Between Nuance and Rigor: Contextualizing and Measuring SNS Desired Privacy Level

Pamela Wisniewski

College of Information Sciences
and Technology
The Pennsylvania State University
pam@pamspam.com

Heather Richter Lipford

Department of Software and
Information Systems
University of North Carolina at
Charlotte
Heather.Lipford@uncc.edu

Abstract

Privacy concern is difficult to measure without adequate context. We describe our approach to developing a contextualized measure for Social Network Site privacy that we have used to explore the relationship between desired privacy and actual behavior.

Author Keywords

Social Network Sites, Privacy, Interpersonal Boundary Regulation

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

Introduction

Privacy, as a measureable construct, is elusive at best. However, this is a shared problem across all social constructs because they simply cannot be objectively measured. For instance, depression, anxiety, social connectedness, neuroticism, and many others emerging from social psychology can arguably be just as embedded in their respective contexts as one's concern for privacy. As social scientists, we have to acknowledge that *context is everything*. In fact, Human-Computer Interaction (HCI) networked privacy

research has adopted the social informatics perspective of context-dependency (Sawyer and Tapia 2007) to the extent that many HCI researchers reject positivist approaches and heavily favor qualitative nuance over statistical rigor. Our position is that quantitative measures for Social Network Site (SNS) privacy can reflect context when grounded in qualitative, empirical theory. By combining qualitative and quantitative approaches, we can best tackle the "three-horned dilemma" of all research methodologies, which is optimizing precision, realism, and generalizability (McGrath, Martin et al. 1982).

We developed a second-order construct for SNS desired privacy level based on a qualitatively derived taxonomy of SNS boundary types. By contextualizing and measuring one's desired privacy level by more granular boundary types, we were able to show a statistically significant relationship between desired privacy level and one's actual privacy behaviors. However, we also uncovered that various other factors, such as feature awareness, moderate the relationship between one's SNS desired privacy level and actual privacy behaviors. We consider this is a first step in unpacking the "privacy paradox" (Barnes 2006).

Background

Altman defines 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 (Altman 1975). However, privacy within the SNS research community is often defined as "the ability of individuals to control when, to what extent, and how information about the self is communicated to others" (Ellison, Vitak et al. 2011). Thus, focusing specifically on the boundary between

private versus public disclosures (Lampinen, Lehtinen et al. 2011). Yet, this definition has moved away from Altman's conceptualization of privacy as an "interpersonal event" enmeshed in relationships for optimally regulating one's social interactions (Altman 1975). We believe that SNS privacy boundaries extend beyond information disclosure to also include more nuanced types of interactional relationship management. Therefore, we contextualized SNS privacy by first trying to understand the types of interpersonal privacy boundaries SNS users manage. With this in-depth understanding, we were then able to measure the relationship between one's desired privacy level and their privacy behaviors.

Contextualizing Privacy

We first combined two qualitative approaches to develop a taxonomy of interpersonal boundary types within SNSs. We systematically identified prominent interface controls that could be leveraged for interpersonal boundary regulation on five popular SNSs: Facebook, MySpace, LinkedIn, Hi5, and Ning. Features were abstracted and conceptually grouped to lay the foundation of the taxonomy. Next, we conducted and analyzed semi-structured interviews of SNS users asking them how they managed their SNS social interactions. The final taxonomy is shown in Table 1 (Wisniewski, Lipford et al. 2011).

Operationalizing Privacy

We then operationalized desired privacy level as the desire to open or close oneself (Altman 1975) with respect to the different types of interpersonal boundaries identified in our taxonomy. We modeled each desired privacy level type as a reflective construct, where the individual measures all represent

the underlying construct and are expected to be correlated (Freeze and Raschke 2007). We did this by compiling a list of initial item pools to measure each dimension based on quotes from qualitative interviews and the review of the literature. We simplified item wordings and removed redundant items. Following the "rule of three (Freeze and Raschke 2007)," we chose three items to measure desired privacy level for each of the ten boundary types. To pre-validate the measures of the different types of SNS desired privacy for discriminant validity, we applied established q-sorting (card sorting) techniques (Moore 1991; Straub 2004). We performed five rounds of card sorting where participants were asked to electronically sort items into pre-defined, and items were revised subsequent to each round. The accuracy rates suggested adequate initial construct validity for SNS desired privacy level (Moore 1991; Straub 2004). We present the full set of measures for desired privacy level in Table 1 (Wisniewski 2012).

Examining Desired Privacy and Privacy Behaviors

To validate our new measures for SNS desired privacy level with respect to the ten boundary types, we collected responses from 308 Facebook users through a web-based survey. We also captured other relevant factors, such as perceived risk, actual privacy behaviors, privacy feature awareness, and burden of use. We did this by asking participants to log into their Facebook accounts and report various privacy settings and feature usage. Data were screened for missing data, outliers, and normality prior to analysis. We first conducted a confirmatory factor analysis (CFA) of the measures to assess convergent validity, discriminant validity, and internal consistency of the constructs. We then tested the models using structural equation modeling (SEM) in two steps. First, we tested the SEM model without the moderating effects to obtain general model fit. Then we conducted a latent interaction analysis in order to appropriately test the moderation effects. We created separate SEMs for each of the ten theoretically derived types of privacy boundaries from the taxonomy. Data were analyzed using MPlus covariance SEM.

