Give Social Network Users the Privacy They Want

Pamela Wisniewski[*]   **A.K.M. Najmul Islam**[†‡]   **Bart P. Knijnenburg**[♯]   **Sameer Patil**[†ξφ]

[*]College of Information Sciences and Technology, Pennsylvania State University
University Park PA 16802, USA
[†]Helsinki Institute for Information Technology HIIT / Aalto University
P O Box 15600, 00076 Aalto, Finland
[‡]Information Systems Science, University of Turku, 20500 Turku, Finland
[♯]Department of Informatics, University of California, Irvine, Irvine CA 92697, USA
[ξ]Department of Information Systems and New Media, University of Siegen, 57068 Siegen, Germany
[φ]Yahoo Labs, 701 First Avenue, Sunnyvale, CA 94089, USA
puw16@psu.edu, najmul.islam@utu.fi, bart.k@uci.edu, sameerpatil@yahoo-inc.com

ABSTRACT

Social Network Sites (SNS) are often characterized as a trade-off where users must give up privacy to gain social benefits. We investigated the alternative viewpoint that users gain the most benefits when SNSs give them the privacy they desire. Applying structural equation modeling to questionnaire data of 303 Facebook users, we examined the complex relationship between privacy and SNS benefits. We found that SNS users whose privacy desires were met reported higher levels of social connectedness (i.e., perceived relational closeness with others) than those who achieved less privacy than they desired. Social connectedness, in turn, played a pivotal role in building social capital (i.e., the benefits derived from relationships with others). These findings suggest that more openness may not always be better; SNSs should aim to achieve 'Privacy Fit' with user needs to enhance user experience and ensure sustained use.

Author Keywords

Privacy; Facebook; social capital; social connectedness; Social Network Sites; SNS.

ACM Classification Keywords

H.5.2. Information Interfaces and Presentation (e.g. HCI): User Inferfaces

INTRODUCTION

In recent years, Social Network Sites (SNSs) have become an integral part of people's everyday online activities. Interpersonal interactions through SNSs have been shown to have a positive impact on a host of factors, including social capital, social connectedness, self-esteem, and personal well-being [5, 9, 10, 24]. At the same time, there is increasing concern about the negative impact of SNSs on personal privacy [30]. Technology related issues that raise privacy concern range from deliberate abuses to inadvertent violations [4]. SNS users may regret past disclosures and face negative social and professional consequences as a result of SNS interactions [49]. Inadequate privacy support has often led to user protests and has been shown to impact user participation negatively, e.g., through self-censorship or temporary or even full abandonment of SNSs [2, 39, 52, 53]. Thus, there seems to be a considerable rift between the primary SNS goal of promoting social engagement and the secondary goal of protecting users' personal privacy [29].

Privacy researchers have historically conceptualized privacy as a *trade-off* between risks and benefits [27]. The argument that one must make a trade-off between personal privacy and the interactional benefits of technology-mediated sociality has been a prevailing paradigm also within the CSCW research community: "There is a tacitly held assumption in CSCW and social psychology that some degree of privacy risk is the inevitable cost of social life" [4]. In light of this trade-off, popular SNSs typically downplay the importance of privacy preservation in favor of facilitating social connection. For instance, Facebook CEO Mark Zuckerberg has frequently asserted that SNS users are no longer concerned about their personal privacy because sharing has become the new social norm: *"People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time,"* Zuckerberg explained [31].

Yet, not all SNS users share Zuckerberg's belief. While some SNS users have become more open, others continue to value their privacy [30]. Does this mean that only users who are unconcerned about their privacy are able to derive benefits from SNS use? Or can SNS users maintain a level of privacy they desire *and simultaneously* benefit from SNS engagement?

Several privacy scholars have already challenged the assumption that users must give up personal privacy in order to benefit from technology use and have explored the opportunities of simultaneously enhancing privacy and benefits [4, 18, 26, 36]. Our study extends this approach specifically to the context of SNSs. We follow the suggestion of these contemporary theo-

rists to move beyond a definition of privacy in absolute terms (i.e., as the opposite of being "public"). Specifically, we take a user centered approach to SNS privacy, which defines privacy in relative terms based on the unique privacy preferences of individual users (cf., Altman's definition of privacy [1]). Additionally, we take an *evaluative* approach (i.e., examining the effect of a match between preferred and achieved levels of privacy on socialization benefits in an existing SNS) rather than a generative approach (i.e., offering design principles). Our goal is to provide empirical weight to the argument that helping users attain an optimal level of privacy can increase their perceived benefits of using SNSs. Specifically, we hypothesized that meeting SNS users' privacy needs is a crucial aspect of supporting social benefits and proposed that if a user gives up more personal privacy than he or she desires, it can actually be detrimental to fostering effective and meaningful social connections. In this way, we further unpack the complex relationship between privacy and sociality and extend the existing SNS privacy literature by empirically examining the relationship between user based privacy preferences, achieved privacy outcomes, and SNS benefits.

To this end, we administered a Web based questionnaire to Facebook users (N=303) and applied structural equation modeling (SEM) to study the effects of the match between users' desired privacy level and the privacy level they actually achieved. We labeled this match as *Privacy Fit*. Privacy Fit occurs when a user has either a low level of desired privacy and achieves it, or alternatively, when a user has a high desire for privacy and achieves it. Conversely, *Privacy Mismatch* occurs when a user's desired privacy level is not sufficiently met. Our results indicate that Facebook users who achieved Privacy Fit (regardless of high or low desired level of privacy) reported higher levels of Social Connectedness than those who achieved less privacy than desired. Higher levels of Social Connectedness were in turn associated with increased Bridging and Bonding Social Capital. Additionally, we found that Privacy Fit was associated with higher levels of Facebook Usage Intensity and that the positive effect of Privacy Fit on Social Connectedness was moderated by Facebook Usage Intensity (i.e., Privacy Mismatch negatively impacted casual Facebook users more strongly than avid users).

Our work provides empirical weight to Boyle and Greenberg's claim that catering to users' privacy desires can increase the perceived benefits of using a system [4]. This highlights the need to re-examine the assumed dichotomy between privacy and socialization. Consequently, we argue that SNS providers could maximize the benefits of their service by promoting user tailored privacy, rather than simply urging users to share as much as possible. Specifically, our work makes the following contributions to SNS privacy research:

- Operationalizes and statistically validates a broader conceptualization of privacy in the form of a *measurement instrument* that captures users' desired versus achieved privacy levels across 10 different aspects of SNS privacy,

- Examines privacy relative to SNS users' individual privacy preferences, as opposed to viewing privacy in absolute terms,

- Empirically confirms that Privacy Fit affords more social benefits than Privacy Mismatch, thereby challenging the assumption that SNS users must share more and give up personal privacy in order to benefit from SNS use,

- Uncovers additional relationships between Privacy Fit, Facebook Use, Social Connectedness, and Social Capital, and

- Advocates for designing user tailored SNS privacy mechanisms that optimize the fit between users' desire for privacy and their actual privacy experiences.

In the next section we summarize related work on SNS privacy and explain our contribution beyond extant literature. We then lay out the theoretical groundwork leading to structural models of hypothesized relationships among Privacy Fit, Facebook Use, Social Connectedness, and Social Capital. Next, we operationalize our constructs, test our models, and present the results of our analyses. We conclude with a discussion of how our findings provide theoretical, methodological, and design implications for SNS privacy.

RELATED WORK

Empirical SNS privacy research typically frames privacy as "the ability of individuals to control when, to what extent, and how information about the self is communicated to others" [11], thus narrowing SNS privacy specifically to examining the regulation of private versus public disclosures [25]. By framing SNS privacy in such absolute terms, privacy management is often presented as a trade-off or balancing act, where giving up privacy through information disclosures is necessary for connecting with others [29]. For example, Stutzman et al. [44] found that Facebook users who disclosed more personal information reported higher levels of Social Capital but also higher privacy concerns.

