Communications of the Association for Information Systems

Volume 38 Article 10

1-2016

Framing and Measuring Multi-dimensional Interpersonal Privacy Preferences of Social Networking Site Users

Pamela Wisniewski
The University of Central Florida, pam@pamspam.com

A. K. M. Najmul Islam
University of Turku

Heather Richter Lipford
The University of North Carolina at Charlotte

David C. Wilson
The University of North Carolina at Charlotte

Recommended Citation
Wisniewski, Pamela; Islam, A. K. M. Najmul; Richter Lipford, Heather; and Wilson, David C. (2016) "Framing and Measuring Multi-dimensional Interpersonal Privacy Preferences of Social Networking Site Users," *Communications of the Association for Information Systems*: Vol. 38 , Article 10.
DOI: 10.17705/1CAIS.03810
Available at: http://aisel.aisnet.org/cais/vol38/iss1/10

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

Framing and Measuring Multi-dimensional Interpersonal Privacy Preferences of Social Networking Site Users

Pamela J. Wisniewski
The University of Central Florida
College Engineering and Computer Science
Harris Corporation Engineering Center
pam@pamspam.com

A. K. M. Najmul Islam
University of Turku, Finland
Information Systems Department

Heather Richter Lipford
The University of North Carolina at Charlotte
Software Information Systems Department

David C. Wilson
The University of North Carolina at Charlotte
Software Information Systems Department

Abstract:

In this paper, we focus on interpersonal boundary regulation as a means to balance the tradeoffs between engaging with others and protecting one's privacy on social networking sites (SNSs). We examine boundary regulation from the combined perspectives of SNS design and end user behavior; we conduct a feature-oriented domain analysis of five popular SNS interfaces and 21 semi-structured SNS user interviews. We use this information to construct a taxonomy of 10 types of interpersonal boundaries SNS users regulate to manage their privacy preferences. We then develop and validate scales to operationalize these 10 boundary types to measure the multi-dimensional nature of SNS users' privacy preferences by using a sample of 581 Facebook users. Our taxonomy provides a theoretical foundation for conceptualizing SNS user privacy, and our scales provide a more robust way to measure SNS users' multi-faceted privacy preferences.

Keywords: Interactional Privacy, Social Network Sites, Interpersonal Boundary Regulation, Information Disclosure.

This manuscript underwent editorial review. It was received 09/29/2015 and was with the authors for 1 month for 2 revisions. Dirk Hovorka served as Associate Editor.

1 Introduction

Privacy "paces and regulates" our interactions with others by adjusting the level of access we give of ourselves to others and is an integral part of our self-identity, self-esteem, and our overall wellbeing (Altman, 1975). According to Altman's (1975) seminal work *The Environment* and *Social Behavior*, privacy is a process of interpersonal boundary regulation and the key to maintaining appropriate levels of interaction in one's social environment. This conceptualization of privacy has been beneficial in understanding privacy preferences and social outcomes in physical environments (Harris, Brown, & Werner, 1996; Kaya, Webb, & Miller, 2005; Kaya & Weber, 2003) and has more recently been applied to the context of virtual social environments, such as social networking sites (SNSs). For example, Petronio's communication privacy management (CPM) theory on the dialects of disclosure (2002) extends Altman's metaphor of privacy as boundary regulation, and scholars have applied it to blogs and SNSs (Child, Haridakis, & Petronio, 2012; Child, Pearson, & Petronio, 2009; Child, Petronio, Agyeman-Budu, & Westermann, 2011; De Wolf, Willaert, & Pierson, 2014). Several studies in the computer-mediated communications (CMC) and human-computer interaction (HCI) fields have leveraged Altman's definition of privacy to help understand information disclosure behaviors and outcomes in SNSs (Lampinen, Lehtinen, Lehmuskallio, & Tamminen, 2011; Palen & Dourish, 2003; Stutzman & Hartzog, 2009; Stutzman, Vitak, Ellison, Gray, & Lampe, 2012; Tufekci, 2008; Wisniewski, Knijnenburg, & Lipford, 2014).

In contrast, information systems (IS) field has traditionally taken a different approach to conceptualizing privacy by using privacy concern as a proxy measure for information privacy and examining it as a mediating factor between information privacy antecedents and outcomes, such as behavioral reactions, trust, and regulatory actions (Anton, Earp, & Young, 2010; Dinev & Hart, 2006; Hui, Teo, & Lee, 2007; Malhotra, Kim, & Agarwal, 2004; Pavlou, Liang, & Xue, 2007; Smith, Dinev, & Xu, 2011; Smith, Milberg, & Burke, 1996; Son & Kim, 2008). Several IS privacy frameworks have resulted from researchers' trying to understand consumer disclosure behaviors in the context of e-commerce (Dinev & Hart, 2006; Malhotra et al., 2004). With the proliferation of social media and its rising importance in business and IS-related contexts (Kane, Alavi, Labianca, & Borgatti, 2014), more recent IS studies have begun to examine the role of privacy and information disclosure specifically in SNSs (Li, Lin, & Wang, 2015; Xu, Michael, & Chen, 2013; Zhou & Li, 2014). Even with the different conceptualizations of privacy, one commonality among these different fields, however, is the unilateral emphasis on privacy as it relates to information disclosure. Unlike Altman's original conceptualization of privacy, which encompasses the richer social processes of interacting with others (Altman, 1975), information disclosure represents only one facet of privacy: whether to withhold or disclose private information. We argue that the intense focus on information privacy as opposed to the broader lens of interpersonal privacy limits our overall understanding of privacy in the context of SNSs. For instance, Child and Petronio (2011, p. 35) duly note that "one of the most obvious issues emerging from the impact of social network site use is the challenge of drawing boundary lines that denote where relationships begin and end". As such, one can use social processes, such as friending and unfriending, as mechanisms for regulating interpersonal privacy boundaries in addition to directly managing one's privacy through limiting information disclosures.

We do not adequately understand the subset of mechanisms available for managing interpersonal boundaries in SNSs that inform this broader perspective of SNS privacy. Thus, our main contribution through this work is applying Altman's conceptualization of privacy as a boundary-regulation process (inspired by the CMC and HCI fields) to develop a theoretical framework of SNS privacy. We do this by leveraging established IS methodologies (Gefen, Rigdon, & Straub, 2011; Moore & Benbasat, 1991; Straub, Boudreau, & Gefen, 2004; Strauss & Corbin, 1998) to build our theory and empirically confirm our theoretical framework by operationalizing and statistically validating new scales derived from our qualitative findings. Further, we explore interpersonal boundary regulation as a way to balance benefits and drawbacks that individuals experience when forming and fostering relationships in online social networks. With this paper, we first build a theoretical framework of interpersonal boundary regulation mechanisms that are relevant to SNSs and to better understand how end users employ these mechanisms to manage their social interactions with others. Second, we use this theoretically derived understanding to operationalize new scales, which measure SNS users' multi-dimensional privacy preferences based on their desired levels of privacy. The empirical validation of these scales provides pre-validated measures that future research can leverage.

To do these two things, we first performed a feature-oriented domain analysis (Kang, Cohen, Hess, Novak, & Peterson, 1990) using SNSs as our application domain to identify prominent features that we could leverage for interpersonal boundary regulation. We examined commonalities and variations in the

features available in five popular SNSs: Facebook, MySpace, LinkedIn, Hi5, and Ning (at the time we performed this analysis, Google+ had not yet launched). Second, we conducted 21 semi-structured SNS user interviews to better understand how users actually leverage these interface features and, more generally, how they manage their online social interactions. Combining these two qualitative approaches, we present a taxonomy of 10 distinct types of interpersonal boundaries SNS users regulate to manage their privacy preferences, which fall into five high-level categories: 1) disclosure, 2) relationship, 3) network, 4) territorial, and 5) interactional privacy boundaries. Finally, we operationalized and validated measures for each of the 10 dimensions in the boundary taxonomy through card-sorting techniques (Moore & Benbasat, 1991; Straub et al., 2004) and a confirmatory factor analysis (CFA) on data collected from 581 Facebook users. Our qualitative work provides a deeper, theoretical understanding of interactional privacy in SNSs by examining current SNS interface designs and end user behaviors. Our empirical findings indicate that boundary regulation is a mounting concern for SNS users that, if improved, could serve to enhance SNS users' experience and possibly facilitate stronger connections through online social networking. We also make a methodological contribution by developing scales that future research can use for measuring SNS users' multi-dimensional privacy preferences; these scales extend beyond information privacy concern, which has traditionally been the proxy measure in privacy research (Dinev, Xu, & Smith, 2009; Malhotra et al., 2004; Smith et al., 2011; Xu, Dinev, Smith, & Hart, 2008).

2 Background and Motivation

Interpersonal boundary regulation is a dialectal process in which individuals dynamically change their desire for social interaction and, thus, must continually negotiate their boundaries with others. To do so, they employ different boundary mechanisms, which are behaviors or strategies that help them achieve their desired level of privacy (Altman, 1975). While this conceptualization of privacy is very applicable to inherently social environments such as SNSs, Altman's original work on privacy focuses specifically on social behavior in relation to the physical environment. Therefore, the primary mechanisms he identifies in his work to negotiate boundaries include personal space, territory, verbal behavior, and nonverbal behavior. However, these mechanisms do not readily translate into virtual environments such as SNSs. For example, boundary mechanisms, such as eye contact and body language, are not an option in SNS interfaces. Moreover, new SNS boundary mechanisms have emerged that are not often employed in the physical world. It would be awkward, for instance, to explicitly unfriend someone in person. Therefore, we first define the set of boundary mechanisms available and applicable to SNS environments so that we can further contextualize Altman's conceptualization of privacy to SNS environments. Specifically, we are interested in identifying the interface controls SNSs provide so that users can manage all aspects of their social relationships. Also, we are interested in understanding if and how SNS users leverage these interface controls as mechanisms for interpersonal boundary regulation.

