Spring 6-20-2012

Beyond the Individual Privacy Paradigm: Implications for Interpersonal Interactions on Facebook

Pan Shi
The Pennsylvania State University, University Park, United States, pzs125@ist.psu.edu

Heng Xu
The Pennsylvania State University, University Park, United States, hxu@ist.psu.edu

Cheng Zhang
Fudan University, Shanghai, China, zhangche@fudan.edu.cn

25th Bled eConference
eDependability:
Reliable and Trustworthy eStructures, eProcesses, eOperations and eServices for the Future
June 17, 2012 – June 20, 2012; Bled, Slovenia

Beyond the Individual Privacy Paradigm: *Implications for Interpersonal Interactions on Facebook*

Pan Shi
The Pennsylvania State University, University Park, United States
pzs125@ist.psu.edu

Heng Xu
The Pennsylvania State University, University Park, United States
hxu@ist.psu.edu

Cheng Zhang
Fudan University, Shanghai, China
zhangche@fudan.edu.cn

Abstract
Privacy is widely viewed as an interpersonal boundary regulation process in the context of online social networks (OSNs). Mediated by technologies provided by the OSNs, users manage both identity information and social relationships on OSNs. While previous studies mainly focus on users' information sharing and disclosure behaviors from an individual perspective, this work looks into the social nuances of users' interactional privacy concerns within their social circles from an interpersonal perspective. Through a case analysis of launching "Friendship Pages" by Facebook, we aim to examine the trigger conditions under which users perceive the launch of such feature to aggregate interpersonal interactions as privacy problems. This work calls for more research in conceptualizing and measuring users' interpersonal privacy concerns in the context of OSNs. We conclude this work with a discussion on research challenges in support of mitigating users' interpersonal concerns in OSNs.

Keywords: Interactional privacy concerns, online social networks (OSNs), privacy boundary regulation, Facebook, Friendship Pages.

1 Introduction

The booming popularity of Online Social Networks (OSNs) has received significant attention during recent years. With more than 800 million active users globally (Facebook Statistics, 2012), *Facebook* – the largest OSNs in the world – provides its users with a variety of technologies to support and encourage continuous connectivity and active information sharing. Users' social interactions in OSNs generate a large

volume of personal data and the intensive propagation of such data introduces a variety of privacy risks. Prior research has identified a wide range of privacy threats associated with the use of OSNs, such as damaged reputation and image, unwanted stalking, and unauthorized use of personal data by third-party applications (boyd & Ellison, 2008; Egelman et al., 2011; Gross & Acquisti, 2005).

An additional aspect that denotes the complexity of examining privacy issues in OSNs is added by the dynamic *interpersonal* interactions with rich data exchange. Millions of Facebook users are "befriending" each other through various social ties on a daily basis (Facebook Statistics, 2011). Users are actively creating contents that may not only reveal their own identities but also connect with their social ties (e.g., tagging a friend in a shared photo, or linking to a friend's profile in a wall post). Such interactive nature of activities raise a new set of privacy challenges, because a person's private information can be easily revealed by contents created by others. In other words, inability to monitor others' information disclosure about oneself could intensify users' privacy concerns in current settings of OSNs (Kelly, 2008).

Research on information privacy has mainly focused at the individual level of analysis (see Smith, Dinev, & Xu, 2011), for two reasons: an emphasis on the conventional information exchange between a single user and a website that requests data (e.g., Xu et al, 2011), and the focus on identifying individual privacy responses to data requests (e.g., Son and Kim 2008). Other studies that have examined privacy have been concerned with organizational (e.g., Culnan and Bies 2003) and societal dynamics (e.g., Dinev et al. 2008). Largely missing from current understandings of privacy are studies focusing on the *interpersonal* level of privacy issues related to social interactions and content sharing among social ties (e.g., friends, and friends of friends on Facebook). This work will be targeted to this under-researched level of analysis by highlighting the tension or conflict that a user faces when creating contents that may connect with others' identities.

The objective of this work is to extend the notion of privacy from an individual user's perspective to an interpersonal perspective. Through a case analysis of launching "Friendship Pages" on Facebook, we aim to examine the trigger conditions under which users perceive the launch of such feature to aggregate interpersonal interactions as privacy problems. In what follows, we first provide an overview of existing privacy research. Next we present the case of "Friendship Pages" on Facebook, describing the background of this case, and discussing the emerging themes. Then we unveil the interpersonal privacy apprehensions of users in OSNs by examining the social nuances of users' interactional privacy concerns within their social circles. This paper concludes with a discussion of research and design implications, and directions for future research.