In contrast, contemporary privacy theorists have attempted broader conceptualizations of privacy issues. For example, Langheinrich [26] and Iachello and Abowd [18] offered principles for design of ubiquitous computing systems based on application of the legal principles of Fair Information Practices and the Principle of Proportionality, respectively. In the domain of technology mediated interpersonal interactions, Palen and Dourish [36] described how Altman's work on interpersonal boundary regulation in physical interactions [1] could be applied to interactions mediated by technology. Using the example of video media spaces, Boyle and Greenberg [4] further linked the conceptual insight of Palen and Dourish with operational design guidance for effective privacy management support. In particular, Boyle and Greenberg explored the opportunities of simultaneously enhancing privacy and utility in the design of video conferencing systems [4]. We aim to promote a similar broadening of the discourse on privacy and design in the SNS context by challenging the assumption that users must give up privacy in order to benefit from SNS use. We thus extend existing SNS privacy literature by unpacking the complex relationships between expressed privacy preferences, achieved privacy outcomes, and social benefits of SNS.

Boundary Type	Dimensions	Definition
Disclosure	Self Disclosure (SELF)	Regulating what personal information one discloses within one's network
	Confidant Disclosure (CONF)	Regulating how co-owned personal information is disclosed within one's network
Relationship	Connection (CONN)	Regulating whom to let into one's social network
	Context (CONT)	Regulating appropriate interpersonal interactions given the type of relationship
Territorial	Inward Facing (IN)	Regulating incoming content for personal consumption
	Outward Facing (OUT)	Regulating semi-public content available through interactional spaces
Network	Discovery (DISC)	Regulating access others have to one's network connections
	Intersection (INTER)	Regulating social interactions between connections or groups of connections
Interactional	Disabling (DIS)	Regulating potential interaction through turning on/off interface features
	Blocking (BLOCK)	Regulating overall access of oneself to specific individuals outside of one's network

Table 1. SNS interpersonal privacy boundary types.

We frame SNS privacy using Altman's work on interpersonal boundary regulation [1]. Altman defined privacy as "an interpersonal boundary process by which a person or group regulates interaction with others" by altering the degree of openness of the self to others [1]. Boundary regulation is an interactive process where two or more individuals collaborate in order to negotiate an acceptable level of social interaction [1, 37]. The process is dialectic, balancing both the restriction and seeking of social interaction based on an individual's changing privacy needs. Altman proposes that meeting one's privacy needs through this process of interpersonal boundary regulation is the key to effective social interactions. Ineffective boundary regulation can lead to sub-optimal outcomes, such as a state of *social crowding* or *social isolation*, experiencing much more or much less social interaction than one desires, respectively [1].

Several SNS privacy researchers have adopted Altman's definition of privacy as a boundary regulation process [25, 35, 36, 43, 45]. However, these works primarily focused on boundaries related to information disclosure, not considering Altman's broader framing of privacy as any 'interpersonal event' that serves to optimally regulate one's social interactions [1]. In this sense, interpersonal boundaries help us define who we are, as well as with whom, how, and when we interact. Part of the problem may be that Altman's boundary control mechanisms — coping behaviors, verbal, paraverbal, nonverbal, personal space, and territorial behaviors — were originally identified in the *physical realm* and are difficult to translate to analogous online behaviors [4].

Previous qualitative work by Karr-Wisniewski et al. [19, 52, 54] extended Altman's broader conceptualization of privacy as an interpersonal boundary regulation process specifically to the realm of SNSs. This prior work provided better understanding of the unique coping behaviors [52] and other mechanisms SNS users employ to regulate various aspects of interpersonal privacy [19, 54]. In addition to *disclosure* boundaries, SNS users were found to negotiate *relationship*, *network*, *territorial*, and *interactional* boundaries to regulate their privacy levels. For instance, hiding annoying posts from a friend's game application helps regulate *inward fac-*

ing territorial boundaries (such as one's News Feed), but this is orthogonal to whether the information is considered private [19]. Table 1 summarizes the taxonomy of the different SNS boundary types proposed by Karr-Wisniewski et al. We operationalized this taxonomy by developing a measurement scale that quantifies SNS users' desired and achieved privacy levels according to each of these privacy dimensions. Our examination of SNS privacy, therefore, considers privacy from this broader perspective rather than limiting our scope to public versus private disclosures.

HYPOTHESIZED STRUCTURAL MODEL

Figure 1 summarizes our research framework with hypothesized relationships between Privacy Fit, Facebook Usage Intensity, Social Connectedness, and Social Capital. Below, we introduce our theoretical constructs and provide justification for our hypotheses.

Social Capital

Social Capital refers to the benefits afforded through social networking that are derived from the development and maintenance of relationships with others [24, 50]. It is one of the most prevalent dependent variables examined in SNS research [9–11, 24, 46, 47, 50]. Williams [50] developed an 'Internet Social Capital Scale' (ISCS) through an in-depth review of the literature coupled with statistical validation of the emergent dimensions of Social Capital. He found that Social Capital varies along two dimensions: *Bridging Social*
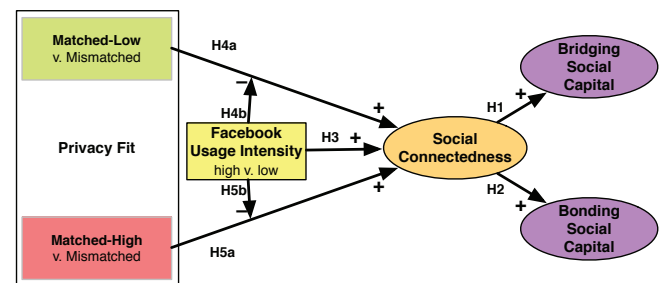

Figure 1. Structural model combining all hypotheses. This model was tested for each of the 10 boundary types.

Capital refers to the resources gained through connections with weak ties (e.g., acquaintances) whereas *Bonding Social Capital* deals with the benefits derived through more intimate relationships, such as those between close friends and family. Benefits of Bridging Social Capital include a sense of community, an increased curiosity for the world-at-large, and a desire to try new things while benefits of Bonding Social Capital include emotional support and the ability to mobilize resources, such as obtaining a reference, borrowing money, or receiving advice [9, 50].

Social Connectedness

Koroleva et al. [24] differentiated between the sources and benefits of Social Capital. They suggested that *Social Connectedness* is a cognitive dimension of perceived relational closeness, which is necessary to activate connections between individuals and realize the benefits of social capital. Social Connectedness involves staying in touch with and connecting with other individuals. In this way, Social Connectedness acts as a *source* of and/or prerequisite for obtaining the *benefits* of Social Capital [24]. Therefore, we hypothesized that:

H1: *Social Connectedness is positively associated with Bridging Social Capital.*

H2: *Social Connectedness is positively associated with Bonding Social Capital.*

Facebook Usage Intensity

We define *Facebook Usage Intensity* as the degree to which users are emotionally connected to Facebook and the extent to which Facebook is integrated in their daily activities [9]. Facebook has become a pervasive means of social interaction and communication among adults. Prior research found Facebook usage linked to positive social outcomes, such as greater social capital, increased self-esteem, and enhanced well-being [9]. In early SNS research, Facebook Usage Intensity showed positive relationships with both Bonding and Bridging Social Capital, with the latter being stronger, while general Internet usage did not influence social capital [9]. Later research clarified that the generation of social capital was driven by social information-seeking behaviors, not by the initiation of new relationships or the maintenance of existing relationships on Facebook [10]. Further, the increase in social capital was attributed to active content contribution rather than passive information consumption [10]. These findings indicate that the relationship between Facebook Usage Intensity and Social Capital is driven by the type and the quality of connections with others. Therefore, we argue that Social Connectedness *mediates* the relationship between Facebook Usage Intensity and Social Capital; those with high levels of Facebook Usage Intensity remain socially connected to their friends, which in turns helps them generate Social Capital. We thus hypothesized that:

H3: *Facebook Usage Intensity is positively associated with Social Connectedness.*

In conjunction with H1 and H2, this hypothesis effectively links Facebook Usage Intensity to Bridging and Bonding Social Capital through its relationship to Social Connectedness.

In the remainder of this paper, we refer to those with high levels of Facebook Usage Intensity as *avid* Facebook users and those with low levels of Facebook Usage Intensity as *casual* Facebook users.