Second, we both broaden and integrate the current conceptualizations of SNS privacy in academic research. Researchers often define SNS privacy as "the ability of individuals to control when, to what extent, and how information about the self is communicated to others" (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011). Such a definition emphasizes privacy's informational aspects over its interactional aspects. For example, individuals may feel comfortable disclosing personal information in their social networks but may not be comfortable accepting friend requests from strangers. Both of these desires for open information disclosure and intimate relational connections are aspects of personal privacy preference. Yet, much of the research in SNS privacy tends to focus on the former.

In IS privacy research, early work focused primarily on consumer information privacy. For example, Smith et al. (1996) developed the concern for information privacy (CFIP) scale in the context of offline direct marketing, consisting 15 items and four dimensions: collection, errors, secondary use, and unauthorized access to information. Malhotra et al. (2004) developed the Internet users' information privacy concerns (IUIPC) scale using three dimensions: collection, control, and awareness of privacy practices. More recently, Anton et al. (2010) reported a scale of IUIPC using access/participation, information collection, information storage, information transfer, notice/awareness, and personalization. Similarly, these conceptualizations of privacy have also moved away from Altman's (1975) and Petronio's (2002) conceptualizations of privacy as an "interpersonal event" enmeshed in relationships for optimally regulating one's social interactions through a process of boundary negotiation to a definition more focused on limiting information disclosure or increasing privacy control (Tufekci, 2008; Xu, Dinev, Smith, & Hart, 2011). However, privacy, as a construct for social contexts, extends beyond information disclosure decisions, to a broader range of social interactions that require regulating interpersonal boundaries.

As such, our work acknowledges that the nature of interpersonal boundary regulation is dialectical, where individuals negotiate with others to open and close their boundaries to achieve their desired level of privacy. In this way, privacy is an optimization process for achieving one's desired level of social interaction instead of a means of social withdrawal. Second, our work illustrates how interpersonal boundary mechanisms are not confined to one's "privacy settings" and how interactional privacy regulation extends beyond the decision whether or not to disclose personal information. Given this lens of privacy as interpersonal boundary regulation, we describe the methodology for creating a taxonomy, which provides a theoretical framework to understand the multi-faceted nature of SNS privacy boundaries and for operationalizing scales to measure SNS users' privacy preferences based on this theoretical framework.

3 Boundary Taxonomy

The most important and basic step in conducting any form of scientific inquiry involves ordering, classifying, or otherwise grouping the objects or phenomena under investigation (Carper & Snizek, 1980). Researchers have suggested taxonomy, defined as "theoretical study of classification, including its bases, principles, procedures and rules" (Simpson, 1961, p. 11), as an important first step toward developing constructs (Doty & Glick, 1994). Taxonomy helps one identify dimensions and similarities and difference among these dimensions (Bailey, 1994). Thus, we first develop a boundary taxonomy for the SNS context.

3.1 Methodology

We combined two qualitative approaches to develop a taxonomy of SNS interpersonal boundary types. First, we conducted a feature-oriented domain analysis (Kang et al., 1990) across five popular SNSs: Facebook, MySpace, LinkedIn, Hi5, and Ning. Features relevant to interpersonal boundary regulation were abstracted and conceptually grouped to lay the foundation of our taxonomy. Next, we conducted semi-structured interviews with SNS users on how they used these features and how they managed their social interactions online. For instance, we asked participants how they handled friending and unfriending, overlapping social circles, personal disclosures, updates from others, and interpersonal conflicts in their SNSs. Boundaries are often the points where interpersonal conflicts occur; therefore, understanding the types of conflicts that SNS users experienced helped us identify the different types of privacy boundaries SNS users had to manage. For the interviews, we recruited participants via postings on Facebook and through email. We asked the participants to base their responses on actual past experience. We conducted the interviews via Google Voice, Skype, or email, transcribed them using InqScribe, and qualitatively coded them using Atlas.ti 5.5. We first used open coding (Strauss & Corbin, 1998) to conceptually group the SNS interface features by the type of interpersonal boundary they supported. We then used these codes as a priori codes (Lewins & Silver, 2007) for coding our interview data. We continued interviewing new SNS users until we had achieved saturation in our a priori codes (Strauss & Corbin, 1998). Throughout this paper, we use pseudonyms to protect the anonymity of our participants.

3.2 Participants

We collected interview data from 21 SNS users (10 females and 11 males). We audio recorded 13 interviews that averaged 58 minutes each. We completed eight interviews via email with follow-up questions totaling 50 single-spaced pages (out of over 200 pages overall). The users' average age was 36 years old (ages ranged from 21 to 60). Participants primarily used Facebook, with 16 participants logging in daily and four participants logging in weekly. Six participants reported using MySpace weekly to annually, and three said they used to have MySpace accounts but had deactivated them. Eight participants reported having Twitter accounts and six participants had LinkedIn accounts. Participants also reported a variety of other sites, including Ning, Hi5, LibraryThing, Shelfari, Xanga, and others. We interviewed one participant who was not a member of any SNS. The interviews confirmed our a priori codes (territorial, disclosure, and relationship boundaries) and identified additional, emerging boundary mechanism categories (network and interactional boundaries). They also led us to build a hierarchical taxonomy by identifying key dimensions in each of the categories we present in Section 3.3.

3.3 Boundary Taxonomy Results

Table 1 summarizes the taxonomy of SNS boundary types, and we define each component of the taxonomy in detail in Sections 3.3.1 to 3.3.5. Table 3 summarizes the feature-oriented domain analysis of SNS interface controls that support each of the various boundary types across the five SNSs.

Table 1. Taxonomy of SNS Boundary Types

Boundary type	Dimensions	Definition
Disclosure	Self-disclosure	Regulating what personal information one discloses in one's network
	Confidant-disclosure	Regulating how co-owned personal information is disclosed in one's network by others
Relationship	Connection	Regulating whom one lets be a part of their social network
	Context	Regulating appropriate interpersonal interactions given the unique type of relationship
Network	Discovery	Regulating access others have to one's network connections
	Intersection	Regulating social interactions between connections or groups of connections
Territorial	Inward-facing	Regulating incoming content for personal consumption
	Outward-facing	Regulating semi-public content available through interactional spaces
Interactional	Disabling	Regulating potential interaction through turning on/off interface features
	Blocking	Regulating overall access of one's self to specific individuals

3.3.1 Disclosure Boundaries

Existing SNS privacy literature heavily focuses on disclosure boundaries, otherwise known as personal information privacy (Acquisti & Gross, 2006; Besmer & Lipford, 2010; Christofides, Muise, & Desmarais, 2009; Lampinen et al., 2011; Palen & Dourish, 2003; Stutzman, Capra, & Thompson, 2011; Stutzman, Gross, & Acquisti, 2012; Tufekci, 2008); therefore, disclosure boundaries are also an integral component of our taxonomy. We examined two types of disclosure boundaries: self-disclosure involving private information about one's self and confidant-disclosure boundaries for information that others "co-own" (Petronio, 2002).

Self-disclosure is one of the most supported boundary mechanisms in SNS interfaces (see Table 2 and Table 3) and is often characterized as the "privacy settings" of one's user profile. Because personal information disclosure and privacy settings have both been studied in detail (Acquisti & Gross, 2006; Debatin, Lovejoy, Horn, & Hughes, 2009; Ellison et al., 2011), we highlight two dimensions in which they tend to vary. First is the level of granularity or type of information that one can share with others. Facebook is the most complex in that it allows users to disclose and control more granular boundaries for categories such as biography, website, email address, and eight other categories. The other SNSs had fewer information groupings, which made user profiles chunkier and, thus, self-disclosure boundaries less granular. Second is whom one can share this information with or one's access-level permissions. All SNSs we examined erred on the side of sharing more information to more people by allowing users (often by default) to give access to "everyone" or "all users". However, all five SNSs gave the option for sharing profile information with only "friends" or "connections" in one's network. Facebook gave the most flexibility by giving users the most options for controlling personal information through granularity and access level control by group, network, or individual (Table 2).

Table 2. Self-disclosure Access Level

Access level	Facebook	MySpace	LinkedIn	Hi5	Ning
Everyone	X	X	X	X	X
Friends/connections	X	X	X	X	X
Everyone 18 and older		X			
Friends of friends	X				
Friends and networks	X				
Specific individuals	X				
Only me	X		X	X	X

In terms of self-disclosure boundaries, our participants were unconfident or skeptical about their SNS privacy settings and, thus, tended to not take advantage of the granularity or access levels provided to manage self-disclosures. Seven participants displayed a lack of understanding in their settings or

experienced an accidental, negative disclosure that made them distrust that the settings even worked correctly. For example, Gina (student, 30) said: "I was annoyed that Facebook had my phone number for all my friends and family and their friends and family to see."