2 Literature Review

At the individual level, much of the contemporary privacy research focuses on information privacy as a multidimensional construct (e.g., Angst and Agarwal, 2009; Malhotra et al., 2004; Smith et al., 1996; Son and Kim, 2008). As Xu (2009) pointed out, privacy research at the individual level has often been understood through three theoretical lenses. The first theoretical lens, referred as the *information exchange* lens, conceptualizes privacy as a "privacy calculus" which represents the cost-benefit analysis that individuals are willing to conduct when they exchange their personal

information for economic or social gains (Culnan and Armstrong, 1999; Culnan and Bies, 2003; Xu et al., 2010). The second theoretical lens, referred as the *social contract* lens, highlights the importance of trust between organizations and individuals over information disclosure (Hoffman et al., 1999; Milne and Gordon, 1993; Xu et al., 2005). For instance, many studies on trust have proposed to consider the organizational privacy policies and privacy seals (e.g., TRUSTe seal) as the institutional structural assurances built into a Web site which may influence individuals' trusting beliefs and privacy perceptions toward the Web site (e.g., Gefen et al., 2003; McKnight and Chervany, 2002). The third theoretical lens, referred as the *information control* lens, emphasizes the role of perceived control in explaining individuals' privacy perceptions or attitudes. Prior research has indicated that individuals would have lower levels of privacy concerns when they believe that they are able to control the disclosure and subsequent use of their personal information (Culnan, 1993; Stone and Stone, 1990; Xu, 2007).

At the organizational level, current privacy literature has provided insights about factors explaining organizational responses and behaviors (Greenaway and Chan, 2005). As Parks et al. (2011a; 2011b) pointed out, only limited research examined the privacy measures and practices undertaken by organizations. In their analysis of privacy literature, Parks et al. (2011a; 2011b) highlighted three theoretical lenses to understand organizational privacy practices. The first theoretical lens, referred as the *institutional theory* lens, posits that organizations respond to institutional pressures imposed by the government, industry sector, or general public (Oliver, 1991), by adopting changes to achieve legitimacy and conformity (DiMaggio and Powell, 1983; Meyer and Rowan, 1977). The second theoretical lens, referred as the *Resource Based View* (RBV), has been used as a theoretical explanation for organizations seeking competitive advantage through their privacy programs (Greenaway and Chan, 2005). The third theoretical lens, referred as the *ethical* lens, has been discussed about the conditions under which information sharing might be in the interest of customers and customer services, and when information sharing operates to classify customers, create unfair competitive advantage, or result in price discrimination (Culnan and Williams 2009).

In summary, the current privacy literature mainly focuses on *individual* and *organizational* actions, which only considers privacy behavioral responses either at the individual level or the organizational level, and fails to recognize the need for privacy actions at the small group level (e.g., interpersonal level in the context of OSNs). Based on an interdisciplinary review of 320 privacy articles and 128 books and book sections, Smith et al. (2011) noted that there have been very few studies that considered privacy at the small group level and concluded that "the paucity of studies at this level strikes us as a significant weakness in the privacy literature stream" (p.1007).

To provide a richer conceptual description of privacy management, this research will be targeted to this under-researched level of analysis in the specific context of interpersonal communications in OSNs. We argue that interpersonal privacy management differs from personal privacy management because of its change of agency (from the self to a social group), its inclusion of interactional privacy decision making, and its collective domain where users and their social ties share responsibilities for keeping their shared data safe and private.

3 The Case of "Friendship Pages" on Facebook

We chose the event of launching "Friendship Pages" on Facebook as a crucible to examine users' interpersonal privacy concerns for two reasons. First, it triggered users' privacy concerns, discontent, anxiety, and mass media's questioning of privacy breach as soon as it was introduced (Facebook Blog, 2010). Second, rather than being a single feature that was only related with one genre of interaction, Friendship Pages aggregated information from a comprehensive set of interactions between two users. Thus, the case of Friendship Pages can provide us with a representative artifact to examine the dynamism inherent in users' interpersonal interactions and data sharing.

3.1 Friendship Pages on Facebook

In Oct 2010, Facebook introduced the Friendship Pages, which chronicled the history of social interactions between two friends including wall conversations, photos with both tagged in, comments they share, events they attended together, things they both like, and mutual friend lists (see Figure 1).