Privacy Fit

According to Altman, individuals try to reach their *desired privacy level* in order to achieve an optimal level of social interaction [1]. In optimal cases, boundary negotiation results in boundary coordination. We labeled this optimum as *Privacy Fit*. Failure to achieve Privacy Fit results in what has been termed 'boundary turbulence' [37] or boundary violation [1, 20]. We characterized this lack of Privacy Fit as *Privacy Mismatch*. Two types of mismatches can occur: *social crowding* refers to over-stimulation by undesirably high levels of social interaction (i.e., less privacy than needed); inversely, *social isolation* leads to less social interaction than desired (i.e., more privacy than intended) [1]. Both crowding and isolation are sub-optimal and may result in a variety of negative outcomes, including physical, physiological, and psychological stress, vulnerability, illness, anxiety, embarrassment, bewilderment, discomfort, flight reactions, and anger [1]. For example, older adults living in assisted living facilities were found to be prone to feeling more crowded than those living independently and this social crowding was associated with lower levels of adjustment to the living environment [21]. Another study found that students living in family housing felt more attached to their living arrangements if they felt that the space afforded them adequate means to adjust privacy boundaries [17].

Recent work suggests that the findings from these studies conducted in the physical world [17, 21] may also apply to SNSs. For instance, Ellison et al. [11] found that the use of advanced privacy settings on Facebook was *positively* associated with the number of Facebook friends and perceived social capital. This finding provides some empirical indication that effective interpersonal boundary regulation within SNSs may afford enhanced social benefits. However, little research has explored the relationship between SNS privacy and benefits. We attempt to fill this gap with structural models that link the match or mismatch between desired and actual privacy levels to the social benefits of SNS use (i.e., Social Capital and Social Connectedness). Specifically, we argue that Privacy Fit leads to more beneficial SNS interactions than Privacy Mismatch. Consequently, users who attain Privacy Fit will have better SNS interactions *regardless of whether they desire and attain low (Matched-Low) or high (Matched-High) levels of privacy*. Given that enhanced social interactions foster greater Social Connectedness, we hypothesized that:

H4a: *Facebook users who report a Matched-Low Privacy Fit perceive greater Social Connectedness than those who experience a Privacy Mismatch.*

H5a: *Facebook users who report a Matched-High Privacy Fit perceive greater Social Connectedness than those who experience a Privacy Mismatch.*

However, we acknowledge that the relationship between Privacy Fit and Social Connectedness (Hypotheses H4a and

H5a) may be influenced by Facebook Usage Intensity. Based on cognitive dissonance theory [14], avid Facebook users are likely to engage in dissonance reduction to achieve uniformity between their privacy cognition and their high Facebook Usage Intensity. As a result, these individuals may justify their avid usage by ascribing lower importance to Privacy Fit. Moreover, avid users may experience habituation in their Facebook usage. Automatic and habitual behaviors require little (if any) conscious attention and only minimal mental effort [28]. Therefore, Privacy Mismatch is less likely to reduce the ability of these users to maintain social connections. This led us to the following two moderating hypotheses:

H4b: *The difference in Social Connectedness between those who achieve Matched-Low Privacy Fit and those who experience a Privacy Mismatch is smaller for avid Facebook users than for casual Facebook users.*

H5b: *The difference in Social Connectedness between those who achieve Matched-High Privacy Fit and those who experience a Privacy Mismatch is smaller for avid Facebook users than for casual Facebook users.*

We combined the above hypotheses into the theoretical structural model shown in Figure 1. Since we examine the contrasting outcomes between Privacy Fit (Matched-Low and Matched-High) and Privacy Mismatch, we chose to represent Privacy Mismatch as the baseline condition. We compared the two types of Privacy Fit — low and high — against this baseline. We tested 10 separate instances of the model, one for each of the 10 privacy boundary types defined in Table 1.

METHOD
To test our 10 hypothesized models, we operationalized and measured relevant constructs in the form of a questionnaire.

Construct Operationalization
We utilized pre-validated measures for Bridging and Bonding Social Capital [9, 50], Social Connectedness [24], and Facebook Usage Intensity [9]. We created our own measures for desired and actual SNS privacy levels across the 10 privacy boundary types described in Table 1. The Appendix provides the individual items for these measures along with associated psychometric properties. Prior to data collection, we confirmed the face validity of these measures using card sorting techniques [32, 42].

Data Collection
We obtained a random sample of 10,000 email addresses of students, faculty, and staff from the registrar of the University of North Carolina at Charlotte.[1] These individuals were invited to fill out a Web based questionnaire between February and April 2012. Only those over 18 years of age with an active Facebook account qualified for participation. The questionnaire could be completed in about 20–25 minutes. At the end, respondents could enter a random drawing for one of two $100 Amazon gift certificates. Respondents were encouraged to refer others to the study and were offered an additional entry in the drawing for each referral who completed

---

[1]The study was conducted while the first author was a doctoral student at the University of North Carolina at Charlotte.

the questionnaire, up to a maximum of 25. The questionnaire instrument and recruitment procedures were approved by the university's Institutional Review Board (IRB).

Respondents
A total of 331 respondents filled out the questionnaire. We excluded 3 respondents who did not maintain an active Facebook account, 24 respondents who did not answer all questions, and 1 respondent who was a multivariate outlier due to choosing the first option for each answer over 45% of the time. The analyses that follow are based on the remaining 303 responses. Most respondents (96%) reported having an active Facebook account for more than a year. We asked respondents to report how many minutes per day on average they spent on Facebook in the preceding week. 33.6% of respondents reported spending one to more than 3 hours, 45.2% spent 10 minutes to an hour, and 20.5% spent fewer than 10 minutes on Facebook each day. Respondents had an average of 385 Facebook friends with a standard deviation of 333 and median of 300. Respondents covered a broad age range from 18 to 66 years (median: 27), with 74% females and 27% students. The majority of respondents were Caucasian (78%); 8% were African American, 4% Hispanic, and 6% Asian. Most respondents (96%) had attended college, with nearly 80% holding Bachelor's or advanced degrees. Reported occupations included stay-at-home mother, student, teacher, manager, consultant, etc. Some respondents were unemployed.

FINDINGS
We first ascertained the validity of our constructs. Next, we grouped respondents according to Privacy Fit and employed Partial Least Squares (PLS) based Structural Equation Modeling (SEM) using WarpPLS to test our hypothesized models [23]. We tested 10 separate models, one for each privacy boundary type.

Validity of Constructs
We evaluated construct validity by carrying out a confirmatory factor analysis and examining convergent validity, discriminant validity, and internal consistency of our measures [7]. The measures are included in the Appendix along with corresponding questionnaire items and factor analysis results. All constructs exceeded the recommended convergent validity cutoff values for Composite Reliability (CR) and Average Variance Extracted (AVE) of 0.7 and 0.5, respectively [15, 33]. To verify discriminant validity, we confirmed that the square root of the AVE was larger for each construct than the correlation between the construct and any other construct [6]. For internal consistency, prior research has recommended that loadings of individual items in factor analysis be at least 0.7 [33]. This criterion was met for all except two items: "I want to be able to choose what to share and what to hold back on Facebook." (*desired Self Disclosure*) and "My friends keep personal information they know about me between us." (*actual Confidant Disclosure*). However, we decided to retain these two items since the corresponding constructs met the requirements of CR and AVE. Given adequate construct validity of all measures, this analysis provided additional confirmation of the validity of the measurement scales we created for the 10 privacy boundary types.
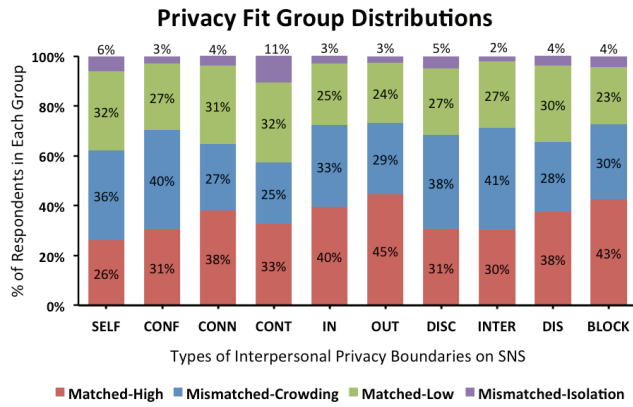
Figure 2. Distribution of respondents across the four Privacy Fit profiles for the 10 types of interpersonal privacy boundaries on SNS.