Therefore, instead of supplying personal information to the SNS and managing access level, many simply did not supply the information at all:

> *I may show my marriage status and that's about it. I don't think I have ever really thought about how I manage [personal information], I just don't provide it through the social network with any more information than I would give a stranger.* (Larry, software engineer, 54)

Confidant-disclosures occur when a friend or connection posts one's personal information so that it is viewable for others to see, such as tagging pictures of friends or posting otherwise confidential information about another individual. Our past work has shown that such engagement is associated with higher levels of Facebook use and stronger emotional attachment to Facebook. However, Facebook users who have a high level of concern for their personal privacy tend to engage in these types of activities (Wisniewski, Xu, Lipford, & Bello-Ogunu, 2015). Different SNSs have implemented different techniques for managing confidant-disclosures, including access-level manipulation (managing whom can see what), post or comment deletion, untagging, and moderation (Table 3). For instance, at the time of writing, LinkedIn connections were unable to post content on another LinkedIn member's profile with the exception of recommendations, which are moderated by default. Therefore, LinkedIn inherently prevented incidental confidant-disclosures most likely because it is a professional network that values positive self-promotion. In contrast, Facebook has only recently added the ability for users to moderate friends' tags before sharing on their timelines. Therefore, one either has to take action either proactively by setting access-level permissions to prevent confidant-disclosures in one's network or retroactively by deleting or untagging unwanted content after the fact.

While participants generally distrusted SNS privacy settings to manage self-disclosure boundaries, which is consistent with past research (Besmer & Lipford, 2010), they exhibited a general trust towards those in their social networks to not breach confidant-disclosure boundaries. Kristine (author, 37) said: "Most people are pretty good. I think that is…because so many people are friends with people who are family and you know people from high school or whatever.".

Three participants noted using an offline coordination process to gain consensus before tagging pictures of themselves or others. However, a failure to coordinate confidant-disclosures beforehand often led to unintentional interpersonal conflict. We found cases where participants needed to clarify their confidant-disclosure boundaries with others after a breach. When this happened, they would usually delete the information disclosed and privately confront the other person. For instance, Dollie's friend innocently congratulated Dollie on her pregnancy via her Facebook Wall. Dollie had not announced her pregnancy to the majority of her family and friends and was upset by this breach of confidence. As a result, she deactivated her Facebook account for the remainder of her pregnancy. Also, Kristine had to delete a comment from her niece regarding an impending out-of-state move because Kristine's husband had not yet notified his company that he was changing jobs and relocating. Overall, confidant-disclosure boundaries were typically managed reactively after the disclosure of potentially damaging information.

3.3.2 Relationship Boundaries

Relationship boundaries relate to one's deciding whether or not to allow someone to be a member of their social network and subsequently defining the appropriate context for that relationship. While relational boundaries do not tend to fit in the traditional definition of privacy management, we argue that relationship boundaries may be even more important than other privacy boundaries because SNSs implement "friend-based privacy" in that what one shares is directly related to whom one is connected. However, past research suggests that SNS users tend to "hyperfriend": that is, accept friend requests from individuals who are not real friends (Fono & Raynes-Goldie, 2006). Therefore, approximately only 25 percent of our online connections represent true friendship (Zinoviev & Duong, 2009), which allows "weak ties" and true friends to be part of our inner circles (Boyd, 2006). According to Boyd (2004), SNSs typically simplify relationships to a "binary" dimension of friend or not friend. Due to this collapsed context (Grudin, 2001), SNS users often allow acquaintances, family, friends, and coworkers the same level of access, which breaks down the dialectical nature of boundary regulation. Since each context may have different and, at times, mutually exclusive behavioral requirements, acting accordingly in a single space has become a challenge (Tufekci, 2008).

The SNSs we examined are all reciprocal networks (where a friend request must be accepted for a connection to be formed); however, SNSs such as Twitter and Google+ allow unilateral relationships. Therefore, the primary mechanisms for managing relationship-connection boundaries across the five SNSs included: changing access-level permissions for friend requests, denying friend requests, and unfriending (Table 3). These SNS interfaces differed on the access-level options users could specify for allowing friend requests. For instance, Facebook allowed SNS users to specify whether or not "everyone" or "friends of friends" could request friendship, while MySpace users could only specify "everyone", "18 or older", and "bands, filmmakers, or comedians". All SNSs provided controls for denying a friend request or unfriending, but social cues discouraged such actions. For instance, Facebook asked users to "confirm friend" or "quietly ignore" a friend request. In addition, the SNSs often visually encouraged friendship by emphasizing accepting over denying a friend request. Conversely, they de-emphasized interface controls for unfriending, which were even difficult to find.

Our participants had very different boundary permeabilities (Petronio, 2002) or levels of relationship connection openness when choosing whom to friend. Three distinct relationship connection boundary profiles emerged. We validated participants' perception of their boundary permeability and found that their descriptions were congruent based on the average number of friends in each of these groups. The first group (three participants who averaged 51 friends each) only allowed intimate relationships into their networks and were very quick to reject friend requests and remove friends should they cause them problems. For example, Dollie (mother, 34) said: "No strangers, no colleagues, and no immediate family [are in my network]. I wanted to keep it just for friends, close friends not usually anyone that I don't typically associate with on a daily basis.".

The second group (nine participants who averaged 266 friends each) had moderate relationship boundaries by allowing friends to acquaintances into their networks. They were able to articulate criteria for accepting or ignoring a friend request but most (7) rarely unfriended anyone ever. For example, Fred (sales manager, 33) said:

> *First, if I do not know the person, second if is someone that I would believe to be inappropriate due to the relationship I had with them, third if I just do not like them. I do have one that I would not consider a friend due to a falling out, I keep him out there to make sure he is not saying anything bad about my wife, my friends or me.*

Finally, the third group (eight participants who averaged 626 friends each) had very open relationship connection boundaries and allowed anyone from friends to strangers into their networks. This group had a very large deviation in the average number of friends with friend counts ranging from 69 to 1554. Some participants had very open relationship connection boundaries because they needed resources for games that they played online. Four participants attributed their large networks to their using their social networks for both personal and professional reasons. These participants had an average of 1,045 friends. For example, Lynn and Tyrone were both photographers who posted many of their clients' pictures on Facebook for self-promotion. Kurt (32) was a dating coach who often got clients (and picked up girls) through Facebook. Therefore, his very social profession was intertwined with his large social network. He said:

> *I don't have that much of the defined boundary between my personal life in my professional life. In fact, for the dating coach thing part of it is kind of living the life style. Being that guy, if you will. To an extent, it is a little like being a little bit of a celebrity.*

Kristine (37) was an author who said she "blanket accepts" friend requests from almost anyone because they could be one of her fans.

> *When I get a friend request, they might be somebody who has read my book or they might be some random troll or who knows. So I pretty much just blanket accept everyone and just kind of assume that they read my book.*

In addition to accepting almost all requests for friendship, these individuals also rarely unfriended, which left their networks large, open, and often unwieldy. More generally, regardless of boundary permeability, we found that unfriending was rare, if at all. Of our SNS users, 75 percent said they rarely unfriended anyone (1-3 people), while 24 percent had never unfriended anyone. For example. Becky (teacher, 29) said: "I've remained friends with some people because I know it would cause more of an issue if I unfriended them then if I just left them on there.".

In general, individuals let people into their inner circles relatively easily and had a hard time removing them. Therefore, they did not effectively leverage relationship connection boundaries in regulating interpersonal boundaries.

Relationship context defines the appropriate level of interaction with a connection once a relationship connection has been formed. The interaction one desires with a spouse, for instance, is different than interaction that would be considered appropriate with a stranger. Three main groups of SNS friends have been delineated through past research: true friends (strong ties), acquaintances, and random acquaintances (both weak ties) (Zinoviev & Duong, 2009). All the SNSs examined, except Ning, allowed users to label friend groups for personal use (e.g., "college buddies" or "co-workers"). Boyd (2006) describes this as "overloading" friends to represent different contexts than just friendship. However, only Facebook lets users leverage those groups to set access levels for sharing items such as status updates, contact information, and pictures.

Relationship context boundaries were problematic for our SNS users. Only 33 percent of the users separated friends into groups, and only two participants actually used these groups to manage access-level privacy. Individuals characterized grouping friends by type of relationship more as a strategy to 1) organize friends to reference later and 2) to manually use the list to send directed communications to a group. However, grouping rarely led to contextual interactions, such as posting status updates directed to a specific group. Individuals felt that using this mechanism was a hassle or did not trust their own abilities to categorize and keep groups up-to-date. In addition, many of the participants did not know they could use groupings, such as Facebook friend lists, to post directed status updates or pictures. For example, Tia (administrative assistant, 37) said:

> *I've never done that because I did not know that I could…If I am addressing a group, it is a general message to everybody, on my wall anybody can see it, but if I say, "what's up PDC",... the people and that group know who I'm talking about.*

Because interactions lack context, SNS users tended to make those interactions more generic and less personalized and, thus, lost an aspect of intimacy. For example, Gordon (restaurant manager, 48) said:

> *When I am feeling sort of depressed, and I just want to share but I don't want to share it with everybody. That is where it becomes difficult because you want to share like you are sharing with your friends but not everyone is on equal footing…. I find myself sort of trying to speak in code sometimes or just hold back what I really am feeling.*

As a result, some individuals experienced a sense of loss of their authentic selves in their SNSs. This was especially true for the four participants who used their networks for professional and personal use and is likely a key factor for lack of intimacy experienced in SNSs.