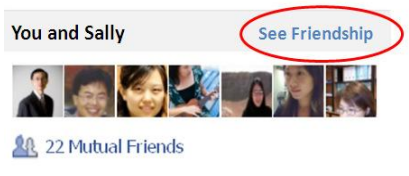
Figure 1: Illustration of a Friendship Page on Facebook (Adapted from Pixel Coaching, 2010)

3.2 Access Friendship Pages on Facebook

With the availability of Friendship Pages on Facebook, users are able to view the friendship pages:

1) between the user and one friend of this user (**U-UF**),
2) between two of the user's friends (**UF-UF**), and
3) between one friend and this friend's friend (**UF-UFF**).

In the first scenario of **U-UF**, a user can click "See Friendship" (see Figure 2) located in the upper-right corner of his or her friend's Wall to access the friendship page between the user and one friend of this user.



[Note. This feature is located in the upper-right corner of the friend's (e.g., Sally's) Wall]

Figure 2: See Friendship U-UF

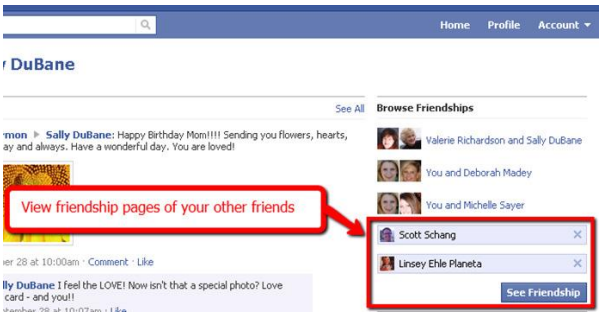


Figure 3: Search to See Friendship (UF-UF by Search)

In the second scenario of **UF-UF**, there are two available approaches on Facebook to access the friendship page between two friends of the user:

a) Search to See Friendship: Users can view the friendship page between any two friends whom they are connected to by inputting their names in the highlighted box (see Figure 3). When they hit "See Friendship", they are directed to the friendship page between these two friends. The user must be friends with both people to see the friendship page between them.

b) Browse to See Friendship: As shown in Figure 4 (1), users can also access friendship pages directly from a friend's wall. Certain activity items (e.g., a wall post from friends) will display a "See Friendship" link next to them. In this case, users can just click the hyperlink of "See Friendship" and they will be able to see the friendship page between two of their friends.

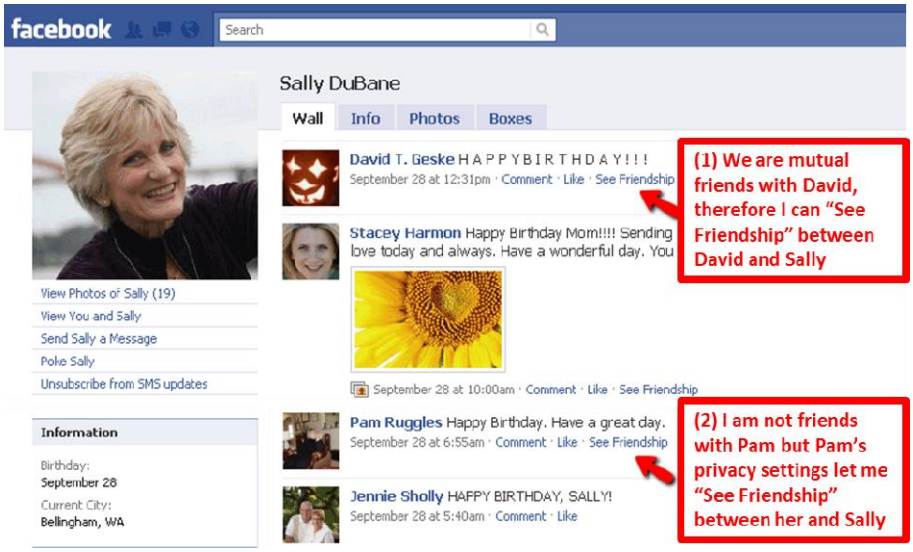


Figure 4: See Friendship UF-UF by Browsing (1), and See Frienship UF-UFF (2) (Adapted from Pixel Coaching, 2010)

In the third scenario of UF-UFF shown in Figure 4 (2), the user was not a friend of Pam Ruggles but Pam's privacy setting on "Things I Share" was set as "friends of friends". In this case, this user was considered Pam's friend of friend and thus had the option to "See Friendship" between Pam and her friend.

