Using Contextual Integrity to Examine Interpersonal Information Boundary on Social Network Sites

Pan Shi
The Pennsylvania State University
University Park, PA 16802
pzs125@ist.psu.edu

Heng Xu
The Pennsylvania State University
University Park, PA 16802
hxu@ist.psu.edu

Yunan Chen
University of California,
Irvine, CA 92697
yunanc@ics.uci.edu

ABSTRACT
Although privacy problems in Social Network Sites (SNS) have become more salient than ever in recent years, interpersonal privacy issues remain relatively understudied. This study aims to generate insights in understanding users' interpersonal privacy concerns by expounding interpersonal information boundaries in SNS. Through a case analysis of Friendship Pages on Facebook, this paper identifies users' interpersonal privacy concerns that are rooted from informational norms outlined in the theory of contextual integrity, as well as the tensions that occur within and cross these informational norms. This paper concludes with a discussion of design implications and future research.

Keywords
Interpersonal privacy issues; Social network sites (SNS); Privacy boundary; Facebook; Friendship Pages.

ACM Classification Keywords
K.4.1 [Public Policy Issues]: Privacy; H.1.2 [User/Machine Systems]: Human factors.

INTRODUCTION
Social Network Sites (SNS) are platforms that provide users with various features to facilitate social connectivity, active content sharing, and relationship development. Over 800 million users are currently active on Facebook and are constantly generating contents that may not only disclose their own information but also reveal the identities of their friends (e.g., tagging a friend in a status update or photo or place checked-in). Such highly interactive nature of interpersonal communication and data exchange impels us to think about privacy as a communal matter. This is because a user's identity can be easily exposed by contents generated or tagged by his or her friends, and vice versa. Therefore, users' personal information could be easily leaked through their friends' information sharing and cross-referencing actions on SNS [10]. The need for interpersonal privacy management arises due to the inability to monitor friends (i.e., co-owners of shared information) and their behaviors on SNS.

A growing body of privacy research in HCI has studied the *behavioral* and *technological* mechanisms for users to enact interpersonal privacy practices for co-managing shared contents [e.g., 3, 7, 14]. For example, Lampinen et al. [7] identify *behavioral* means to collectively manage users' shared information, *e.g.*, negotiating "rules of thumb" or asking for approval before disclosing content from those involved. In terms of *technological* mechanisms, privacy researchers have proposed technical tools associated with interpersonal privacy management [e.g., 6, 13].

Although research has touched interpersonal privacy issues in terms of *how* users react and *what* their privacy practices (via behavioral and technological mechanisms) could be, Barkhuus [2] notes that few studies in HCI have explored *why* users reacted the way they behaved. According to Barkhuus [2], research that addresses *why* is increasingly important because it is rare to see studies that collect in-situ data from implemented real systems. To respond to such compelling call for "contextually-grounded research that explores privacy issues in the wild" [2, p.8], we aim to examine the underlying contextually grounded reasons or triggers for users' interpersonal privacy concerns in SNS. Specifically, we obtained data from users' comments posted on Facebook's official blog[1] to study interpersonal privacy issues mediated through the use of a particular feature – Friendship Pages on Facebook.

CONTEXTUAL INTEGRITY
The theory of *contextual integrity* is particularly useful to understand privacy expectations and the norms of information transmission in a given context [8]. Nissenbaum [8] suggests that information ought to be distributed and protected according to norms governing distinct social contexts. Four key parameters are proposed to conceptualize context-relative information norms [8]: *contexts* are the situations in which the information flows occur; *actors* including senders of information, recipients

CHI 2013, April 27–May 2, 2013, Paris, France.

[1] Facebook Blog serves not only as a public platform for introducing new features and announcing significant events, but also enables users to discuss and give feedbacks towards these announcements. Prior to the data collection, we carefully reviewed and agreed to Facebook's Terms: http://www.facebook.com/apps/site_scraping_tos.php

of information, and information subject (whom the information is about); *attributes* are defined as the types of information in the information flow; *transmission principles* are the constraints to the information flow from one party to another in a given context.

In this paper, we base our argument on the theory of contextual integrity [8] because it ties the notion of privacy to *"norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it*" (p.101). According to Nissenbaum [8], what people really care about when they complain and protest that privacy has been violated is not the act of sharing information itself, but the inappropriate handling of shared information.

RESEARCH CONTEXT AND METHOD

In Oct 2010, Facebook introduced the Friendship Page, which aggregated two friends' social interactions including their wall posts, common tagged photos, comments they share, things they both like, events they attended together, and mutual friend lists (see Figure 1). We chose this feature as a crucible to study users' interpersonal privacy concerns because we believe that it is a representative artifact which can reveal dynamism inherent in users' interpersonal interactions and information sharing.