3.3.3 Network Boundaries

An individual's social network structure contains cliques—groups of people whom all know each other—and independent sets of friends that have no common connections (Scott, 2009). SNS users not only have to manage their boundaries with individual connections but also the transitive interactions that may arise between them. Network boundaries are mechanisms to demarcate one's connections or groups of connections and serve to monitor interactions between one's different circles of friends. Traditional social networks are physically spread out and linkages between individuals are implicit or hidden to others; therefore, they are more easily managed. For example, estranged friends are invited to dinner on separate occasions. Online, those connections become transparent (Boyd & Ellison, 2007) and physical distance is removed, which makes one's network less manageable and affords potential social interaction between otherwise unconnected parties. We uncovered two types of network boundaries in our study: network discovery and network-intersection boundaries. Network discovery deals with how individuals manage the exposed, traversable nature of their networks to regulate overall access by others. Network-intersection boundaries are used to regulate how different social circles in one's network overlap and interact.

We concluded that SNSs lack controls for flexible management of network discovery boundaries. Only Facebook (Table 3) provided a separate functionality for being able to customize who can see one's friend list with the following levels of access: "everyone", "friends of friends", "friends only", or specific individuals. However, Facebook users could not partially hide subsets of friends from others. The other SNSs were even less flexible: they tied one's friends list to one's entire profile visibility. Hi5 and LinkedIn gave a

binary option to show or hide connections for everyone, and MySpace did not provide the option at all. Thus, managing discovery of others in one's network was only available to users at a very high level or not at all.

Serendipitously discovering unknown relationships or, as Allen described it, "six degrees of separation" tended to outweigh potential risks for SNS users when it came to network-discovery boundaries. Six participants shared stories about how they were able to discover interesting linkages between their friends or use connections to find others. When network discovery was an issue, it was typically others' exploiting one's network. In particular, Lynn (photographer, 30) and Tyrone (photographer, age 31) also had competitors in their networks. As Lynn said:

> *Every time I take pictures of someone and tag them in it, he [competitor] will friend request that person to his page, and that bothers me because it feels a little stalker-ish. He is trying to build his numbers to get a bigger name on his page.*

Self-image was also a network-discovery issue for three participants who were mindful of whom was visible in their networks because it could be perceived as a bad reflection on them. However, only two participants had ever hidden their friend list; Alana had done so accidentally.

The same lack of interface flexibility was true for managing network-intersection boundaries. Similar to relationship-context boundaries (Table 3), the only support we found for network-intersection boundaries was the ability to create and leverage friend groups or lists. Again, only Facebook provided a mechanism for posting information to specific groups so that only members of that group can interact within that thread. In this case, Facebook users could prevent groups of friends from overlapping for narrowed contexts, but they still had no way to manage social interactions between individuals outside the context of a specific post. Overall, SNS network-boundary management tended to be unavailable or all-or-nothing in nature.

Network-intersection boundaries tended to be a bigger concern for our participants than network-discovery boundaries due to high potential for conflict and lack of control. As Steve (minister, 57) said: "I have friends and relatives who are at extreme opposites religiously and politically…It is very likely to lead to a heated, sometimes hateful confrontation between my 'friends'. I really don't like that!".

Regina (HIV awareness coordinator) managed how her friends interacted in her network by personally moderating conversations when they got out of hand. She said: "I am 60 years old, so I can pull out the grandma and say 'you know, that really wasn't okay'. Sometimes it works, and sometimes there is a bit of huff but people do pipe down at that point.".

Due to the lack of interface controls for regulating network-intersection boundaries (and awareness of how to use controls that were available), participants did little to manage network boundaries in the interface, which often resulted in unwanted interactions and conflicts between one's friends.

3.3.4 Territorial Boundaries

Territorial boundaries involve using "places and objects in the environment" to personalize or mark "ownership, possession, and occasional active defense" (Altman 1975, p. 104). We found two types of SNS territories in use: inward-facing territories and outward-facing territories. Inward-facing territories such as Facebook's "news feed," LinkedIn's "updates," Hi5's "network updates," MySpace's "stream," and Ning's "latest activity" served as spaces for personal consumption of updates from connections or friends (e.g., photo uploads, links, videos, new connection updates). These SNSs provided three mechanisms for managing inward-facing territories: filters, preference settings, and hiding (Table 3). Filters provided a temporary territorial boundary; managing preference settings gave users more permanent control over what appeared and from whom. Hiding generally occurred on a real-time basis and was specific to all content from a specific individual. Unhiding an individual required additional work of modifying account settings. The five SNSs were inconsistent as to the filters and preference settings provided through their interfaces. For instance, MySpace allowed users to set a preference for what type of friend updates they would like to see in their Stream. In contrast, Facebook did not provide any preference settings to permanently manage news feed updates by type.

Participants perceived inward-facing territories such as Facebook's news feed as ephemeral in nature, impersonal (not directed at them), and private (not seen by others); therefore, inward-facing territorial management was not a high priority. Thus, the predominant mechanism for managing inward-facing territorial boundaries mentioned by 43 percent of our SNS users was to skim or ignore content, which was

possibly a coping mechanism they developed to manage sheer information overload (Wisniewski, Lipford, & Wilson, 2012). As Larry (software engineer, 54) said: “It’s just easier for me to just ignore it. It's kind of like the same thing people get all irritated about strip joints. Hey if you don't like it, don't go in.”.

When managing inward-facing territories, our participants differentiated between hiding games and hiding people on Facebook. While almost half of our participants said they hid Facebook games from their news feed, only 29 percent said they hid individuals from their feed. In some cases, participants chose to hide content from people they wanted to have access to but did not want to be reminded of on a regular basis. Therefore, participants had to actively engage with these individuals or be the recipient of direct communication from the hidden friend in order to have continued interaction through the SNS. As Tia (administrative assistant, 37) said: “I don’t unfriend them but I just cut off their news feed, and if I am that interested in what she is doing then I’ll just go to her page and check her out.”.

Interestingly, hiding tended to be a fairly permanent boundary in that once an individual was hidden, they were rarely unhidden again in the future. Furthermore, four participants expressed confusion over their ability to regulate their inward-facing territories in SNS environments by saying they were unaware or unsure about how to hide someone from their news feeds.

Outward-facing territories, such as Facebook’s wall or timeline, are dynamic representations of users and their SNS activities. We classify such outward-facing territories as secondary or “interactional” territories that are a “blend of public or semipublic availability and controlled by regular occupants” (Altman, 1975, p. 114). Because these secondary territories are bridges between private and public, boundary confusion often occurs. As Altman (1975, p. 114) states, “Secondary territories, because of their semipublic quality often have unclear rules regarding their use and are susceptible to encroachment by a variety of users, sometimes inappropriately and sometimes predisposing to social conflict”. Because technology fully mediates social interactions in SNSs, confidant-disclosures are strongly linked to outward-facing territories. Generally, the same mechanisms that SNS users use to form outward-facing territorial boundaries are the same ones they use to create confidant-disclosure boundaries (Table 3). The distinction in practice is that confidant-disclosure is focused on one individual’s disclosing someone else’s private information. Outward-facing territorial boundaries can be violated when one’s friends post any type of undesirable content in one’s virtual spaces. To illustrate the difference, Tia deleted profanity from her Facebook wall because her outward-facing territorial boundary preference was to not let her friends post obscene content for others to see. However, this content had nothing to do with Tia herself. However, when Dollie deleted a friend’s congratulatory comment on her pregnancy (before she shared the news publicly), she implemented both an outward-facing territorial boundary and a confidant-disclosure boundary.

With our participants, outward-facing territorial boundary regulation was characterized by quite a bit of uncertainty and implied lack of control, which is consistent with past research that has identified spatial and temporal boundaries (Tufekci, 2008) as a challenge in these virtual spaces. Because participants did not have a good sense of their audience and knew that any interaction that occurred could potentially draw attention in the future, participants struggled to maintain appropriate boundaries and expressed frustration and dissatisfaction in SNS use. As Alana (substance abuse counselor, 28) said: “I hate Facebook. I don’t trust it, and I have no idea what I’m really sharing and who’s seeing what.”.

When asked how they managed content shared with others in their network, 29 percent of our participants immediately started talking about how they managed information contained in their user profile instead of what their friends were sharing outwardly, which suggests that individuals felt like they had control over personal information in their profiles but rarely thought about managing how information and interactions were shared through their virtual territories even when SNSs provided the functionality to do so. In the few cases where individuals manipulated access-level viewing permissions, they generally did so to hide pictures (three participants) or posts from others to avoid conflict (two participants). As Allen (technical services, 31) said:

> *My wife and I have had to make her father unable to see any of our photos of a niece, since she is black. [Her] dad is a horrible racist so his knowing about her would negatively affect her and no one deserves that.*

Many participants did report removing content from their virtual territories: 52 percent of our participants said they have deleted a post or comment while 38 percent had untagged themselves in a photo. Reasons for doing so included avoiding conflict, filtering out negativity, protecting personal information, or maintaining a certain self-image. However, some participants expressed discontent because they felt they

always had to monitor their outward-facing territories to delete unwanted content immediately to minimize any potential damage. Three participants who were both MySpace and Facebook users said that they wished Facebook also allowed moderation. As Tia (administrative assistant, 37) said: "I did not accept a friend request from an ex [on Facebook]…not knowing what he was going to say. If I could monitor what he would post before he could post it, then we could have been friends.".

For inward- and outward-facing territories, we found a general frustration with the boundary-regulation process even though interface controls were available for boundary management. Inward-facing territories were just too time consuming to manage, while participants felt they lacked control over their outward-facing territories.