3.3 Data Collection

We conducted a content analysis of user comments posted on Facebook blog in response to the release of Friendship Pages. Such qualitative approach is considered to be well suited for the exploratory research such as ours (Bulgurcu et al., 2010; Strauss & Corbin, 1990). Facebook's official blog is not only a public platform for Facebook to introduce new features and announce significant events, but also a public platform for users to discuss and give feedbacks towards these topics. We believe that analysing user comments posted on the Facebook's blog allowed us to not only obtain a large dataset but also identify real users' privacy concerns.

All the announcements of new features made by Facebook as well as corresponding users' comments are publically available[1]. We downloaded a total of 1463 comments users made on the topic of Friendship Pages between Oct 28th, 2010 to Jan 14th, 2011 from Facebook's blog[2]. We carefully reviewed these comments and extracted 308 comments that were related to users' privacy attitudes or concerns. Two independent coders first developed a coding guideline with multiple categories of privacy related concepts. This was followed by their independent categorizations of the 308 privacy related comments. For the initial round of data coding, we embraced an open coding approach in order to further identify new concepts arisen from the data. Upon completing the first round of coding, we found that there was the emergence of certain categories, which involved an iterative process of collapsing our first round of codes into theoretically distinct themes (i.e., emergence of interpersonal privacy management, users' concerns over violations of temporality boundary, and users' concerns over violations of collective territory boundary). These three themes are presented in the next section.

4 Preliminary Findings

4.1 Emergence of Interpersonal Privacy Management

Users pointed out that the Friendship Pages interrupted the natural flow of social interactions by aggregating interpersonal interaction activities on a single and easily accessible page. Although most users were aware of the fact that the visibility of information displayed on Friendship Pages would be determined by their privacy settings, they still expressed their discomfort as well as worries about the negative consequences caused by the aggregated information displayed on Friendship Pages. For example, one user posted his or her comment on Facebook's blog:

[1] Facebook's official blog is publicly available online at: http://blog.facebook.com

[2] See Facebook's official blog on "Telling the Story of Friendships," available online at: http://blog.facebook.com/blog.php?post=443390892130

"*… That competitive friend / jealous partner who will compare how many times you sent a message to your other friend or how many photos you took together or how many events you attended…*"

Another user complained:

"*… 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...*"

Besides raging users who wanted to instantly shut down this feature, rational users appealed for more privacy control features such as an opt-out option and a turn-off button. However, according to the designers of Friendship Pages, control of Friendship Pages was embedded within the global privacy setting on Facebook. It seems that users did not understand how the global privacy setting could be adjusted to control the access of their Friendship Pages. For example, one user said:

"*Wayne Kao's* [Facebook Designer's] *post about "Friendship pages" is ambiguous: Mr. Kao says "You'll be able to see a friendship page if you are friends with one of the people and have permission to view both people's profiles," but the privacy settings are more fine-grained than that. I let "Everyone" see my photo, my name, and my city--- does that counts as "permission to view" my "profile"? If so, this new feature is a terrible, terrible privacy violation, because it displays things that I specifically marked as private*."

Without having usable control over their interpersonal information, many angry users expressed their intentions to leave Facebook, deactivate accounts, delete profiles, and less usage. For example, one user complained:

"*[This feature] is perfect for stalking people [and] makes me very, very uncomfortable. I might deactivate today in fact.*"

Clearly, the information boundary between an individual user and his/her social ties on Facebook becomes turbulent when Friendship Pages are introduced. The process of privacy boundary management could be confounded by the technology as a double-edged sword (Palen and Dourish 2003): To users, on the one hand, they may identify great values in supporting multidimensional interpersonal information aggregation through Friendship Pages; on the other hand, the deficiency in fulfilling interpersonal boundary management goals may turn them away.

The need for interpersonal boundary management arises due to the uncertainty about others' behaviors on the network. In the case of Friendship Pages, concerned private information will not only reside a single user's own domain, but also be co-owned and co-managed by multiple shareholders. Thus, the task of interpersonal privacy boundary management has to involve other shareholders in a collective domain. A key concern when discussing interpersonal privacy management is its definition. Although there is not a universally accepted characterization of interpersonal privacy management, we conceptualize it as a process of maintaining social boundaries among many social relationships or circles that often overlap, and becomes a group issue when the actions of one individual affect the privacy of another. In this work, we argue that interpersonal privacy management differs from personal privacy management because of its change of agency (from the self to a social group), its inclusion of interactional privacy decision

making, and its collective domain where the user and her social ties share responsibilities for keeping their shared data private.