We conducted a qualitative analysis of user comments posted on Facebook's official blog in response to its release of Friendship Pages [1]. We believe that analyzing user comments posted on Facebook's blog allowed us to not only get data from real users but also explore the contextually grounded reasons explaining users' interpersonal privacy concerns and reactions mediated through their actual use of Friendship Pages. We downloaded a total of 1463 comments users made on the topic of Friendship Pages between Oct 28th, 2010 to Jan 14th, 2011 [1] using an API provided by Facebook. To ensure the reliability of our findings, two researchers independently reviewed these comments and extracted privacy related comments for in-depth coding. For the initial round of data analysis, an open coding approach was adopted to identify new concepts arisen from the data. We then used an iterative coding process of collapsing our first round of codes into conceptually distinct themes.

FINDINGS

Our results describe users' interpersonal privacy concerns that can be aligned with the key parameters outlined in the theory of contextual integrity. Our findings indicate that violations or changes of *contexts*, *actors*, *attributes* and *transmission principles* in context-relative information norms could result in users' interpersonal privacy concerns.

Contexts

According to Nissenbaum [8], the parameter of *contexts* in contextual integrity refers to the circumstances in which information flows are situated. In our dataset, it seemed clear that before the introduction of Friendship Pages, the contextual norms of information flows were in place regarding whom users expected to view their interpersonal information.

Figure 1. Illustration of a Friendship Page on Facebook

This communally understood information boundary was blurred after the introduction of Friendship Pages. For example, users indicated their concerns on potential misperceptions of information flows: "*…the extraction and condensation [of information] can cast the comments and posts in a different light from what I intended*." Further, some users worried about potential negative consequences of using this feature and thus complained: "*Thank you facebook ... for the dawning of a new era where a new boyfriend and girlfriend will haunt the 'relationships' of their exes and their new partner's exes*."

These user comments illustrate Nissenbaum's sense that appropriating information from one situation and introducing it in another can be perceived as a privacy violation by users. Such violation of social appropriateness is rooted from the problem which Boyle and Greenberg [4] called *decontexualization* of interpersonal interactions. In the case of Friendship Pages, when examining a short segment of a conversation between two friends, viewers often have to invent contextual information for appropriate interpretation. The inability to obtain the contexts in which conversations and interactions took place could lead to misinterpretation or even wilful distortion of the relationship information displayed on Friendship Pages, which may raise a user's concern about one's own image and privacy pertaining to interactions with others.

Transmission Principles

According to Nissenbaum [8], the violation of transmission principles often happens when new practices entail a change in the process of information transmission, or when shared information travels beyond the desired boundary. In our case of Friendship Pages, users pointed out that this new feature interrupted their expected flow of personal information: "*Suddenly all of my interaction with a specific person is subject to scrutiny by uninvited guests, all on one convenient page*." Although most users were aware of the fact that the visibility of information shown on Friendship Pages would be determined by their own privacy settings, they still expressed their worries about the information aggregation practice employed by Friendship Pages: "*I understand that all of this is visible anyway, but putting it all in one place is too much, especially since you can view two other people, and not just your own relationships...*"

Interestingly, although the Friendship Page did not reveal any new information, its new activity of chronicling the history of social interactions between two friends widely triggered users' privacy concerns. This is because the new practice of combining information could entail changes in the information flow. As Solove notes: "a difference in quantity becomes a difference in quality—it enhances the risk of the harms of disclosure" [12, p.537]. Aggregating interpersonal information on a single and accessible page could result in synergies that can potentially reveal more details about a person and his or her social ties in new and unexpected ways.

Actors and Attributes

Among all parameters outlined in the theory of contextual integrity, *actors*' roles are among those most influential factors that can directly affect people's perceptions over whether privacy has been violated or properly respected [8]. In the case of launching Friendship Page, making friendship information visible to those who were not involved in that interaction raised users' concerns on unwanted recipients of Friendship Page (i.e., inappropriate actors), which may violate users' privacy expectations. For example, one user commented: "*If it was just a relationship between ME AND MY FRIEND I would be totally stoked. I do not like that I can see relationships between other friends. Nor do I like that they can see relationships between me and other friends all in one place like that. Please fix this.*"

According to Nissenbaum [8], the parameter of *attributes* in contextual integrity circumscribes how different types of information should be revealed or shared in a particular context. It has been found in prior research that individuals hold different sensitivity levels for different types of information [11]. Our results showed that users' comfort levels for having different types of information to be displayed on their Friendship Pages were very different. For example, some users expressed their specific concerns on displaying common events and photos: "*How can I disable this [feature] so people are NOT able to research which events I attended together with another friend or which photos we're jointly tagged in?*"

In addition, our findings suggest that failing to maintain the *temporal boundary* of interpersonal privacy could lead to the breach of context-relative information norms. According to Palen and Dourish [9], temporal boundaries are associated with possible tensions between *actions* on revealed information and *interpretations* of revealed information along the timeline. In the case of Friendship Page, threats to temporal boundaries are due to the persistence of data to which the access can be made in the future. For example, one user complained: "*There is no way of deleting two year old posts on ex's wall. I do not like being reminded of this sh***.*" Thus, future accessibility to disclosed information creates tension in boundary management of interpersonal privacy by prompting concerns on undesired use and interpretation after the initial disclosure.