Boundary Type	H1 Connectedness → Bonding SC	H2 Connectedness → Bridging SC	H3 FBuse → Connectedness
SELF	0·54***	0·55***	1·20***
CONF	0·55***	0·52***	1·20***
CONN	0·55***	0·53***	1·24***
CONT	0·55***	0·54***	1·12***
IN	0·56***	0·53***	1·10***
OUT	0·53***	0·53***	1·39***
DISC	0·55***	0·53***	1·18***
INTER	0·55***	0·54***	1·10***
DIS	0·58***	0·55***	1·55***
BLOCK	0·56***	0·55***	1·06***

*** $p < 0.001$

Table 2. Model verification results: H1–H3.

Distribution of Privacy Fit

To assess Privacy Fit, we first created separate scales for desired and actual privacy by summing the responses to the individual scale items of each boundary type. These scales were then compared with the overall mean across all respondents for the corresponding boundary type. Scores lower than or equal to the mean were classified as 'low,' while those higher than the mean were marked as 'high.' Based on this classification for each of the 10 privacy boundary types, respondents were assigned to one of four groups indicating different Privacy Fit profiles: Mismatched-Crowding (high desired privacy, low actual privacy), Mismatched-Isolation (low desired privacy, high actual privacy), Matched-High (high desired privacy, high actual privacy), and Matched-Low (low desired privacy, low actual privacy). The Mismatched-Crowding and Mismatched-Isolation groups correspond to Altmans conceptualization of social crowding and social isolation, respectively [1]. Note that this classification was done per boundary type; i.e. a given respondent could be classified differently for each of the 10 privacy boundaries.

Figure 2 shows the distribution of respondents across the four Privacy Fit profiles for each of the 10 boundary types. The purple segments show that the Mismatched-Isolation groups were consistently much smaller than the other three groups. We chose to exclude the Mismatched-Isolation groups from further analyses since the small proportions of respondents (3% to 11%) in these groups did not provide sufficient power for meaningful statistical analysis.

Verification of Structural Models

After removing the Mismatched-Isolation group, three Privacy Fit groups remained: Mismatched-Crowding, Matched-High, and Matched-Low. Therefore, the Mismatched-Crowding group was used as the baseline for the structural models in Figure 1. For testing our moderating hypotheses, we employed a mean split to dichotomize Facebook Usage Intensity between casual and avid users. The final structural models for each of the 10 boundary types explained between 44–45% of the variance in Bridging Social Capital, 27–30% in Bonding Social Capital, and 27–31% in Social Connectedness. The explanatory power for the dependent variables in our models is comparable to that found in prior work (e.g., Ellison et al. [11] explained 44% of the variance in Bridging Social Capital and 23% in Bonding Social Capital, while Krasnova et al. [24] explained 26–35% of the variance in Social Connectedness) and is well beyond the recommended threshold of 10% as an indication of substantive explanatory power in the social sciences [12].

Facebook Use, Social Connectedness, and Social Capital
Hypotheses 1, 2, and 3 were supported for all 10 privacy boundary types. Table 2 provides corresponding path coefficients and p-values for the 10 structural models. The path coefficients are based on standardized factor scores. The values of path coefficients in Table 2 indicate that 1.00 standard deviation difference in Social Connectedness is related to a 0.53–0.58 standard deviation difference in Bridging Social Capital and 0.53–0.55 standard deviation difference in Bonding Social Capital. Further, there is a 1.06–1.39 standard deviation difference in Social Connectedness between casual and avid users. These results show that avid Facebook users reported higher levels of Social Connectedness (H3), and in turn, Social Connectedness helped them generate Bridging and Bonding Social Capital (H1 & H2).

Privacy Fit, Facebook Use, and Social Connectedness
Next, we tested the main effects of Privacy Fit on Social Connectedness (H4a & H5a) along with interaction effects between Privacy Fit and Facebook Usage Intensity (H4b & H5b). To understand the true nature of the relationship between Privacy Fit and Social Connectedness, main and interaction effects should be interpreted together. Table 3 provides corresponding path coefficients and p-values for each of the 10 privacy boundary types. Statistically significant path coefficients for H4a and H5a indicate a main effect of Privacy Fit on Social Connectedness such that Privacy Fit is associated with higher levels of Social Connectedness than Privacy Mismatch, independent of Facebook Usage Intensity. As Table 3 shows, our hypotheses were supported for all but two of the privacy boundary types (Inward Facing Territorial and Outward Facing Territorial) for the Matched-Low group and for all but three of the privacy boundary types (Self Disclosure, Confidant Disclosure, and Network Discovery) for the Matched-High group. However, taking interaction effects into account, the only cases when a Privacy Fit did not equate to significantly higher levels of Social Connectedness at ei-

Boundary Type	H4a Matched-Low → Social Connectedness	H4b Matched-Low x FBUse → Social Connectedness	H5a Matched-High → Social Connectedness	H5b Matched-High x FBuse → Social Connectedness
SELF	0·83***	−0·63***	0·09	0·06
CONF	0·80***	−0·76***	0·15	−0·05
CONN	0·43***	−0·31**	0·18*	−0·36**
CONT	0·23*	−0·48***	0·33***	0·18
IN	0·18	−0·38**	0·50***	−0·33***
OUT	0·01	−0·61***	0·38***	−0·49***
DISC	0·36***	−0·40***	0·09	−0·25*
INTER	0·33**	−0·23*	0·20*	−0·05
DIS	0·91***	−0·90***	0·71***	0·63***
BLOCK	0·23*	−0·34**	0·30**	0·07

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$

Table 3. Model verification results: H4ab - H5ab.

ther level of Facebook Usage Intensity were for the Matched-High group across the two Disclosure boundaries, i.e., Self Disclosure and Confidant Disclosure.

Table 3 also shows that H4b was consistently confirmed across all 10 boundary types: the difference in Social Connectedness between Matched-Low versus Mismatched-Crowding was larger for casual users than for avid users. However, H5b was confirmed for only half of the privacy boundary types (Relationship Connection, Inward Facing Territorial, Outward Facing Territorial, Network Discovery, and Interactional Disabling). Arguably, matching high desired levels of privacy for some of the other boundary types is beneficial for both casual and avid Facebook users because these boundaries regulate the flow of information; avid users benefit from this regulation as well, since it increases the effectiveness of their Facebook usage.

Since interaction effects can be hard to interpret using only the coefficients in Table 3, we include graphs of the interaction effects for the 10 privacy boundary types in Figure 3). As Social Connectedness is a latent factor, we set its value to zero for casual Facebook users in the Mismatched-Crowding group across all graphs. The graphs show the differences (in standard deviation terms) in Social Connectedness between the Mismatched-Crowding (blue), Matched-High (red), Matched-Low (green) groups, stratified by casual versus avid Facebook Usage Intensity. We provide tests of the effect of Privacy Fit separately for casual and avid users. In the graphs, an asterisk (*) over a bar signifies that a Privacy Fit (either Matched-High or Matched-Low) resulted in statistically significantly higher Social Connectedness than the Mismatched-Crowding group. Since we did not hypothesize any differences between the two Matched groups, we refrained from testing these differences, thus avoiding the need for post-hoc Bonferroni corrections.

The graphs in Figure 3 show that Matched-Low was consistently associated with greater Social Connectedness than Mismatched-Crowding for casual users (for whom the result was statistically significant for all privacy boundary types). For avid users, the corresponding association was statistically significant for only 2 out of the 10 boundary types (Relationship Connection and Interactional Disabling). Matched-High

was also associated with higher Social Connectedness than Mismatched-Crowding for 7 out of 10 boundary types for casual users (Relationship Connection, Relationship Context, Inward Facing Territorial, Outward Facing Territorial, Network Discovery, Interactional Disabling, and Interactional Blocking) and 4 out of 10 boundary types for avid users (Relationship Context, Inward Facing Territorial, Interactional Disabling, and Interactional Blocking). In other words, for all boundary types, Matched-Low was associated with higher Social Connectedness than Mismatched-Crowding, but primarily for casual users, and Matched-High was associated with higher Social Connectedness for a subset of the boundary types for both casual and avid users.