We found adequate construct validity for our new measures for SNS desired privacy level (Wisniewski, 2012), though construct validity could be improved further by revising some of the item wording. In addition, for half of the boundary types (inward-facing territories, network discovery, interactional blocking, interactional disabling, and self disclosure), we found a positive and statistically significant relationship between one's desired privacy level and one's privacy behaviors, contrary to previous privacy paradox research. For three of the models (outward-facing territories, relationship connection, and confidant disclosures), the relationship between desired privacy level and privacy behaviors was contingent on various moderating factors. For outward-facing territories, high levels of perceived risk and low perceived burden strengthened the relationship between desire and behavior. For relationship connection, self awareness, risk awareness, and feature awareness all had an impact on the relationship. Finally, for confidant disclosures, high levels of risk awareness strengthened the relationship between desire and behavior.

Only for two of the models, network intersection and relationship context, did we not find any relationship between desired privacy level and privacy behaviors –

reminiscent of the privacy paradox. However, returning to our previous interviews, we uncovered that the creation and use of friend lists to manage relationship context and network intersection boundaries seem to be woefully inadequate in current interfaces for meeting one's privacy needs, signaling the need for improved interface design. We believe that a possible explanation, then, for the "paradox", could be the lack of technological affordances available to adequately manage one's desired privacy level for these boundaries. This explanation requires additional research to more deeply examine.

Conclusion

Our research shows the importance of contextualizing privacy through qualitative measures, so that we can measure privacy and its relationship with other constructs in meaningful ways. By operationalizing SNS desired privacy level at a more granular level, we were able to unpack, if not disprove, aspects of the privacy paradox as well as uncover potential areas for future investigation and design.

References

[1]   Altman, I. (1975). The environment and social behavior, Brooks/Cole Monterey, CA.
[2]   Barnes, S. B. (2006). A privacy paradox: Social networking in the United States.
[3]   Ellison, N. B., J. Vitak, et al. (2011). Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environments. Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Heidelberg and New York, Springer.
[4]   Freeze, R. D. and R. L. Raschke (2007). An Assessment of Formative and Reflective Constructs in IS Research. ECIS.
[5]   Lampinen, A., V. Lehtinen, et al. (2011). We're in It Together: Interpersonal Management of Disclosure in Social Network Services. CHI'11 Proceedings of the annual conference on Human factors in computing systems, Vancouver, BC.
[6]   McGrath, J., J. Martin, et al. (1982). Judgment calls in research. Beverly Hills, Sage Publications.
[7]   Moore, G. C. a. B., I. (1991). ., Vol. 2 Issue 3, p192-223. (1991). "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation." Information Systems Research 2(3): 192-223.
[8]   Sawyer, S. and A. Tapia (2007). "From Findings to Theories: Institutionalizing Social Informatics." The Information Society 23: 263-275.
[9]   Straub, D., Boudreau, M. & Gefen, D. (2004). "Validation Guidelines for IS Positivist
[10]   Research." Communications of AIS 2004(13): 380-427.
[11]   Wisniewski, P., H. R. Lipford, et al. (2011). A New Social Order: Mechanisms for Social Network Site Boundary Regulation. Americas Conference on Information Systems, Detroit, MI.
[12]   Wisniewski, P. (2012). Understanding and designing for interactional privacy needs within social networking sites. Ph.D. Dissertation. University of North Carolina at Charlotte.

Boundary Type	Definition	Desired Privacy Level Measures *(7-point Likert Scale 1-Strongly Disagree, 7 – Strongly Agree)*
Relationship Connection	Regulating whom to let into one's social network	• I only want to accept intimate friends and family members as Facebook friends. • I do not want to have Facebook friends who are no longer real friends. • I only want people in my Facebook social network who I associate with on a regular basis in real life.
Relationship Context	Regulating appropriate interpersonal interactions given the type of relationship	• I want my one-on-one interactions on Facebook to be appropriate and unique based on my relationship with that specific person. • I want my interactions on Facebook to be different between me and a close friend than they would be with an acquaintance. • 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.
Network Discovery	Regulating access others have to one's network connections	• I do not want others to have access to my friends through my Facebook friend list. • I want to hide my friend list so that others cannot browse my Facebook friends. • I want to restrict others in my network from being able to see who I am and am not friends with on Facebook.
Network Intersection	Regulating social interactions between connections or groups of connections	• I want to avoid letting specific groups of friends interact with each other on Facebook. • I want to moderate how my different groups of friends interact with one another on my Facebook page. • I want to keep my different social circles separate from each other on Facebook.
Inward-Facing Territories	Regulating incoming content for personal consumption	• I want to hide News Feed updates from others that I would rather not see. • I want to decide whose updates show up in my News Feed. • I want to pick and choose what kinds of updates show up in my News Feed.
Outward-Facing Territories	Regulating semi-public content available through interactional spaces	• I want to remove any content I do not want from my Timeline/Wall. • I want to manage everything that shows up on my Timeline/Wall for others to see. • I want to approve all content before it is posted to my Facebook Timeline/Wall.
Self-Disclosure	Regulating what personal information one discloses within one's network	• I do not want to post very intimate things about myself on Facebook. • I want to be able to choose what to share and what to hold back on Facebook. • I want to share only minimal information about myself on Facebook.
Confidant-Disclosure	Regulating how co-owned personal information is disclosed within one's network	• I want my Facebook friends to keep personal information they know about me between us. • I do not want my friends to tag me in photos or posts without my permission. • I want to limit what personal information my friends share about me on Facebook.
Interactional Disabling	Regulating potential interaction through turning on/off interface features	• 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. • I want to disable the ability for my friends to contact me on Facebook when I want to be left alone. • I want to limit the different ways my friends can communicate with me via Facebook.
Interactional Blocking	Regulating overall access of oneself to specific individuals outside of one's network	• I want to prevent some people on Facebook from having any access to me what-so-ever. • I want to block certain people from finding me or knowing what I am up to on Facebook. • When I do not want to interact with someone anymore, I want to be able to sever all contact with them on Facebook.

Table 1: Boundary Type Definitions and Desired Privacy Level Measures