3.3.5 Interactional Boundaries

Interactional boundaries limit direct access to oneself and, thereby, avoid the need for other types (i.e., relational, territorial, etc.) of boundary negotiation with others. SNS users can erect interactional boundaries by disabling interactive interface features, such as one's Facebook wall or MySpace comments. For example, in "things others share", Facebook allowed users to specify whether or not one's friends "can comment on posts", "suggest photos of me to friends", and "friends can check me into places". Disabling represented a temporary or permanent withdrawal from interaction generally that was not directed at any individual. Five participants said they had disabled features in the past including their wall (two), picture tagging (one), and chat (two). As Allen (technical services, 31) said: "I do not feel safe or trustful of [people] to NOT post bad things on my statuses and photos. I turned off my wall on Facebook as a result.".

Disabling interaction was usually associated with a sense of mistrust of one's network and a high desire to control one's outward-facing territories. In the case of chat, individuals tended to disable chat temporarily to limit interruptions but turned it back on when they welcomed the interaction. However, five participants were unaware or had never thought about disabling interactional features of the interface, while Nelson had accidentally disabled his Facebook wall.

The most drastic form of interactional boundary management is blocking. When one blocks another user, that user cannot view or contact that person at all. In this way, blocking is a means to directly cut off access to oneself from a specific other and, therefore, is often personal when used. LinkedIn is unique that it did not provide any controls for interactional boundary regulation because, perhaps, it targets business professionals and so limits interactions (Table 3). Individuals who implemented blocking interactional boundaries tended to have past negative experiences with an individual and wanted to avoid confrontation and potential future drama. Four participants blocked others due to extreme conflicts, stalking, or "just being nosey". Three participants reported blocking due to spam. But most had never blocked anyone because they never felt "uncomfortable enough" to do so or in fear of being rude. As Lynn (photographer, 30) said:

> *I'm not good with confrontation, so I just [unfriended] him, but I'm struggling with trying to block him because he can still see my pictures. I don't want to be rude to him, so I'm struggling with do I just be rude or do I just let it go? I don't know.*

According to the participants, social norms and feature awareness problems were the primary reasons they did little to create interactional boundaries using SNS interface controls. Users only overcame these two obstacles when extreme negative experiences motivated them to reassess interactional boundaries. It is also possible that such boundaries are rarely implemented because creating them to avoid negative interactions also removes any potential for future positive interactions.

Table 3. SNS Interface Supported Boundary Mechanisms

Boundary type	SNS interface controls	Facebook	MySpace	Hi5	LinkedIn	Ning
Disclosure boundaries: managing personal information						
Self-disclosure	See Table 2					
Confidant-disclosures	Access-level settings	X	X	X		X
	Delete posts or comments	X	X	X	X	X
	Untagging	X	X	X		
	Moderation		X	X	X	X

Table 3. SNS Interface Supported Boundary Mechanisms

Relationship boundaries: managing one's interpersonal interactions						
Connection	Access level—friend request	X	X	X	X	
	Deny friend request	X	X	X	X	X
	Unfriend/remove connection	X	X	X	X	X
Context	Group labeling	X	X	X	X	
	Group management	X				
Network boundaries: managing interactions between one's connections						
Discovery	Access level—friend list	X				
	Access level—profile		X	X		X
	Hide connections		X	X	X	
Intersection	See relationship context above					
Territorial boundaries: managing one's virtual spaces						
Inward facing	Filters	X	X	X	X	
	Preference settings		X	X	X	
	Hiding	X	X		X	
Outward facing	See confidant-disclosure above					
Interactional boundaries: managing access to self						
Disabling	Search (finding you)	X				
	Posts/commenting	X	X	X		
	Tagging	X				
	Friend requests			X		
	Chat	X	X			X
Blocking	Blocking	X	X	X		X

4 Privacy Preference Scale Development and Validation

4.1 Methodology

After we built the taxonomy of different privacy boundary types, we developed scales to measure users' preferences regarding each. We operationalized the measures to reflect Altman's (1975) definition of desired privacy level or the optimal privacy level an individual strives to achieve when interacting with others. To clarify, "optimal" privacy, as Altman defines, is not a state of being more closed to others but instead one's ability to achieve their desired privacy level, which varies from person to person. In psychology, researchers have developed similar multi-dimensional scales to capture individual's desire for privacy in offline contexts and emphasized that "it is not assumed that all individuals with a strong desire for privacy desire all forms of privacy equally" (Harrison, 1993, p. 10). Similarly, our work allows an individual's desire for privacy to vary across the ten boundary types. First, we measured SNS users' desire for privacy across the ten boundary types in our taxonomy. To do this, we first compiled a list of initial item pools to measure each dimension based on quotes from interviews and reviewing the literature. We simplified the item wordings and removed redundant items. Following the "rule of three" (Freeze & Raschke, 2007), we created three items to measure each of the ten boundary types. To pre-validate these measures (10 dimensions x 3 items = 30 items) for discriminant validity, we used card-sorting (q-sorting) techniques (Moore & Benbasat, 1991; Straub et al., 2004). We validated the scales by conducting a partial least squares (PLS) confirmatory factor analysis (CFA) (Gefen & Straub, 2005) on a data set of 581 Facebook users.

4.2 Participants

We developed our scales in two stages: 1) pre-validation and 2) validation. To pre-validate measures for face validity, we recruited 71 participants through messages posted on the primary researcher's Facebook

timeline. To empirically validate our scales on a large-scale, we launched a Web-based survey through Survey Share and recruited 581 active Facebook users over the age of 18. We recruited participants via snowball sampling (Babbie, 2004) seeded through a random sample of university email addresses, the primary researcher's personal SNSs, email, and the Craigslist's volunteer's message board. We incentivized participation through a drawing of four Amazon gift certificates. Each participant who opted in received one drawing entry. As an incentive to share the survey, participants received one additional entry (up to 25) for each successful referral.

4.3 Pre-validation Procedure and Results

We performed five rounds of card sorting to iteratively improve the face validity of our scale items. We asked participants to electronically sort items into pre-defined categories using OptimalSort from OptimalWorkshop.com (OptimalWorkshop.com, n.d.). After each round of card sorting, we revised scale items and recruited new participants for subsequent rounds. For rounds one through four, we gave participants all ten dimensions at once to categorize. However, based on participant feedback, they were overwhelmed by the large number of categories. Therefore, in the fifth card sorting round, we gave four separate groups of participants six categories each that overlapped between the four groups. Table 4 presents the accuracy (based on hit rates) for each of the five rounds: the table shows general improvement with each iteration. For round five, the individual accuracy rates for the four separate groups were 71, 79, 77, and 92 percent; the average accuracy rate across these four groups is shown below for the final round. Overall, the accuracy rates in round five suggested adequate initial construct validity for SNS desired privacy level so that we could move forward.

Table 4. Card-sorting Accuracy Rates

Round	Accuracy rate	Number of participants
1	53%	6
2	71%	5
3	69%	10
4	71%	10
5	79%	40

4.4 Confirmatory Factor Analysis Results

To empirically validate the scales, we conducted a CFA to confirm the construct reliability of our measures (Cook & Campbell, 1979). We tested for internal consistency by examining if all items had statistically significant factor loadings and exceeded a threshold value of 0.7 (Fornell & Larcker, 1981). The composite reliability (CR) values were all greater than 0.80 (Nunnally, 1978), and average variance extracted (AVE) for the constructs were all above Fornell and Larcker's (1981) criterion of 50 percent. Table 5 provides item wordings and psychometric properties of each construct. As Table 5 shows (denoted by a *), only three items had loadings less than 0.70. However, we decided to retain these items as the AVEs and CRs of the constructs passed the respective reliability tests.

Table 5. Scale Items and Psychometric Properties

Scale items	Item loading	Composite reliability	AVE
Self-disclosures		**0.81**	**0.68**
1. I do not want to post very intimate things about myself on Facebook.	0.77		
2. I want to share only minimal information about myself on Facebook.	0.88		
3. I want to be able to choose what to share and what to hold back on Facebook.	0.64*		
Confidant-disclosures		**0.86**	**0.76**
4. I do not want my friends to tag me in photos or posts without my permission.	0.61*		
5. I want to limit what personal information my friends share about me on Facebook.	0.87		

Table 5. Scale Items and Psychometric Properties

6. I want my Facebook friends to keep personal information they know about me between us.	0.87		
Relationship connection		**0.86**	**0.68**
7. I only want people in my Facebook social network who I associate with on a regular basis in real life.	0.78		
8. I do not want to have Facebook friends who are no longer real friends.	0.87		
9. I only want to accept intimate friends and family members as Facebook friends.	0.83		
Relationship context		**0.83**	**0.62**
10. I want to make a distinction between my friends based on the type of relationship I have with them. For example, family, friends, co-workers, etc.	0.78		
11. I want my interactions on Facebook to be different between me and a close friend than they would be with an acquaintance.	0.84		
12. I want my one-on-one interactions on Facebook to be appropriate and unique based on my relationship with that specific person.	0.74		
Inward-facing territorial		**0.84**	**0.73**
13. I want to pick and choose what kinds of updates show up in my news feed.	0.68*		
14. I want to decide whose updates show up in my news feed.	0.84		
15. I want to hide news feed updates from others that I would rather not see.	0.88		
Outward-facing territorial		**0.82**	**0.60**
16. I want to remove any content I do not want from my timeline/wall.	0.71		
17. I want to manage everything that shows up on my timeline/wall for others to see.	0.83		
18. I want to approve all content before it is posted to my Facebook timeline/wall	0.84		
Network discovery		**0.91**	**0.78**
19. I do not want others to have access to my friends through my Facebook friend list.	0.88		
20. I want to restrict others in my network from being able to see who I am and am not friends with on Facebook.	0.91		
21. I want to hide my friend list so that others cannot browse my Facebook friends.	0.86		
Network intersection		**0.88**	**0.72**
22. I want to avoid letting specific groups of friends interact with each other on Facebook.	0.88		
23. I want to keep my different social circles separate from each other on Facebook.	0.83		
24. I want to moderate how my different groups of friends interact with one another on my Facebook page.	0.84		
Interactional disabling		**0.83**	**0.62**
25. I want to be able to turn off chat, my wall, or other Facebook features that allow others to interact with me anytime they want to.	0.71		
26. I want to disable the ability for my friends to contact me on Facebook when I want to be left alone.	0.82		
27. I want to limit the different ways my friends can communicate with me via Facebook.	0.84		
Interactional blocking		**0.83**	**0.62**
28. I want to prevent some people on Facebook from having any access to me what-so-ever.	0.81		
29. When I do not want to interact with someone anymore, I want to be able to sever all contact with them on Facebook.	0.78		
30. I want to block certain people from finding me or knowing what I am up to on Facebook.	0.77		