4.2 Users' Concerns over Violations of Temporality Boundary

The Friendship Pages chronicle the interaction history between two friends on Facebook. Displaying formerly involved activities with friends made users feel unnecessary and annoying:

"[B]ut knowing what events some friends attended or took pictures at up to 5 years ago just really isn't necessary to add on to that [Facebook Friendship Pages]."

A user's shared information on Facebook is exposed to the user's friends once the relationship is established – not only contemporary information, but also historical information disclosed before the start of their relationship. Users worried that simply displaying segments of interactions would diminish the original contexts for the interactions and thus change the desired meanings:

"Facebook communications with any given friend occur within a larger context of unrelated posts made by our friend and others, and they take place over time."

"The Friendship feature plucks them from that context and temporal flow and creates a new, unnatural context that change their apparent meaning or can reveal meanings that would not otherwise have been apparent to anyone but the friend involved."

It seems reasonable to argue that aggregating historical interpersonal interactions failed to maintain the *temporality* boundary of interpersonal privacy. In the privacy literature, Palen & Dourish (2003) used the notion of temporality to describe privacy boundaries related to time: temporal boundaries are associated with possible tensions between *actions* on disclosed information and *interpretations* of disclosed information along the timeline. In our case of Friendship Pages, threats to temporal boundaries are due to persistence of data such that audience can exist in *future*. Therefore, *future* accessibility to *now* or *past* data promotes potential tension in boundary management of interactional privacy by prompting privacy concerns on undesired use and interpretation.

This is especially the case in the context of OSNs. Being a friend of a user's social ties usually grants the friend with permissions to view a fairly large amount of the user's shared information, regardless the time when the disclosed information was created. Although current OSNs such as Facebook provides users with fine-grained privacy settings to control the visibility of specific types of disclosed information, in reality this may not help to address this tension. When users manage their privacy on OSNs, they usually take an *all-or-nothing* approach (Strater & Lipford, 2008), that is, they set the visibility of their online profiles to either 'friends only' or 'public'. According to a survey of 494 undergraduate students (Stutzman and Kramer-Duffield, 2010), 'friends only' is a well-adopted privacy setting among Facebook users. These empirical evidences indicate that majority of a user's information on OSNs is exposed to his or her friends once the relationship is established – not only contemporary information, but also historical information disclosed before the start of their relationship.

4.3 Users' Concerns over Violations of Collective Territory Boundary

Who should be appropriate to view Friendship Pages between two friends? Users indicated their preferences in defining such collective territory boundaries: only the two parties involved with the conversation should be eligible to view their interactions.

"It would be fine if you could see your own interactions with a friend, but for everyone on [our mutual] friends list to see this information as well? No."

Another user said: *"This feature would be great if it were only meant to be used to see ones' OWN relationships, not in addition to seeing the relationships of any of your other friends."*

Some users even argued that the situation of viewing others' friendship information and the situation of their own friendship information being viewed by others were both disturbing and annoying. These concerns implied users' strong desires for defining boundaries of the online territory, more specifically, collective territory boundaries to specify the scope of information disclosure. According to Altman (1977), claiming of territory (e.g. fences, locks, and doors) is one critical behavioral mechanism for individuals to optimize physical privacy in a given situation. Applying the original definition of physical territory to the context of OSNs, the notion of online territory needs to be extended to involve multiple shareholders who are the co-owner or co-author as well as the audience of the shared data. For example, a wall post on Facebook is always associated with the author of this post as well as commentators' comments. The visibility of commentators' information depends heavily on the visibility of the post set by the original author. In other words, commentators' information can be potentially exposed to the author's network and the original wall post can also be exposed to all commentators' networks.

In this work, we argue that the original notion of *territory* should be extended to a level of *collective* analysis, which reflects social interactions within various social circles. In current settings of OSNs, the boundary of *collective territory* is implicit yet has caused users' concerns. For example, some users complained that their commenting activities for one friend's post were sometimes broadcasted to other friends without their awareness. To these users, they would like their posts and comments to be only visible to a specified scope of audience. The violation of *collective territory* boundaries can happen when the shared information travels beyond the desired boundaries and when the information is viewed by unwanted audience.

5 Discussion and Conclusion

5.1 Research Implications

Privacy is a highly situated concept which varies upon different contexts. Compared with the offline environment which provides constraints to keep interactions to be situated within temporal boundary as well as spatial territory boundary, technology-mediated settings may fail in offering users with such boundary management mechanisms in OSNs. The connected nature of OSNs may alter constraints for interpersonal interactions, leading social interactions to be decontextualized (Boyle & Greenberg, 2005).

