS							
	TPC-TPRB	0.452	p < 0.001	0.224	35.616	p < 0.001				

Table C1. Summary of Mediation Tests

TPC-TPRB-IPRB	TPC-TPRB	0.452	p < 0.001	0.052	8.268	p < 0.01	2.477	p < 0.05	**Full Mediation**	0.645
	TPRB-IPRB	0.197	p < 0.01							
	TPC-IPRB	-0.049	NS	0.002	0.318	NS				
TTB-TPRB-TC	TTB-TPRB	-0.049	NS	0.020	3.180	NS	0.594	NS	No Mediation	0.090
	TPRB-TC	0.141	NS							
	TTB-TC	0.070	NS	0.005	0.795	NS				
TTB-TPRB-IPRB	TTB-TPRB	-0.048	NS	0.050	7.95	p < 0.01	0.639	NS	No Mediation	0.048
	TPRB-IPRB	0.176	p < 0.05							
	TTB-IPRB	0.167	p < 0.05	0.038	6.042	p < 0.05				
TPRB-IPRB-PD	TPRB-IPRB	0.183	p < 0.01	0.016	2.544	NS	1.287	NS	No Mediation	0.237
	IPRB-PD	-0.127	NS							
	TPRB-PD	0.075	NS	0.006	0.954	NS				
TPRB-IPRB-TC	TPRB-IPRB	0.183	p < 0.01	0.069	10.971	p < 0.001	1.997	p < 0.05	**Full Mediation**	0.252
	IPRB-TC	0.260	p < 0.01							
	TPRB-TC	0.141	NS	0.020	3.180	NS				

About the Authors

Shuai-fu Lin. Shuai-fu Lin is an assistant professor of management information systems in the College of Business at the University of Central Arkansas. Shuai-fu Lin has developed research interests around individual cognition and behavior, and usage of emerging information technologies. His research has appeared in *the Journal of the Association for Information Systems* and *Computers in Human Behavior*.

Deborah J. Armstrong. Deborah J. Armstrong is an associate professor of management information systems in the College of Business at Florida State University. Deborah Armstrong's research interests cover a variety of issues at the intersection of IS personnel and cognition involving the human aspects of technology, change, and learning. Her research has appeared in *Management Information Systems Quarterly*, *Journal of Management Information Systems*, *the European Journal of Information Systems* and *Communications of the ACM*, among others. To God be all the glory.