Table 5. Scale Items and Psychometric Properties

* Denotes items with factor loadings < 0.70 threshold

To ensure discriminant validity, the square root of the variance shared between a construct and its measures should be greater than the correlations between the construct and any other construct in the model (Campbell & Fiske, 1959). As Table 6 shows, this condition was also met in our study, which suggests satisfactory discriminant validity between constructs.

Table 6. Convergent and Discriminant Validity

	BLOCK	CONF	CONN	CONT	DIS	DISC	INTER	IN	OUT	SELF
BLOCK	**0.79**									
CONF	0.48	**0.87**								
CONN	0.33	0.35	**0.82**							
CONT	0.38	0.38	0.27	**0.79**						
DIS	0.52	0.45	0.28	0.44	**0.79**					
DISC	0.47	0.47	0.39	0.42	0.50	**0.88**				
INTER	0.37	0.40	0.39	0.45	0.44	0.56	**0.85**			
IN	0.42	0.37	0.26	0.47	0.42	0.35	0.29	**0.85**		
OUT	0.49	0.54	0.16	0.46	0.45	0.36	0.26	0.54	**0.77**	
SELF	0.23	0.37	0.13	0.33	0.36	0.32	0.12	0.29	0.37	**0.82**

Note: interactional blocking (BLOCK), confidant-disclosure (CONF), relationship connection (CONN), relationship context (CONT), interactional disabling (DIS), network discovery (DISC), network intersection (INTER), inward-facing territorial (IN), outward-facing territorial (OUT), self-disclosure (SELF)

5 Discussion

We combined qualitative and quantitative techniques to develop an in-depth understanding of SNS users' multi-faceted privacy preferences. First, we compared and contrasted the interface controls that support interpersonal boundary regulation and the problems SNS users encounter when they attempt to enact their privacy preferences using the available SNS controls. We accomplished this through a feature-oriented domain analysis to compare and contrast the different interface features available for privacy regulation in five popular SNS websites (Table 3). Then, we conducted 21 semi-structured interviews to understand how SNS users actually used these controls and problems they encountered while doing so. From this analysis, we abstracted our qualitative analyses of the five SNS interfaces and 21 user interviews to create a taxonomy that conceptually grouped users' privacy preferences into ten dimensions based on different aspects of privacy regulation (Table 1). Second, we created and empirically validated scales based on this taxonomy to measure the multi-dimensional nature of SNS users' privacy preferences through a survey-based study of 581 Facebook users. We provide both theoretical implications and practical insights into SNS users' interpersonal privacy preferences and behaviors below. We also discuss the limitations of our work and future research directions.

5.1 Contributions and Implications

Our taxonomy expands the theoretical discourse of personal privacy preference and privacy management in the context of social network sites. At the conceptual level, the taxonomy of privacy boundary types demonstrates that SNS users have a variety of ways to regulate their boundaries through SNS interfaces. For instance, our interview data analysis revealed that different SNS users had distinct profiles for managing their privacy using different boundary mechanisms. Kristine had very open relationship connection boundaries and friended most everyone but managed boundaries with high levels of self-censorship. Lynn, however, balanced her open relationship connection boundaries by closely managing relationship context through groups; therefore, she did not have to self-censor. Alternatively, Dollie kept her relationship connection boundaries very closed and had only a small number of people in her network so that she could disclose whatever "the hell" she wants or "damn please[s]". Instead, it may be that users (e.g., Dollie) manage their privacy boundaries through using closer-knit relationship connections, which

results in a smaller network size and, according to many of our participants, a higher level of intimacy with their connections. In other words, just because some SNS users choose to disclose a large amount of personal information in their social network does not necessarily mean that they are "unconcerned" (Louis Harris & Associates & Westin, 1997; Louis Harris & Associates & Westin, 2003; Westin & Louis Harris & Associates, 1981) about their personal privacy.

Thus, our taxonomy of different dimensions of privacy preference opens up new opportunities for researchers to examine SNS privacy with the broader lens of interpersonal boundary management, which is more appropriate given the complex social interactions that take place via social media. For instance, we found that confidant-disclosures made through apps and tagging on Facebook are related to higher levels of emotional attachment and frequency of use on Facebook. However, privacy-related perceptions, such as privacy concern and the effectiveness of Facebook's privacy policy, are related to lower levels of confidant-disclosures (Wisniewski et al., 2015). We have also conducted some initial work to empirically confirm our qualitative observations that SNS users (on Facebook) have distinct strategies for how they choose to manage their personal privacy. We uncovered six privacy profiles that vary based on the predominant strategies Facebook users use to manage their privacy. For example, "self-censors" manage their privacy by withholding basic contact information and other types of information disclosures, while "selective sharers" disclose more personal information but only to specific audiences (Wisniewski et al., 2014a). Future work can build on our taxonomy to further delineate nuance involved in SNS users' personal privacy preferences and build solutions that support the wide array of privacy-management strategies.

At the empirical level, our validating the desired privacy scales confirms the multi-dimensionality of SNS users' privacy preferences that we observed in building the boundary taxonomy. We created scales that operationalize SNS users' interpersonal privacy preferences by framing these preferences as desired privacy levels (cf. Altman, 1975). Through advanced statistical methods (i.e., a PLS based CFA), we validated that the 10 aspects of SNS privacy exhibited both convergent and discriminant validity. In other words, each of these 10 aspects of SNS privacy preference is related but unique from one another. Therefore, when attempting to understand SNS users' privacy preferences, it is necessary to acknowledge that users' preferences may vary by these different dimensions as Harrison (1993) originally suggested. Thus, only measuring one aspect of privacy preference (i.e., typically information disclosure privacy) provides incomplete information about SNS users' privacy preferences. For example, if we measured Kristine's, Lynn's, and Dollie's privacy preferences (as discussed above) using IUIPC (Malhotra et al., 2004), for instance, only Kristine would have appeared to exhibit privacy preserving behaviors (i.e., self-censorship). However, Lynn and Dollie also enacted their privacy preferences through managing relationship context and relationship connections, respectively.

Additionally, our empirical scale validation from our taxonomy provides researchers a pre-validated tool for measuring the multi-dimensional nature of SNS users' personal privacy preferences and the opportunity to identify salient antecedents and determinants of the same. We have already done some work to this end to show, for instance, that meeting SNS users' desired privacy level for each of the ten privacy boundary types is related to higher levels of social connectedness with one's Facebook friends (Wisniewski, Islam, Knijnenburg, & Patil, 2015). Although the IS privacy field has several frameworks that address information privacy, we demonstrate how our scales are more contextualized to the unique interpersonal privacy boundaries of SNS users and more complete than privacy scales that focus only on disclosure. Yet, this also limits the scales because the specificity reduces the generalizability of our measures. Our goal was to strike a balance between rigor and nuance (Lipford, Wisniewski, Lampe, Kisselburgh, & Caine, 2012) so that future empirical studies on this topic can achieve more meaningful results while maintaining statistical validity. Other researchers may be able to use these scales to identify other key relationships between SNS users' privacy preferences and social-networking outcomes. In some cases, it may make sense to only use a single dimension or subset of the desired privacy scales to conduct an in-depth analysis on understudied areas of interpersonal privacy (e.g., those not related to self-disclosure). For example, it may be interesting to compare the social outcomes for users with varying desired privacy levels for relationship connection and context. Dollie, for instance, had strict rules for relationship connection, while Lynn managed her privacy through the contexts of her relationships, which allowed for a larger and more diverse social network. It would be interesting to examine whether or not different privacy preferences result in differing behavior and outcomes. It is possible that Dollie's smaller network could preclude her from some social benefits, such as serendipitous network discovery. Using a targeted subset of our scales in combination with various outcome measures may lend insight into more socially beneficial privacy practices.