The case of Friendship Pages indicates that violations of *temporality* and *collective territory* boundaries could cause decontexualization of interpersonal interactions, which may lead to users' interpersonal privacy concerns. Findings of this work are summarized in a conceptual framework in Figure 5. Consistent with Palen and Dourish's (2003) classification of interpersonal privacy boundaries, our conceptual framework describes two dimensions of users' interpersonal privacy concerns rooted from the *collective territory* and *temporality* boundaries, as well as the tensions that occur within these two boundaries. *Collective territory* boundary settings often reflect users' conceptualizations of their virtual space in OSNs – limited access reflects tight privacy settings while public access reflects loose or open privacy settings. As Palen and Dourish (2003) pointed out, "determinations [of territory boundaries] are made about what information might be disclosed under what circumstances, albeit with varying degrees of direct control (p.131)." Features of territory are managed in situations where privacy and publicity are in tension (Palen and Dourish 2003). As shown in Figure 5, the other dimension is the *temporality* boundary, which is caused by the persistence of disclosed information such that audience can exist in *future*. According to Palen and Dourish (2003, p.131), "temporality describes the boundaries associated with time, that is, where past, present and future interpretations of and actions upon disclosed information are in tension." In other words, *future* accessibility to *now* or *past* data promotes potential tension in interpersonal boundary management by prompting privacy concerns on undesired use and interpretation.

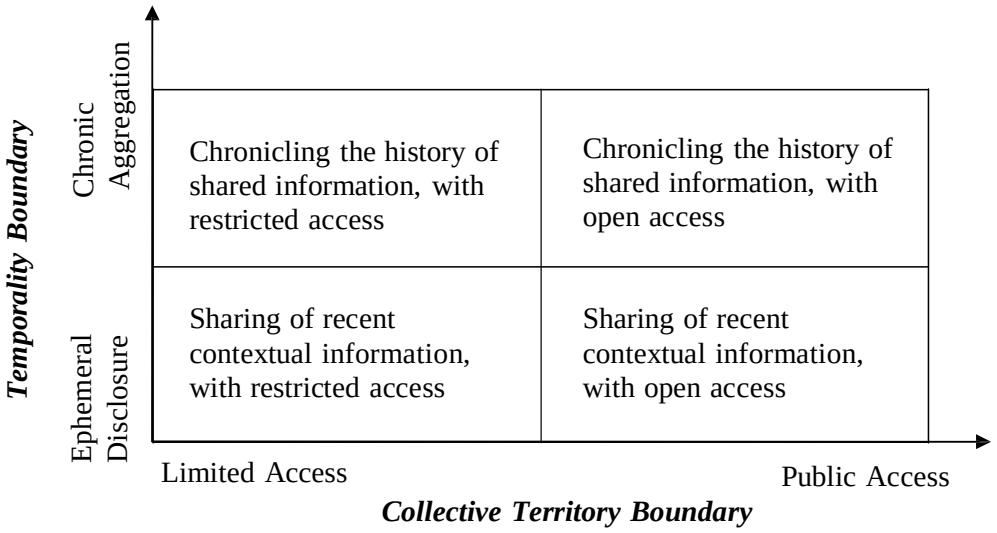


Figure 5. Conceptual Framework

Our conceptual framework depicted in Figure 5 can be a starting point for future work to understand users' interpersonal privacy practices that lie beneath social and technical specifications of interpersonal information disclosure and privacy concerns. Exploration of interpersonal privacy management is particularly important, as these are often confused in technical designs, in service providers' data collection practices, and in users' privacy expectations.

Researchers have only recently begun to examine the *behavioral* and *technological* means for users to enact interpersonal privacy practices for co-managing their shared information and contents on OSNs (e.g., Besmer et al., 2009; Lampinen et al., 2011). These interpersonal privacy practices usually comprise strategies or tools that allow individuals and their social groups collectively act as control agents to exercise collective control over their shared information. Lampinen et al. (2011) identifies *behavioral* strategies for users to collectively manage their shared information, e.g., negotiating and agreeing on "rules of thumb" concerning sharing with other users, asking for approval before disclosing content from those involved, and asking another person to delete content.