DISCUSSION
Our results point to a number of insights important for characterizing the SNS privacy discourse.

Contemporary SNSs May Encourage Oversharing
Our focus on Privacy Fit versus Privacy Mismatch led to the notable finding that very few of our participants experienced *social isolation*, (i.e., Mismatched-Isolation or more privacy than they desired). Figure 2 shows that this finding was consistent across the 10 privacy boundary types with only 3-11% of participants achieving higher levels of privacy than desired. This finding, combined with the predominance of people who attained low levels of privacy (i.e., Mismatched-Crowding or Matched-Low), confirms the common belief that SNSs tend to urge their users to share as much as possible [38]. This tactic may be based on the belief that social connectedness and social capital can be increased only via pervasive sharing. Our results show that this belief is mistaken. A practical implication of our findings, therefore, would be the importance of questioning the social norms, values, motivations, and assumptions that currently drive SNS interface design.

Privacy May Enhance, Not Hinder Social Connection
If plentiful and strong social connections required unbounded openness and sharing, then one would expect the highest levels of Social Connectedness from avid Facebook users who desired and achieved low levels of privacy (Matched-Low). However, Figure 3 indicates that such a relationship is unequivocally true for only Relationship Connection, not for
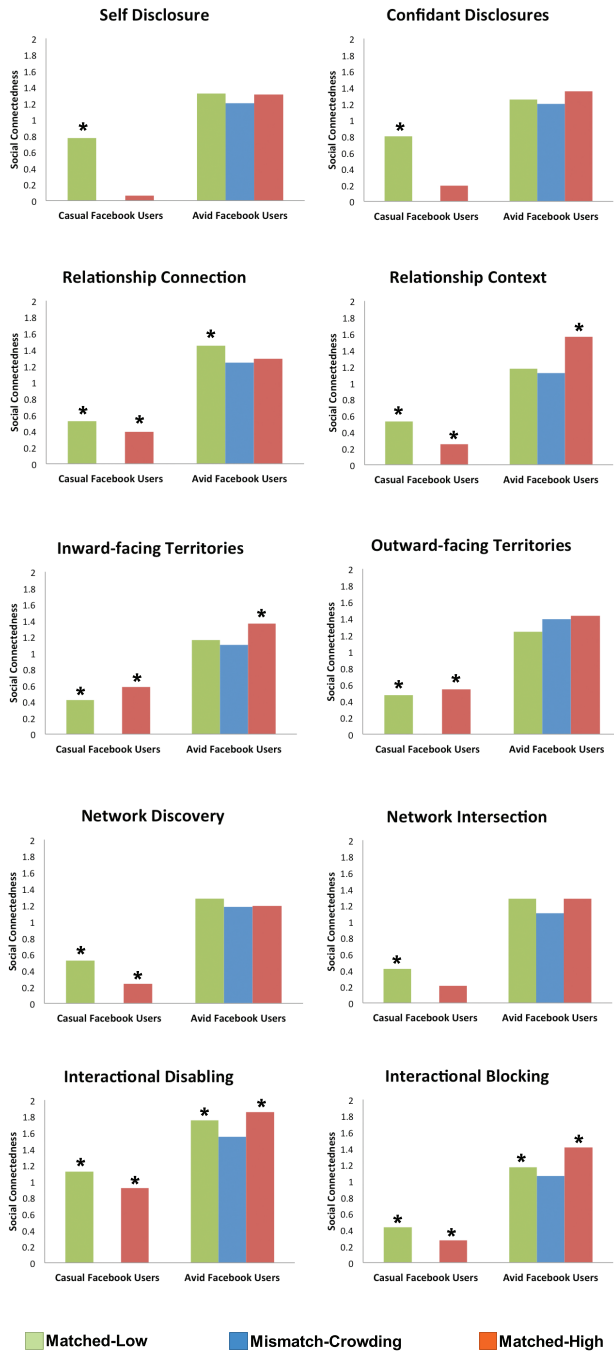
Figure 3. Interaction effects between Privacy Fit and Facebook Usage Intensity for each privacy boundary type.

any other privacy boundary types. This finding suggests that when users desire and acquire a large and open network of friends, family, acquaintances, and strangers, they tend to have higher levels of Social Connectedness. Yet, Figure 3 also shows that avid Facebook users who desired and achieved high levels of privacy (Matched-High) perceived the highest level of Social Connectedness for 3 of the 10 boundary types (Relationship Context, Inward Facing Territorial, Interactional Blocking). Further, the positive effect of Pri-

vacy Fit at high privacy levels is even more prominent for casual Facebook users. Indeed, casual Facebook users in the Matched-High group perceived higher levels of Social Connectedness across 7 of the 10 privacy boundary types (note that in these cases the Matched-Low group often perceived even higher levels of Social Connectedness).

Overall, these findings suggest that supporting certain privacy boundaries may actually aid in building intimate social connections instead of hindering them, especially at casual usage levels. For example, both casual and avid users who wish and believe that they can closely manage their Inward Facing Territorial boundaries, such as filtering the Facebook News Feed in order to see only the content from friends that matter the most to them, also reported the highest levels of Social Connectedness.

Social Connectedness as a Mediator

H1 and H2 confirmed a positive relationship between Social Connectedness and Bridging and Bonding Social Capital. Consequently, Social Connectedness *mediates* the effects of Privacy Fit and Facebook Usage Intensity on the two types of Social Capital. We tested whether this mediation is a *full mediation* with saturated models [16] which included six additional paths that examined direct effects of Facebook Usage Intensity and Privacy Fit on Bridging and Bonding Social Capital. All statistically significant path coefficients in the original hypothesized models remained statistically significant in the saturated models. Moreover, only one of the additional paths in the saturated models was statistically significant: the direct path from Facebook Usage Intensity to Bridging Social Capital, which is consistent with the strong relationship between the two shown by past research [9]. The analysis of the saturated models implies that Social Connectedness fully mediates the relationship between Facebook Usage Intensity and Bonding Social Capital and partially mediates the relationship between Facebook Usage Intensity and Bridging Social Capital. The effect of Privacy Fit and its interaction with Facebook Usage Intensity on the two types of social capital is also fully mediated by Social Connectedness. The fully mediated relationships suggest that Social Connectedness is an important factor that should be taken into account in future studies that address social capital generation and maintenance via SNSs.

Privacy Fit Matters Most for Casual SNS Users

The effect of Privacy Fit was most prominent for casual Facebook users. For these users, Privacy Fit was almost always associated with higher levels of Social Connectedness than Privacy Mismatch. Arguably, due to the lower levels of Facebook Usage Intensity, casual SNS users need to 'make every interaction count.' Therefore, fulfillment of privacy expectations might have a stronger influence on their overall perception of online connections. In contrast, avid users, who use Facebook frequently, to the point where it is highly enmeshed in their daily lives, likely derive Social Connectedness as a natural side-effect of active participation. As a result, they may become less attentive to Privacy Mismatch due to habituation. Alternatively, they may downplay any Privacy

Mismatch as a means to achieve uniformity between their privacy cognition and their high levels of Facebook Use (i.e., to reduce cognitive dissonance).

To further explore the interplay between Privacy Fit and Facebook Usage Intensity, we tested the direct path from Privacy Fit to Facebook Usage Intensity. We found a statistically significant positive relationship (for either Matched-Low or Matched-High) for 7 out of the 10 the boundary types. Compared to Privacy Mismatch, Privacy Fit was associated with higher Facebook Usage Intensity about 40% of the time; users whose privacy desires were satisfied used Facebook more intensely than those with unmet privacy needs. Privacy Fit thus creates a virtuous cycle, leading casual users to feel more socially connected as well as increase their Facebook Usage Intensity, thereby further increasing Social Connectedness. We must also point out that a subset of casual Facebook users in our sample may have been relatively new to Facebook and, as a result, yet to achieve avid usage. Therefore, our findings suggest that early achievement of Privacy Fit may be crucial to ensuring that such users increase participation and achieve greater connectedness over time. A longitudinal study could provide important insight regarding this potential accelerating effect of Privacy Fit on the evolution of SNS practices.