5.2 Limitations

Before concluding, we also discuss some of the limitations of our research and approach. First, we initially performed the SNS feature analysis in 2012 and each of the SNS interfaces have since changed aspects of their functionality as they frequently do. However, the main benefit of conducting the feature analysis was to be able to compare and contrast across different applications in the same domain to abstract the key dimensions of privacy boundaries in which they support. Therefore, small variances in privacy features should not have a major impact on our overall findings. Second, even though we tried to target a variety of users for our semi-structured interviews, the majority of our SNS user interviews primarily focused on Facebook use because it was and remains the predominant SNS with an estimated 968 million daily active users in June 2015 (Facebook, 2015). This bias toward Facebook use is a potential limitation of our boundary taxonomy, which was largely reliant on our interviews of SNS users. Even though our sample of 21 SNS users was sufficient for theoretical saturation (Strauss & Corbin, 1998) of the 10 boundary types presented in this paper and the empirical validation of our scales confirmed the internal consistency, convergent, and discriminant validity of the dimensions derived from our theoretical framework, other SNS boundary types may exist that are not included here. Third, due to the critical mass of Facebook users we encountered during our interviews, we chose to target Facebook users as the user population for validating our survey measures. Finally, because we specifically focused our statistical analysis of the privacy scales on confirming construct validity, our cross-sectional survey did not capture the more dialectical processes associated with SNS users' privacy preferences as they change over time.

5.3 Future Research Directions

We suggest several future research directions based on the limitations we state above and on emergent themes that we identified during our interface analysis and SNS user interviews. To address the limitations of our work, we suggest that future research validate our theoretical framework and test our measures explicitly with non-Facebook SNS users. Doing so would help ensure the completeness of our taxonomy and our scales' generalizability. Future work may also examine how our scales can be extended to capture privacy preferences and related processes over time as opposed to a snap-shot of personal privacy preferences at one point in time. Longitudinal studies or controlled experiments with repeated measures may be a more appropriate method for modeling the dialectical processes involved in SNS users' privacy preferences as they change over time and context. For example, an individual's privacy preferences measured by our scales may prove to be drastically different as SNS users go through major transitional periods, such as moving from high school to college or from college to the professional world.

Various SNS privacy challenges also emerged from our data during the qualitative coding process that should be explored in more depth in future work. We illustrate these privacy challenges through the feature comparisons and quotes in Section 3.3 and include: 1) lack of SNS user feature awareness, 2) ineffective or difficult-to-use interface controls, 3) social cues and norms discouraged setting boundary privacy, 4) users' experiencing a high-level of boundary conflicts, and, thus 5) users' developing (often unhealthy) coping mechanisms to reclaim their privacy boundaries. We briefly describe each of these emergent themes and suggest possible directions for future inquiry related to these themes.

Lack of awareness was a key reason many of our participants did not leverage SNS interface controls as a way to manage their relationships with others. We were surprised to see that fairly seasoned SNS users were not aware of features such as unfriending, untagging, creating friend lists, or hiding individuals from their news feeds. A possible reason for this lack of awareness is that people have traditionally characterized privacy as something that is managed through one's privacy settings. Because these privacy mechanisms were in the context of a particular social interaction, not grouped under privacy settings, our participants may not have associated them with privacy regulation. Our initial work has provided some evidence that feature awareness is an integral component of privacy for technology-mediated social interactions (Wisniewski, 2012; Wisniewski & Lipford, 2013). A lack of feature awareness may help explain what some researchers have identified as an apparent "privacy paradox" between SNS users' stated privacy concerns and their privacy behaviors (Acquisti & Gross, 2006; Barnes, 2006). Therefore, future work should consider SNS users' awareness of privacy features when trying to understand their subsequent privacy behaviors.

Even when SNS users were aware that a feature existed, they often felt that it was either ineffective for managing their privacy boundary needs or too difficult to use. For example, some participants felt that creating friend lists still did not solve the problem of "context collapse" (Grudin, 2001) when trying to

manage their relationship context or network intersection boundaries. Based on the interface analysis, we found that some privacy features were provided but too inflexible to be useful. For example, SNS users often had to resort to hiding their friends list completely in order to make sure one or two people in their networks did not exploit their connections. This all-or-nothing design made interpersonal boundary regulation impossible due to its blanket approach to relationship management. In addition, other privacy features were too permanent in nature and neglected the dialectical nature of privacy boundaries. For instance, some participants realized that they meant to hide a friend from their Facebook news feed for a time but had forgotten to reconnect with them afterward. Finally, many privacy features had to be employed retroactively after a particular boundary had already been violated, such as deleting an unwanted post from outward-facing territories, untagging photos, or hiding offensive content from one's inward-facing territories. These interface shortcomings speak directly to the HCI design community in that new privacy interfaces need to be designed that allow SNS users to enact their privacy preferences easily and effectively as to meet their privacy needs.

SNS interfaces frequently discouraged boundary setting behaviors by visually de-emphasizing options for disengaging with others (such as ignoring a friend request or unfriending) or by sharing content by default, which required SNS users to take action when they wanted to manage their boundaries. While such "opt-out" privacy policies may facilitate more sharing, they also have the potential of disengaging SNS users who desire higher levels of privacy (Baumer et al., 2013; Wang, Wisniewski, Xu, & Grossklags, 2014; Wisniewski, Xu, & Chen, 2014b; Wisniewski et al., 2015b). Possibly because SNSs discouraged it or from external social pressures, SNS users often felt uncomfortable enacting interpersonal boundaries even when it was appropriate to do so. For example, unfriending and blocking were rare, and participants expressed pressure to accept friend requests from people who were not their friends. Overall, the majority of our participants experienced some kind of privacy violation that led to conflict or negative emotional consequences. As a result, SNS users were often frustrated and chose to withdraw from engagement through self-censorship, ignoring, and generalizing their SNS interactions to be appropriate for all audiences instead of fostering deeper relationships through their social networks. For a more detailed discussion about the coping mechanisms that emerged from this analysis, see Wisniewski et al. (2012).

Due to the tensions between SNS providers and users over privacy protection, we need more research on to understanding the potential benefits and drawbacks and the motivations for nudging (Wang et al., 2013) SNS users towards certain privacy practices. The motivation for SNSs to protect end user privacy may be secondary to organizational goals, such as facilitating e-commerce transactions. However, our research suggests that not providing appropriate privacy mechanisms to SNS users may reduce user satisfaction, engagement with others, information sharing, SNS use, and consumer loyalty to a particular SNS (Wang, Xu, & Grossklags, 2011; Wisniewski et al., 2015a; Wisniewski et al., 2015b). We hope that future research can build on our work to confirm the potential individual benefits and business-value associated with understanding and supporting SNS users' unique privacy preferences.

6 Conclusion

Boundary mechanisms used in the physical world do not translate well to the new world of online social networking and, thus, need to be understood in this new context. With this paper, we help to address the issue by extending established theories of interpersonal boundary regulation from social psychology. Our taxonomy serves as a foundation to build additional SNS boundary regulation theories and to design improved SNS interfaces. We broaden the definition of SNS privacy so that it is no longer focused solely on protecting private, personal information and instead acts as a means of optimizing social interactions. Our approach is novel in that it incorporates both the actual SNS interface controls available for privacy boundary management (i.e., the feature analysis) and information on how SNS users actually leverage these mechanisms (i.e., semi-structured interviews) into one cohesive taxonomy. By showing that SNS users struggle to negotiate their social interactions online, we motivate the need for design considerations to improve support for these mechanisms. Our taxonomy can also be used as a framework to benchmark boundary regulation features across the domain of SNSs or evaluate new SNSs. For example, Google+ improved support for relationship context boundaries through circles and reduced emphasis of outward-facing territories by not implementing the equivalent to Facebook's wall. Of the five SNSs in our study, Facebook provided the most features for interpersonal boundary regulation. Yet, overall, we found that SNS interface controls were not effective in facilitating boundary negotiation. Altman (1975, p. 198) argues that "we should attempt to design responsive environments, which permit easy alternation between a state of separateness and a state of togetherness" to meet changing privacy needs. With better understanding

of interpersonal boundary regulation with respect to SNS design, we can create SNS interfaces that support flexible and intuitive controls that can help meet individuals' dynamic needs for both separating from and connecting to others.

References

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook* (Vol. 4258). Berlin: Springer.

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole.

Anton, A. I., Earp, J. B., & Young, J. D. (2010). How Internet users' privacy concerns have evolved since 2002. *IEEE Security and Privacy*, *8*(1), 21-27.

Babbie, E. (2004). *The practice of social research* (10th ed.). Belmont, CA: Wadsworth Publishing Company.

Bailey, K. D. (1994). *Typologies and taxonomies: An introduction to classification techniques*. Thousand Oaks, CA: Sage.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). Retrieved from http://firstmonday.org/article/view/1394/1312

Baumer, E., Adams, P., Khovanskaya, V., Liao, T., Smith, M., Sosik, V. S. (2013). *Limiting, leaving, and (re)lapsing: An exploratoration of Facebook non-use practices and experiences*. Paper presented at the Conference on Human Factors in Computing Systems, Paris, France.

Besmer, A., & Lipford, H. R. (2010). *Moving beyond untagging: Photo privacy in a tagged world*. Paper presented at the ACM Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA.

Boyd, D. (2004). *Friendster and publicly articulated social networking*. Paper presented at the CHI '04 Extended Abstracts on Human Factors in Computing Systems, Vienna, Austria.

Boyd, D. (2006). Friends, friendsters, and myspace top 8: Writing community into being on social network sites. *First Monday*, 11(2). Retrieved from http://firstmonday.org/article/view/1418/1336

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

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, *56*(1), 81-105.

Carper, W. B., & Snizek, W. E. (1980). The nature and types of organizational taxonomies: An overview. *Academy of Management Review*, *5*(1), 65-75.

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, *28*(5), 1859-1872.

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. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet. In K. W. L. Webb (Ed.), *Computer mediated communication in personal relationships* (pp. 21-40). New York: Peter Lang.