In terms of *technological* strategies, researchers have begun proposing the privacy enhancing technologies associated with interpersonal privacy management. Technical solutions include addressing the conflicting privacy preferences among multiple content owners (Squicciarini, et al. 2009), restricting shared content to a selected group of contacts (Mannan, et al. 2008), proposing a user-centric privacy architecture to support collaborative privacy practices (Kolter, et al. 2010), developing technical means to facilitate interactions among co-owners for co-managing shared content (Squicciarini, et al. 2011), and promoting collaborative privacy awareness through facilitating a group's social collaborations in privacy decision making (Besmer, et al. 2009).

In sum, although research has touched technical issues concerning the theme of interpersonal privacy management among shareholders, their focus is largely on algorithms, rather than designs to support user interpersonal interactions. Our work suggests that effective interpersonal privacy management mechanisms should be able to enable users to maintain both temporality and collective territory boundaries. However, due to the limit of current interpersonal privacy settings in OSNs, users often have to sacrifice either their privacy needs or social needs when managing access control in OSNs (Strater and Lipford 2008). To envision powerful but flexible privacy control features to facilitate interpersonal privacy management remains a key research issue.

5.2 Limitations and Future Work

Our work adds to the growing literature of privacy in the context of OSNs by investigating interpersonal privacy issues. The conceptual investigations lend a support to better define privacy in this domain. Our content analysis of users' reactions in real world provides first-hand insights in identifying and understanding their interpersonal privacy concerns. However, this data set is inadequate to provide us with deep insights regarding users' actual behavioural patterns on Facebook. In future research, we should address this limitation through interview or field studies. In addition, our work is limited with a specific IT artifact (i.e., Friendship Pages) on a single social networking platform (i.e., Facebook.com). Future research should study other social networking platforms that offer similar sets of interpersonal communication features to examine the generalizability of our findings. Third, the user sample in this work is limited to a small sub-sample of Facebook users who had posted their comments on the topic of launching Friendship Pages on Facebook's official blog. In other words, user comments were only collected from those users who were willing to post their comments to express their privacy concerns. Care must be taken in any effort to generalize our findings beyond the boundary of our sample.

Acknowledgement

The authors are very grateful to the three anonymous reviewers for their constructive and helpful comments. Heng Xu gratefully acknowledges the financial support of the U.S. National Science Foundation under grant CNS-0953749. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

References

Altman, I. 1977. "Privacy Regulation: Culturally Universal or Culturally Specific?" *Journal of Social Issues*, (33:3), pp. 66-84.

Angst, C.M., and Agarwal, R. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2) 2009, pp 339-370.

Besmer, A., Lipford, H., Shehab, M., and Cheek, G. "Social Applications: Exploring A More Secure Framework," *Proceedings of the Symposium On Usable Privacy and Security*, Mountain View, CA, 2009.

boyd, D. M. and Ellison, N. B. (2008) Social network sites: Definition, history, and scholarship. *Journal of Computer Mediated Communication*, (13:1), pp.210-230.

Boyle, M. and Greenberg, S. (2005) "The Language of Privacy: Learning from video media space analysis and design," *ACM Transactions on Computer-Human Interaction* (TOCHI), (12:2), pp. 328-370.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. "Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook," *Proceedings of International Conference on Information Systems* (ICIS 2010), St. Louis, MO., paper 230.

Culnan, M.J. "'How Did They Get My Name'? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3) 1993, pp 341-364.

Culnan, M.J., and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), Jan-Feb 1999, pp 104-115.

Culnan, M.J., and Bies, J.R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2) 2003, pp 323-342.

Culnan, M.J., and Williams, C.C. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly* (33:4) 2009, pp 673-687.

DiMaggio, P.J., and Powell, W.W. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *Rationality in Organizational Fields* (48) 1983, pp 147-160.

Dinev, T., Hart, P., and Mullen, M.R. "Internet privacy concerns and beliefs about government surveillance - An empirical investigation," *Journal of Strategic Information Systems* (17:3), 2008, pp 214-233.

Egelman, S., Gaithersburg, M. D., Oates, A., Krishnamurthi, S. and Providence, R. I. (2011) Oops, I Did It Again: Mitigating repeated access control errors on Facebook. *Proceedings of 29th SIGCHI Conference on Human Factors in Computing Systems* (CHI'11), Vancouver, BC, Canada, ACM Press, 2295-2304.

Facebook Statistics. (2011) Retrieved March 10, 2011, from http://facebook.com/press/info.php?statistics

Facebook Statistics. (2012) Retrieved March 13, 2012, from http://facebook.com/press/info.php?statistics

Facebook Blog: Telling the Story of Friendships. (2010) http://blog.facebook.com/blog.php?post=443390892130

Gefen, D., Karahanna, E., and Straub, D.W. "Trust and TAM in online shopping: an integrated model," *MIS Quarterly* (27:1), March 2003, pp 51-90.