DISCUSSION AND CONCLUSION

The case of Friendship Page indicates that violations or changes of *contexts*, *actors, attributes* and *transmission principles* in context-relative information norms could result in users' interpersonal privacy concerns. Besides voicing their explicit concerns on privacy, users directly expressed their emotional reactions by describing the feature as: *creepy*, *scary*, *disgusting*, or *invasive*. Some rational users asked for more privacy enhancing features such as an opt-out option or a turn-off button.

Nevertheless, without having control over their Friendship Pages, many users expressed their intentions to leave Facebook, deactivate accounts, delete profiles, and use less frequently. For example, one user complained: *"…i have begun deleting my photos online, and have untagged myself and all of my friends."*

This work demonstrates the theoretical contribution of the contextual integrity of privacy to the understanding of tensions or conflicts that a user faces when creating contents that may connect with others' identities. The question of *how* this understanding can be turned into powerful but flexible designs of privacy enhancing features is still a challenge. We argue that it is crucial to align the design of privacy enhancing features with users' privacy needs and information access in *context*. Towards this end, future research should consider the approach of *Privacy by ReDesign* [5]. This approach suggests that it is not always possible to design appropriate privacy enhancing features from the outset; instead, the design should be based on an understanding of the actual system-in-use embedded in a user's daily behaviors.

In conclusion, this qualitative study of users' comments on the launch of Friendship Page on Facebook provides preliminary insights in understanding users' interpersonal privacy concerns. Our work sheds light on future research to investigate the problem of interpersonal privacy that lies beneath social and technical specifications of interpersonal information disclosure and privacy management. We are continuing this research from two perspectives: *measurement* and *design*. First, privacy measurement has focused more on emphasizing informational privacy concerns at the individual level [11] and is less effective at capturing interpersonal and interactional privacy concerns. We are in the process of extending and validating the components of interpersonal and interactional privacy concerns through a large-scale survey. Second, this work has straightforward and practical significance for re-designing existing privacy enhancing features or privacy settings on Facebook. The interpersonal and interactional dynamics we identified in this work should be embedded in context-relative information norms, as they reveal the ways in which existing privacy features could be designed to align with users' understandings and behaviors in *context*.

ACKNOWLEDGMENTS

The authors are very grateful to the AC and anonymous reviewers for their constructive comments on an earlier version of this manuscript. The authors gratefully acknowledge the financial support of the U.S. National Science Foundation under grant CNS-0953749. Any opinions, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

1. Telling the Story of Friendships. *Facebook Blog* (2010), online available at: http://blog.facebook.com/blog.php?post=443390892130
2. Barkhuus, L. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. *Proc. CHI 2012*, ACM (2012), 367-376.
3. Besmer, A. and Lipford, H. Moving Beyond Untagging: Photo Privacy in a Tagged World. *Proc. CHI 2010*, ACM (2010), 1563-1572.
4. Boyle, M. and Greenberg, S. The language of privacy: learning from video media space analysis and design. *ACM Transactions on Computer-Human Interaction*, *12*, 2 (2005), 328-370.
5. Cavoukian, A. and Prosch, M. *Privacy by ReDesign: Building a Better Legacy*. 2011.
6. Kolter, J., Kernchen, T. and Pernul, G. Collaborative Privacy Management. *Computers & Security*, *29*, 5 (2010), 580-591.
7. Lampinen, A., Lehtinen, V., Lehmuskallio, A. and Tamminen, S. We're in it Together: Interpersonal Management of Disclosure in Social Network Services. *Proc. CHI 2011*, ACM (2011), 3217-3226.
8. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford Law Books, 2010.
9. Palen, L. and Dourish, P. Unpacking "privacy" for a networked world. *Proc. CHI 2003*, ACM Press (2003), 129-136.
10. Pesce, J. P., Casas, D. L., Rauber, G. and Almeida, V. Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook. *Workshop on Privacy and Security in Online Social Media*, ACM (2012), Article 4.
11. Smith, H. J., Dinev, T. and Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*, 4 (2011), 989-1015.
12. Solove, D., J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*, 3 (2006), 477-560.
13. Squicciarini, C. A., Xu, H. and Zhang, X. CoPE: Enabling Collaborative Privacy Management in Online Social Networks. *Journal of the American Society for Information Science and Technology 62*, 3 (2011), 521-534.
14. Wisniewski, P., Lipford, H. and Wilson, D. Fighting for my space: Coping mechanisms for SNS boundary regulation. *Proc. CHI 2012*, ACM (2012), 609-618.