Privacy Is More Complex than Information Disclosure

SNS users manage their social interactions in a number of ways, including but not limited to information disclosure. Our findings were consistent with past research that suggested the necessity for some trade-off between privacy and social benefits when it comes to information disclosure on SNSs [44]; only users who desired and achieved low levels of disclosure privacy reported significantly higher levels of social connectedness (see the results for the Self Disclosure and Confidant Disclosure boundaries in Table 3 and Figure 3). However, treating privacy only in terms of information disclosure provides an incomplete picture. Among the 10 privacy boundary types in our models, the information disclosure privacy boundaries (Self Disclosure and Confidant Disclosure) were in fact the least affected by Privacy Mismatch. When privacy boundaries other than information disclosure were considered, we found that Privacy Fit could lead to more Social Connectedness, even when users desired and achieved high levels of privacy.

The psychometric properties of our models confirmed the discriminant validity of the 10 different privacy boundary types, emphasizing the need to broaden the conceptualization of privacy in future research. Our validated scales can be used and/or modified for future SNS privacy studies to help broaden privacy measures beyond private versus public information disclosure. The consistency of our results across the 10 boundary types confirms the robustness of these scales. At the same time, the interaction graphs (Figure 3) illustrate unique and nuanced differences between the 10 boundary types that enrich our overall understanding of privacy.

IMPLICATIONS FOR DESIGN

To our knowledge, our models are the first to assess the effects Privacy Fit — the match between desired and achieved

levels of privacy — on Social Connectedness and Social Capital within the context of SNSs. We first point to a potentially fruitful design direction focusing on Privacy Fit, followed by ethical considerations when pursuing this direction.

A Call for User-Tailored Privacy Design

Overall, we found strong support that Privacy Fit is associated with higher levels of Social Connectedness than Privacy Mismatch, especially for casual users. Yet, the large proportion of users who experienced a lack of Privacy Fit — i.e., social crowding (see Figure 2) — confirms reports that SNS users have a hard time translating their desired privacy level into concrete interface actions [30]. As our study illustrates, users have the complex task of maintaining no less than 10 types of interpersonal privacy boundaries; attaining Privacy Fit across all these boundaries is a formidable task. Our results show that SNS providers seeking to maximize the benefits of their service should opt to *help their users attain Privacy Fit*, rather than urge them to share as much as possible. However, as SNS users vary wildly in their desired level of privacy [34], this is not simply a matter of urging them to share less (e.g., using *privacy nudging*, cf. [48]), because that could force some users from the Matched-Low group into the Mismatched-Isolation group.

The best solution, then, may be to move beyond the one-size-fits-all approach to privacy towards 'user tailored' [22] privacy design that personalizes the conceptualization and operationalization of privacy to fit the unique needs of each user. Existing work on user tailored privacy shows that users' privacy preferences can be predicted with a reasonable level of accuracy [3, 13, 40, 41]. Given the large amount of personal user data SNSs collect (implicitly via interaction traces as well as explicitly via user input), they may already be equipped with the resources necessary to explore such personalization. Alternatively, 'privacy profiles' can be created to characterize SNS users based on the strategies they employ for attaining their privacy needs [51]. In sum, the work on privacy personalization shows that it is *possible* to predict SNS users' personal privacy preferences and then help them meet these desires. Our work further motivates existing work on privacy personalization within SNSs by empirically demonstrating the importance and benefits of leveraging these user tailored approaches to help users attain Privacy Fit.

Ethical Considerations

Some argue that the interests of SNS providers are inherently in conflict with privacy needs of SNS users, thus leading providers to promote and normalize openness and sharing with little regard to privacy [31]. Our Privacy Fit profile distributions (Figure 2) lend some credence to this claim by showing that it is rare for Facebook users to achieve high privacy levels unless driven by a strong personal desire for privacy; few users in our sample achieved high levels of privacy despite desires for low levels.

Our findings support an alternative design approach that helps users be more effective in attaining the level of privacy they desire: "Give SNS users the privacy they want," whether this is a lot of privacy, little privacy, or no privacy at all. Our work

demonstrates the *doubly beneficial* effect of Privacy Fit — enhancing Privacy Fit may not only reduce privacy concerns for the users themselves, but may also enrich SNS interactions and encourage greater participation from casual users, which is typically in the interest of the SNS provider. Thus, such an approach has the potential to enhance the interactional benefits derived by SNS users and would likely serve the commercial interests of SNS providers and affiliated advertisers. Yet, as designers and privacy researchers, we must also raise the ethical question of whether striving to meet users' privacy desires is always the right course of action. Instead, it may sometimes be necessary to influence a *change* in these desires (e.g., by nudging users toward choices that provide more privacy [48] or educating them about potential consequences of reduced privacy). While this ethical debate is beyond the scope of this paper, we mention it here to emphasize that user tailored privacy design may involve more than simply giving users what they want.

LIMITATIONS AND FUTURE RESEARCH

While our structural models imply causal directions, it must be kept in mind that such models cannot confirm or disprove causality. When we report that a match between desired and actual privacy levels is associated with higher Social Connectedness, we essentially confirm that the two are correlated. The hypothesized causal direction (Privacy Fit → Social Connectedness) is based on Altman's theory, not on explicit confirmation by our analyses. It is possible that higher Social Connectedness leads users to feel that their privacy needs are being met rather than vice versa. Given that prior research has found it challenging to resolve the apparent conflict between privacy and social networking benefits, the positive association is noteworthy regardless of causal direction.

Further, we examined only one type of mismatch between desired and actual privacy, i.e., social crowding. Although research within social psychology makes a theoretical distinction between social crowding and social isolation [1], analysis of the latter (i.e., Mismatched-Isolation) was statistically infeasible due to the dearth of participants in this category. Therefore, our findings and implications regarding Privacy Mismatch apply only when SNS users achieve less privacy than they desire. Additionally, our sample has an inherent self-selection bias and is therefore skewed toward Facebook users who are well-educated, Caucasian, and female adults from the US. Further research is needed to ascertain generalizability to the populations of the US and other countries.

Our work motivates a number of directions for future research. For example, past studies that examined SNS outcomes in terms of information disclosure may benefit from replication to confirm whether their findings remain stable across our broader conceptualization of SNS privacy as interactional boundary regulation. Follow up studies may also examine how SNS users' privacy management strategies influence their subsequent perception of Privacy Fit. Additionally, longitudinal investigations are needed to examine how our current findings hold up as the interactive capabilities and privacy interfaces of SNSs undergo changes, as SNS users gain experience, and as social norms related to SNS usage evolve.

CONCLUSION

The interactive benefits of using SNSs are often described as being in conflict with people's desire for personal privacy. Therefore, proponents of online social networking often advocate for open and 'frictionless' sharing with little regard for privacy [8, 31]. However, disregarding users' privacy concerns may either encourage SNS users to overshare [49] or, alternatively, to curtail or even cease their SNS usage altogether [2, 52, 53], limiting the potential social benefits of SNSs. Social psychologists remind us that sharing too much and too soon can be just as detrimental as social isolation [1,37]. Therefore, the key to optimizing the interactional benefits of SNS use may be to tailor privacy to fit the unique needs of each individual user. Indeed, our findings show that SNS users can fulfill their desires for privacy without sacrificing social benefits. In fact, doing so may actually enhance their social interactions with others. Moreover, our results suggest that enabling users to meet their privacy needs could serve the interests SNS providers as well. Thus, we believe that promoting a fit between users' desired and achieved SNS privacy is a step toward reconciling the tension between the goals of privacy and online social networking.

REFERENCES

1. Altman, I. *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks/Cole Publishing Company, Monterey, CA, USA, 1975.

2. Baumer, E. P., Adams, P., Khovanskaya, V. D., Liao, T. C., Smith, M. E., Schwanda Sosik, V., and Williams, K. Limiting, leaving, and (re)lapsing: An exploration of facebook non-use practices and experiences. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, ACM (New York, NY, USA, 2013), 3257–3266.

3. Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M., and Hubaux, J.-P. Adaptive information-sharing for privacy-aware mobile social networks. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, ACM (New York, NY, USA, 2013), 657–666.

4. Boyle, M., and Greenberg, S. The language of privacy: Learning from video media space analysis and design. *ACM Trans. Comput.-Hum. Interact. 12*, 2 (June 2005), 328–370.

5. Burke, M., Marlow, C., and Lento, T. Social network activity and social well-being. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, ACM (New York, NY, USA, 2010), 1909–1912.

6. Campbell, D. T., and Fiske, D. W. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological bulletin 56*, 2 (1959), 81.

7. Cook, T. D., Campbell, D. T., and Day, A. *Quasi-experimentation: Design & analysis issues for field settings*. Houghton Mifflin, Boston, MA, USA., 1979.

8. Eler, A. Top trends of 2011: Frictionless sharing, December 2011. `http://readwrite.com/2011/12/14/top_trends_of_2011_frictionless_sharing`.

9. Ellison, N. B., Steinfield, C., and Lampe, C. The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication 12*, 4 (2007), 1143–1168.

10. Ellison, N. B., Steinfield, C., and Lampe, C. Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society 13*, 6 (2011), 873–892.

11. Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., and Lampe, C. Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy Online*, S. Trepte and L. Reinecke, Eds. Springer Berlin Heidelberg, 2011, 19–32.

12. Falk, R. F., and Miller, N. B. *A primer for soft modeling*. University of Akron Press, Akron, OH, USA, 1992.

13. Fang, L., and LeFevre, K. Privacy wizards for social networking sites. In *Proceedings of the 19th International Conference on World Wide Web*, WWW '10, ACM (New York, NY, USA, 2010), 351–360.

14. Festinger, L. *A theory of cognitive dissonance*, vol. 2. Stanford University Press, Palo Alto, CA, USA, 1962.

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

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

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

18. Iachello, G., and Abowd, G. D. Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, ACM (New York, NY, USA, 2005), 91–100.

19. Karr-Wisniewski, P., Wilson, D., and Richter-Lipford, H. A new social order: Mechanisms for social network site boundary regulation. In *Americas Conference on Information Systems*, AMCIS 2011 (2011).

20. Katherine, A. *Boundaries Where You End and I Begin: How to Recognize and Set Healthy Boundaries*. Hazelden Publishing, 1994.

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

22. Knijnenburg, B. P. Simplifying privacy decisions: Towards interactive and adaptive solutions. In *Workshop on Human Decision Making in Recommender Systems*, Decisions@ RecSys '13 (2013), 40–41.

23. Kock, N. WarpPLS 4.0 user manual, 2010. `http://scriptwarp.com/warppls/UserManual_v_4_0.pdf`.

24. Koroleva, K., Krasnova, H., Veltri, N., and Günther, O. It's all about networking! Empirical investigation of social capital formation on social network sites. In *International Conference on Information Systems*, ICIS 2011 (2011).

25. Lampinen, A., Lehtinen, V., Lehmuskallio, A., and Tamminen, S. We're in it together: Interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, ACM (New York, NY, USA, 2011), 3217–3226.

26. Langheinrich, M. Privacy by design — principles of privacy-aware ubiquitous systems. In *Proceedings of the Third International Conference on Ubiquitous Computing*, UbiComp '01, Springer-Verlag, Springer-Verlag (London, UK, 2001), 273–291.

27. Laufer, R. S., and Wolfe, M. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues 33*, 3 (1977), 22–42.

28. Limayem, M., Hirt, S. G., and Cheung, C. M. How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly 31*, 4 (2007), 705–737.

29. Lipford, H. R., Wisniewski, P. J., Lampe, C., Kisselburgh, L., and Caine, K. Reconciling privacy with social media. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work Companion*, CSCW '12, ACM (New York, NY, USA, 2012), 19–20.

30. Madden, M. Privacy management on social media sites. Tech. rep., Pew Research Center's Internet & American Life Project, Washington, DC, USA, February 2012. `http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf`.

31. Matyszczyk, C. Zuckerberg: I know that people don't want privacy, February 2010. `http://news.cnet.com/8301-17852_3-10431741-71.html`.

32. Moore, G. C., and Benbasat, I. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information systems research 2*, 3 (1991), 192–222.

33. Nunnally, J. C. *Psychometric Theory*, 2nd ed. McGraw-Hill, New York, NY, USA, 1978.

34. Olson, J. S., Grudin, J., and Horvitz, E. A study of preferences for sharing and privacy. In *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '05, ACM (New York, NY, USA, 2005), 1985–1988.

35. Page, X., Kobsa, A., and Knijnenburg, B. P. Don't disturb my circles! Boundary preservation is at the center of location-sharing concerns. In *The Sixth International AAAI Conference on Weblogs and Social Media*, ICWSM 2012 (2012).

36. Palen, L., and Dourish, P. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, ACM (New York, NY, USA, 2003), 129–136.

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

38. Rainie, L., Kiesler, S., Kang, R., and Madden, M. Anonymity, privacy, and security online. Tech. rep., Pew Research Center's Internet & American Life Project, Washington, DC, USA, Sept. 2013. `http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf`.

39. Rainie, L., Smith, A., and Duggan, M. Coming and going on Facebook. Tech. rep., Pew Research Center's Internet & American Life Project, Washington, DC, USA, February 2013. `http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Coming_and_going_on_facebook.pdf`.

40. Ravichandran, R., Benisch, M., Kelley, P. G., and Sadeh, N. M. Capturing social networking privacy preferences: Can default policies help alleviate tradeoffs between expressiveness and user burden. In *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*, PETS '09, Springer-Verlag (Berlin, Heidelberg, 2009), 1–18.

41. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing 13*, 6 (2009), 401–412.

42. Straub, D., Boudreau, M.-C., and Gefen, D. Validation guidelines for IS positivist research. *Communications of the Association for Information Systems 13*, 1 (2004), 380–427.

43. Stutzman, F., and Hartzog, W. Boundary regulation in social media. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, CSCW '12, ACM (New York, NY, USA, 2012), 769–778.

44. Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., and Lampe, C. Privacy in interaction: Exploring disclosure and social capital in Facebook. In *The Sixth International AAAI Conference on Weblogs and Social Media*, ICWSM 2012 (2012).

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

46. Valenzuela, S., Park, N., and Kee, K. F. Lessons from Facebook: The effect of social network sites on college students' social capital. In *9th International Symposium on Online Journalism* (2008).

47. Valenzuela, S., Park, N., and Kee, K. F. Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust, and participation. *Journal of Computer-Mediated Communication 14*, 4 (2009), 875–901.

48. Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., and Sadeh, N. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, ACM (New York, NY, USA, 2014), 2367–2376.

49. Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., and Cranor, L. F. "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, ACM (New York, NY, USA, 2011), 10:1–10:16.

50. Williams, D. On and off the 'Net: Scales for social capital in an online era. *Journal of Computer-Mediated Communication 11*, 2 (2006), 593–628.

51. Wisniewski, P., Knijnenburg, B. P., and Richter Lipford, H. Profiling facebook users' privacy behaviors. In *SOUPS 2014 Workshop on Privacy Personas and Segmentation* (2014).

52. Wisniewski, P., Lipford, H., and Wilson, D. Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, ACM (New York, NY, USA, 2012), 609–618.

53. Wisniewski, P., Xu, H., and Chen, Y. Understanding user adaptation strategies for the launching of facebook timeline. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, ACM (Toronto, Canada, 2014), 2421–2430.

54. Wisniewski, P. J. *Understanding and Designing for Interactional Privacy Needs Within Social Networking Sites*. PhD thesis, University of North Carolina at Charlotte, Charlotte, NC, USA, 2012. AAI3527994.

APPENDIX

The Tables below provide the items used for operationalizing our constructs in the questionnaire.

Facebook Usage Intensity ($CR = 0.92$, $AVE = 0.67$)	**Loading**
Facebook is part of my everyday activity.	0·86
I am proud to tell people I'm on Facebook.	0·75
Facebook has become part of my daily routine.	0·88
I feel out of touch when I haven't logged onto Facebook for a while.	0·81
I feel I am part of the Facebook community.	0·84
I would be sorry if Facebook shut down.	0·77

Table 4. Facebook Usage Intensity items.