Greenaway, K.E., and Chan, Y.E. "Theoretical Explanations for Firms' Information Privacy Behaviors," *Journal of the Association for Information Systems* (6:6) 2005, pp 171-198.

Gross, R. and Acquisti, A. 2005. Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (WPES'05) ACM Press, 71-80.

Hoffman, D.L., Novak, T., and Peralta, M.A. "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society* (15:2) 1999, pp 129-139.

Kelly, S. (2008). "Identity 'at risk' on Facebook" in: BBC News. Retrieved from http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm

Kolter, J., Kernchen, T., and Pernul, G. "Collaborative Privacy Management," *Computers & Security* (29:5) 2010, pp 580-591.

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 2011 ACM Conference on Human Factors in Computing Systems (CHI)*, ACM, Vancouver, Canada, 2011, pp. 3217-3226.

Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), December 2004, pp 336-355.

Mannan, M., and Oorschot, P.C.v. "Privacy-enhanced sharing of personal content on the web," *Proceedings of the Sixteenth International WWW Conference*, 2008, pp. 487-496.

McKnight, D.H., and Chervany, N.L. "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *International Journal of Electronic Commerce* (6:2) 2002, pp 35-59.

Meyer, J.W., and Rowan, B. "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2) 1977, pp 340-363.

Milne, G.R., and Gordon, E.M. "Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework," *Journal of Public Policy and Marketing* (12:2), Fall 1993, pp 206-215.

Oliver, C. "Strategic Responses to Institutional Processes," *Academy of management review* (16:1) 1991, pp 145-179.

Palen, L. and Dourish, P. (2003) Unpacking privacy for a networked world. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'03), Ft. Lauderdale, FL, USA, ACM Press, 129-136.

Parks, R., Chu, C.-H., and Xu, H. "Healthcare Information Privacy Research: Issues, Gaps and What Next," *Proceedings of the 17th Americas Conference on Information Systems* (AMCIS), Detroit, MI, 2011a.

Parks, R., Chu, C.-H., Xu, H., and Adams, L. "Understanding the Drivers and Outcomes of Healthcare Organizational Privacy Responses," *Proceedings of 32nd Annual International Conference on Information Systems* (ICIS), Shanghai, China, 2011b.

Pixel Coaching. (2010) Facebook Friendship Pages Launches, retrieved from http://www.pixelcoaching.com/public/facebook-friendship-pages-launches/

Smith, H.J., Milberg, J.S., and Burke, J.S. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), June 1996, pp 167-196.

Smith, H. J., Dinev, T., and Xu, H. (2011) Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* (35:4), 989-1016.

Son, J.Y., and Kim, S.S. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3) 2008, pp 503-529.

Squicciarini, A., Shehab, M., and Paci, F. "Collective Privacy Management in Social Networks," *Proceedings of the 17th International World Wide Web Conference*, ACM Press, Madrid, Spain, 2009, pp. 461-484.

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, pp 521-534.

Stone, E.F., and Stone, D.L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8:3) 1990, pp 349-411.

Strater, K. and Lipford, H. R. (2008) Strategies and struggles with privacy in an online social networking community. *Proceedings of the 22nd British HCI Group Annual Conference* (BCS-HCI'08), Swinton, UK, British Computer Society, 111-119.

Strauss, A.L, and Corbin, J. 1990. *Basic of Qualitative Research*, Sage publications, NP.

Stutzman, F. and Kramer-Duffield, J. (2010) Friends only: examining a privacy-enhancing behavior in facebook. *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (CHI'10), ACM Press, New York, NY, USA, 1553-1562.

Xu, H. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," *Proceedings of the 28th Annual International Conference on Information Systems* (ICIS 2007), Montréal, Canada, 2007.

Xu, H. "Consumer Responses to the Introduction of Privacy Protection Measures: An Exploratory Research Framework," *International Journal of E-Business Research* (5:2) 2009, pp 21-47.

Xu, H., Teo, H.H., and Tan, B.C.Y. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," *Proceedings of 26th Annual International Conference on Information Systems* (ICIS 2005), Las Vegas, NV, 2005, pp. 897-910.

Xu, H., Teo, H.H., Tan, B.C.Y., and Agarwal, R. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3) 2010, pp 137-176.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12) 2011, pp. 798-824.