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.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, *12*(3), 341-345.

Cook, M., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston: Houghton Mifflin.

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.

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

Dinev, T., Xu, H., & Smith, H. J. (2009). *Information privacy values, beliefs and attitudes: An empirical analysis of Web 2.0 privacy*. Paper presented at the Proceedings of 42th Hawaii International Conference on System Sciences, Big Island, Hawaii.

Doty, D. H., & Glick, W. H. (1994). Typologies as a unique form of theory building: Toward improved understanding and modeling. *Academy of Management Review*, *19*(2), 230-251.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environments. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 19-32). Berlin: Springer-Verlag.

Facebook. (2015). *Newsroom*. Retrieved from http://newsroom.fb.com/company-info/

Fono, D., & Raynes-Goldie, K. (2006). Hyperfriendship and beyond: Friends and social norms on LiveJournal. In M. Consalvo & C. Haythornthwaite (Eds.), I*nternet Research Annual Volume 4: Selected papers from the Association of Internet Researchers Conference*. New York: Peter Lang.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(2), 39-50.

Freeze, R. D., & Raschke, R. L. (2007). *An assessment of formative and reflective constructs in IS research*. Paper presented at the European Conference on Information Systems.

Gefen, D., Rigdon, E., & Straub, W. D. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, *35*(2), iii-xiv.

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.

Grudin, J. (2001). Desituating action: Digital representation of context. *Human Computer Interaction*, *16*(2-4), 269-286.

Louis Harris & Associates, & Westin, A. F. (1997). *Commerce, communications, and privacy online: A national survey of computer users*. Hackensack, NJ: Privacy & American Business.

Louis Harris & Associates, & Westin, A. F. (2003). *Consumer privacy attitudes: A major shift since 2000 and why.* Harris Interactive.

Harris, P. B., Brown, B. B., & Werner, C. M. (1996). Privacy regulation and place attachment: Predicting attachments to a student family housing facility. *Journal of Environmental Psychology*, *16*(4), 287-301.

Harrison, C. L. (1993). *The development of a desire for privacy scale*. Retrieved from http://digitalcommons.uconn.edu/dissertations/AAI9405263/

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19-33.

Kane, G. C., Alavi, M., Labianca, G. J., & Borgatti, S. P. (2014). What's different about social media networks? A framework and research agenda. *MIS Quarterly*, *38*(1), 274-304.

Kang, K. C., Cohen, S. G., Hess, J. A., Novak, W. E., & Peterson, A. S. (1990). *Feature-oriented domain analysis (FODA) feasibility study* (Technical Report CMU/SEI-90-TR-021). Software Engineering Institute.

Kaya, N., Webb, J. D., & Miller, N. G. (2005). Adjustment to congregate living environments: Older adults and privacy regulation. *Journal of Interior Design*, *31*(1), 14-24.

Kaya, N., & Weber, M. J. (2003). Cross-cultural differences in the perception of crowding and privacy regulation: American and Turkish students. *Journal of Environmental Psychology*, *23*(3), 301-309.

Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011). *We're in it together: Interpersonal management of disclosure in social network services.* Paper presented at the Proceedings of the annual conference on Human factors in computing systems, Vancouver, BC.

Lewins, A., & Silver, C. (2007). *Using software in qualitative research—a step-by-step guide*. London: SAGE Publications.

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.

Lipford, H. R., Wisniewski, P., Lampe, C., Kisselburgh, L., & Caine, K. (2012). *Reconciling privacy and social media.* Paper presented at the 2012 ACM Conference on Computer Supported Cooperative Work, Seattle, WA.

Malhotra, N. K., Kim, S. 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.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

OptimalWorkshop.com. (n.d.). *Optimal workshop*. Retrieved from https://apps.optimalworkshop.com/suite/optimalsort/admin/dashboard.jsf

Palen, L., & Dourish, P. (2003). *Unpacking "privacy" for a networked world*. Paper presented at the ACM Conference on Human Factors in Computing Systems, Ft. Lauderdale, FL.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal- agent perspective. *MIS Quarterly*, *31*(1), 105-136.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: SUNY Press.

Scott, J. (2009). *Social network analysis*. Los Angeles, CA: Sage.

Simpson, G. G. (1961). *Principles of animal taxonomy*. New York: Columbia University Press.

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

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

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

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*, 380-427.

Strauss, A. L., & Corbin, J. M. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Thousand Oaks, CA: Sage.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. C*omputers in Human Behavi*or, *27*(1), 590-598.

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7-41.

Stutzman, F., & Hartzog, W. (2009). *Boundary regulation in social media*. Paper presented at the AOIR 2009, Milwaukee, WI.

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., & Lampe, C. (2012). *Privacy in interaction: Exploring disclosure and social capital in Facebook*. Paper presented at the Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20-36.

Wang, N., Wisniewski, P., Xu, H., & Grossklags, J. (2014). *Designing the default privacy settings for facebook applications.* Paper presented at the Proceedings of the companion publication of the

17th ACM conference on Computer supported cooperative work and social computing, Baltimore, Maryland, USA.

Wang, N., Xu, H., & Grossklags, J. (2011). *Third-party apps on Facebook: Privacy and the illusion of control.* Paper presented at the Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology, Cambridge, Massachusetts.

Wang, Y., Leon, P. G., Scott, K., Chen, X., Acquisti, A., & Cranor, L. F. (2013). *Privacy nudges for social media: An exploratory Facebook study.* Paper presented at the Second International Workshop on Privacy and Security in Online Social Media.

Westin, A. F., & Louis Harris & Associates. (1981). *The dimensions of privacy: A national opinion research survey of attitudes toward privacy*. New York: Garland Publishing.

Wisniewski, P. (2012). *Understanding and designing for interactional privacy needs within social networking sites* (doctoral dissertation). University of North Carolina at Charlotte, Charlotte, NC.

Wisniewski, P., Islam, N., Knijnenburg, B., & Patil, S. (2015a). *Give social network users the privacy they want.* Paper presented at the the 2015 ACM Conference on Computer Supported Cooperative Work (CSCW 2015), Vancouver, BC, Canada.

Wisniewski, P., Knijnenburg, B. P., & Lipford, H. R. (2014a). P*rofiling Facebook users' privacy behaviors*. Paper presented at the the Workshop on Privacy Personas and Segmentation at the Symposium On Usable Privacy and Security (SOUPS 2014), Menlo Park, CA.

Wisniewski, P., Lipford, H., & Wilson, D. (2012). *Fighting for my space: Coping mechanisms for SNS boundary regulation*. Paper presented at the ACM Conference on Human Factors in Computing Systems, Austin, TX.

Wisniewski, P., & Lipford, H. R. (2013). *Between nuance and rigor: Contextualizing and measuring SNS desired privacy level.* Paper presented at the 2013 ACM Conference on Computer Supported Cooperative Work, San Antonio, TX.

Wisniewski, P., Xu, H., & Chen, Y. (2014b). *Understanding user adaptation strategies for the launching of facebook timeline.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, Ontario, Canada.

Wisniewski, P., Xu, H., Lipford, H., & Bello-Ogunu, E. (2015b). Facebook apps and tagging: The trade-off between personal privacy and engaging with friends. *Journal of the Association for Information Science and Technology*, *66*(9), 1883-1896.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research*, *13*(2), 151-168.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). *Examining the formation of individual's privacy concerns: Toward an integrative view.* Paper presented at the Twenty Ninth International Conference on Information Systems, Paris, France.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824.

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, *37*, 283-289

Zinoviev, D., & Duong, V. (2009). Toward understanding friendship in online social networks. International *Journal of Technology, Knowledge, and Society*, *5*(2), 1-8.

About the Authors

Pamela Wisniewski is an Assistant Professor in the College of Engineering and Computer Science at the University of Central Florida. Her research interests are situated in Human-Computer Interaction and lie at the intersection of social computing and privacy. Her goal is to frame privacy as a means to not only protect end users but, more importantly, to enrich online social interactions that individuals share with others. Her work has won best paper (top 1%) and best paper honorable mentions (top 5%) at premier conferences in her field.

A. K. M. Najmul Islam is a Post-doctoral Researcher in the Department of Information Systems at the University of Turku, Finland. He has a Master degree in Telecommunications Engineering from Tampere University of Technology, Finland and a PhD degree in Information Systems from the University of Turku, Finland. His research interests are in Human-Computer Interaction, with a focus on negative consequences of technology use. His research has been published in outlets such as *Computers in Human Behavior*, *Computers & Education, Journal of Information Systems Education, AIS Transaction on Human-Computer Interaction* and *Behaviour & Information Technology.*

Heather Richter Lipford is an Associate Professor in the Department of Software and Information Systems at the University of North Carolina at Charlotte. Her research interests are in Human Computer Interaction, with a focus in usable privacy and security, secure programming, and social computing. At UNC Charlotte, Dr. Lipford is a member of the HCI Lab, the Cyber Defense and Network Assurability Center, and the Cognitive Science Academy. She received a Bachelor of Science degree from Michigan State University in 1995, and a PhD from the College of Computing at the Georgia Institute of Technology in 2005.

David C. Wilson is a Professor in the Department of Software and Information Systems at UNC Charlotte. His research interests span Data Science, Intelligent Systems, and Human-Computer Interaction with emphasis on Recommender Systems and Spatial Content. At UNC Charlotte, He is a member of the HCI Lab, The Charlotte Visualization Center, and the Center for Education Innovation. He received his MS and PhD degrees from Indiana University, Bloomington.