Social Connectedness ($CR = 0.89$, $AVE = 0.58$)	**Loading**
On Facebook, I feel close to the people in my friend list.	0·76
On Facebook, I have a feeling of being connected to others.	0·79
On Facebook, I am updated about my friends.	0·64
On Facebook, I stay in touch with my friends.	0·81
On Facebook, I keep in contact with the people in my friend list.	0·80
Now that I use Facebook, I interact with my friends more.	0·74

Table 5. Social Connectedness items.

Bridging Social Capital ($CR = 0.95$, $AVE = 0.65$)	**Loading**
Talking with people on Facebook makes me curious about other places in the world.	0·79
Interacting with people on Facebook makes me feel like a part of a larger community.	0·85
Interacting with people on Facebook reminds me that everyone in the world is connected.	0·78
Interacting with people on Facebook makes me want to try new things.	0·83
Interacting with people on Facebook gives me new people to talk to.	0·79
I am willing to spend time to support general Facebook community activities.	0·76
On Facebook, I come into contact with new people all the time.	0·72
Interacting with people on Facebook makes me interested in things that happen outside of my town.	0·87
Interacting with people on Facebook makes me interested in what people unlike me are thinking.	0·80
Interacting with people on Facebook makes me feel connected to the bigger picture.	0·86

Table 6. Bridging Social Capital items.

Bonding Social Capital ($CR = 0.91$, $AVE = 0.63$)	**Loading**
There are several people on Facebook I trust to solve my problems.	0·82
The people I interact with on Facebook would help me fight an injustice.	0·79
There is someone on Facebook I can turn to for advice about making very important decisions.	0·85
The people I interact with on Facebook would put their reputation on the line for me.	0·82
When I feel lonely, there are several people on Facebook I can talk to.	0·75
If I needed an emergency loan of $500, I know someone on Facebook I can turn to.	0·73

Table 7. Bonding Social Capital items.

Desired Privacy		**Actual Privacy**	
Self Disclosure ($CR = 0.80, AVE = 0.57$)	**Loading**	**Self Disclosure** ($CR = 0.91, AVE = 0.78$)	**Loading**
I do not want to post very intimate things about myself on Facebook.	0·78	I post very intimate things about myself on Facebook.	0·89
I want to share only minimal information about myself on Facebook.	0·82	I share only minimal information about myself on Facebook.	0·88
I want to be able to choose what to share and what to hold back on Facebook.	0·65	I choose what to share and what to hold back on Facebook.	0·88
Confidant Disclosure ($CR = 0.82, AVE = 0.60$)	**Loading**	**Confidant Disclosure** ($CR = 0.75, AVE = 0.51$)	**Loading**
I do not want my friends to tag me in photos or posts without my permission.	0·77	My friends do not tag me in photos or posts without my permission.	0·75
I want to limit what personal information my friends share about me on Facebook.	0·81	I limit what personal information my friends share about me on Facebook.	0·81
I want my Facebook friends to keep personal information they know about me between us.	0·75	My friends keep personal information they know about me between us.	0·55
Relationship Connection ($CR = 0.85, AVE = 0.66$)	**Loading**	**Relationship Connection** ($CR = 0.84, AVE = 0.64$)	**Loading**
I only want people in my Facebook social network who I associate with on a regular basis in real life.	0·82	I only have people in my Facebook social network who I associate with on a regular basis in real life.	0·79
I do not want to have Facebook friends who are no longer real friends.	0·80	I do not have Facebook friends who are no longer real friends.	0·77
I only want to accept intimate friends and family members as Facebook friends.	0·82	I only accept intimate friends and family members as Facebook friends.	0·83
Relationship Context ($CR = 0.83, AVE = 0.62$)	**Loading**	**Relationship Context** ($CR = 0.82, AVE = 0.57$)	**Loading**
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	I make a distinction between my friends based on the type of relationship I have with them. For example, family, friends, co-workers, etc.	0·70
I want my interactions on Facebook to be different between me and a close friend than they would be with an acquaintance.	0·82	My interactions on Facebook are different between me and a close friend than they would be with an acquaintance.	0·79
I want my one-on-one interactions on Facebook to be appropriate and unique based on my relationship with that specific person.	0·76	My one-to-one interactions on Facebook are appropriate and unique based on my relationship with that specific person.	0·78
Inward Facing Territorial ($CR = 0.83, AVE = 0.62$)	**Loading**	**Inward Facing Territorial** ($CR = 0.89, AVE = 0.73$)	**Loading**
I want to pick and choose what kinds of updates show up in my News Feed.	0·81	I pick and choose what kinds of updates show up in my News Feed.	0·84
I want to decide whose updates show up in my News Feed.	0·80	I decide whose updates show up in my News Feed.	0·88
I want to hide News Feed updates from others that I would rather not see.	0·76	I hide News Feed updates from others that I would rather not see.	0·84

. . . continued from previous page.

Desired Privacy		**Actual Privacy**	
Outward Facing Territorial ($CR = 0.79, AVE = 0.56$)	**Loading**	**Outward Facing Territorial** ($CR = 0.84, AVE = 0.64$)	**Loading**
I want to remove any content I do not want from my Timeline/Wall.	0·70	I remove any content I do not want from my Timeline/Wall.	0·79
I want to manage everything that shows up on my Timeline/Wall for others to see.	0·83	I manage everything that shows up on my Timeline/Wall for others to see.	0·85
I want to approve all content before it is posted to my Facebook Timeline/Wall	0·72	I approve all content before it is posted to my Facebook Timeline/Wall.	0·75
Network Discovery ($CR = 0.82, AVE = 0.59$)	**Loading**	**Network Discovery** ($CR = 0.89, AVE = 0.74$)	**Loading**
I do not want others to have access to my friends through my Facebook friend list.	0·71	Others do not have access to my friends through my Facebook friend list.	0·92
I want to restrict others in my network from being able to see who I am and am not friends with on Facebook.	0·83	I restrict others in my network from being able to see who I am and am not friends with on Facebook.	0·86
I want to hide my friend list so that others cannot browse my Facebook friends.	0·77	I hide my friend list so that others cannot browse my Facebook friends.	0·89
Network Intersection ($CR = 0.86, AVE = 0.68$)	**Loading**	**Network Intersection** ($CR = 0.90, AVE = 0.74$)	**Loading**
I want to avoid letting specific groups of friends interact with each other on Facebook.	0·80	I avoid letting specific groups of friends interact with each other on Facebook.	0·87
I want to keep my different social circles separate from each other on Facebook.	0·86	I keep my different social circles separate from each other on Facebook.	0·84
I want to moderate how my different groups of friends interact with one another on my Facebook page.	0·81	I moderate how my different groups of friends interact with one another on my Facebook page.	0·88
Interactional Disabling ($CR = 0.82, AVE = 0.60$)	**Loading**	**Interactional Disabling** ($CR = 0.90, AVE = 0.76$)	**Loading**
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.	0·72	I turn off chat, my Wall, or other Facebook features that allow others to interact with me anytime they want to.	0·91
I want to disable the ability for my friends to contact me on Facebook when I want to be left alone.	0·82	I disable the ability for my friends to contact me on Facebook when I want to be left alone.	0·82
I want to limit the different ways my friends can communicate with me via Facebook.	0·79	I limit the different ways my friends can communicate with me via Facebook.	0·88
Interactional Blocking ($CR = 0.83, AVE = 0.63$)	**Loading**	**Interactional Blocking** ($CR = 0.86, AVE = 0.68$)	**Loading**
I want to prevent some people on Facebook from having any access to me what-so-ever.	0·78	I prevent some people on Facebook from having any access to me what-so-ever.	0·82
When I do not want to interact with someone anymore, I want to be able to sever all contact with them on Facebook.	0·74	When I do not want to interact with someone anymore, I sever all contact with them on Facebook.	0·78
I want to block certain people from finding me or knowing what I am up to on Facebook.	0·85	I block certain people from finding me or knowing what I am up to on Facebook.	0·87

Table 8. Items for measuring *desired* and *achieved* privacy across the 10 interpersonal boundary types on SNS.