# Profiling Facebook Users' Privacy Behaviors

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

Bart P. Knijnenburg
Department of Informatics
University of California, Irvine
bart.k@uci.edu

Heather Richter Lipford
Department of Software and Information Systems
UNC Charlotte
heather.lipford@uncc.edu

## ABSTRACT

Social Network Sites (SNSs) such as Facebook offer a plethora of privacy controls, but users rarely exploit all of these controls, nor do they do so in a similar manner. In this paper, we analyze distinct *profiles* of users' privacy management strategies on Facebook (including but also going beyond information disclosure behavior). We cluster the self-reported privacy behaviors of 308 Facebook users based on the privacy settings and features available in Facebook's user interface. We extrapolate six distinct privacy profiles, which include: 1) *Privacy Maximizers*, 2) *Selective Sharers*, 3) *Privacy Balancers*, 4) *Self-Censors*, 5) *Time Savers/Consumers*, and 6) *Privacy Minimalists*. Creating such profiles will enable deeper exploration of privacy concerns and behaviors, as well as expose opportunities for personalization of privacy settings, recommendations, and training.

## 1. INTRODUCTION

Privacy is a major concern of Social Network Site (SNS) users [13], even though most SNSs provide users with a variety of mechanisms to control how they interact and share information with one another. Users' efficacy in privacy management is hampered by their bounded rationality [1] and their limited motivation to control their privacy [4, 6]. Thus, understanding and exploiting *all* the mechanisms necessary to manage every aspect of a one's privacy on an SNS such as Facebook is nearly impossible. In this paper, we demonstrate that Facebook users instead use a *subset* of the available mechanisms to manage their privacy. We find that not every user leverages the same subset of privacy mechanisms and uncover distinct *profiles* of behavior that give insight into different users' privacy management strategies.

## 2. BACKGROUND

Our work frames privacy in a broad sense 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 [2]. Managing information disclosures is just one strategy SNS users employ to manage their interpersonal privacy with others. For example, some SNS users leverage friend lists in Facebook or circles in Google+ in order to disclose more personal information but to smaller audiences [7, 20, 23]. Others adopt coping strategies, such as managing multiple Facebook profiles or using pseudonyms to prevent different social circles from over-lapping or engaging with unwanted others [22]. Previously, we conducted a feature-oriented domain analysis across five popular SNS websites, including Facebook to conceptually group the different interface features available for regulating interpersonal privacy [23]. By doing this, we were able to build a theoretical framework to better understand the various types of interpersonal privacy boundaries that SNS users manage [21, 23]. In many cases, we found that the ability to manage various types of interpersonal boundaries was directly dependent on the interface features available within the SNS for doing so. Therefore, for the purposes of this paper, we define ***privacy behaviors*** as the privacy features and/or settings that Facebook users leverage in order to manage interpersonal privacy boundaries. On Facebook, managing one's personal user profile information, the content displayed or posted onto one's Timeline or Wall, the content that filters into one's News Feed from one's friends, or even whom one chooses to friend or unfriend are all examples of interpersonal boundary decisions that SNS users can combine to form a strategy for regulating their interpersonal privacy boundaries.

A variety of research has examined individuals' use of various privacy controls, and their relationships with privacy concerns, demographics, or other behaviors and outcomes. For example, Stutzman et al. [17] examined the factors which contributed to Facebook users' decisions on whether or not to set their Facebook profiles to "Friends Only." Ellison et al. [5] found a positive relationship between Facebook users' use of advanced privacy settings (such as changing privacy settings from the default and limiting content sharing to specific groups within one's network) and perceived social capital, the benefits derived from being an active member of a social network. Other researchers have also explored the use of selective sharing through friend lists or circles [7, 20].

The majority of privacy research has focused on privacy settings as they relate specifically to information disclosure behaviors [10-12, 16, 19]. Yet few studies have examined overarching privacy management strategies of SNS users: How do users employ various *subsets* of the available mechanisms to manage their privacy and how do these strategies vary across users? In this paper, we investigate the *dimensionality* of various privacy behaviors on Facebook and classify users into different *privacy profiles* based on these dimensions. This work moves beyond Knijnenburg et al. [10] and other SNS privacy research by analyzing not just information disclosure behaviors, but a wide range of available privacy management strategies based upon our previous feature analysis. In the next section, we describe our data collection procedures and method of analysis for examining the underlying dimensionality of different privacy behaviors and classifying Facebook users based on varying levels of these dimensions. Then, we present the different dimensions of privacy behavior and describe six unique privacy profiles that emerge from our analysis. Finally, we discuss the potential use of these privacy profiles in further understanding and supporting SNS users' privacy needs.



Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.

# 3. PROCEDURE

## 3.1 Data Collection

Data were collected through a web-based survey using Survey Share. Participants had to be over 18 and have an active Facebook account. We asked them to simultaneously login to their Facebook accounts in order to report various privacy behaviors and settings. Participant recruitment was done through snowball sampling [3] using two different methods: First, the primary researcher seeded the snowball through her personal SNSs, (such as Facebook Twitter, and LinkedIn), via email, and posting to Craigslist's volunteer's message board in her local city. Second, a random sample of 5,000 university email addresses were selected and emailed an invitation to participate in the survey. Participation was incentivized through a drawing with a chance to win one of two $200 Amazon gift certificates. Each participant who opted in received one drawing entry. As an extra incentive to share the survey, participants received one additional entry for each successful referral, up to a maximum of 25 entries.

## 3.2 Method of Analysis

### *3.2.1 Operationalization of Constructs*

In our domain-oriented feature analysis [23], our goal was to methodically identify the full set of Facebook privacy settings and features that were available within the interface for negotiating interpersonal boundary regulation. We leveraged these findings in our current study to provide participants with written directions and a screenshot on how to access these various settings and features. Next, we asked participants about specific actions they had previously taken using each privacy setting or feature. All questions asked regarding privacy behaviors are displayed in **Table 1**. Question order was optimized to reduce the number of clicks participants needed to take to access the various settings or features once they logged into their Facebook accounts.

Figure 1 shows an example of the privacy options for managing the content that filters into one's Facebook News Feed. What follows are the instructions participants received regarding these privacy options:

*"The next set of questions will ask you to report some basic information about how you manage updates in your Facebook News Feed from your friends."*

*"To do this: You would have had to click on the drop down arrow at the top, right corner of a post on your News Feed as shown below."*

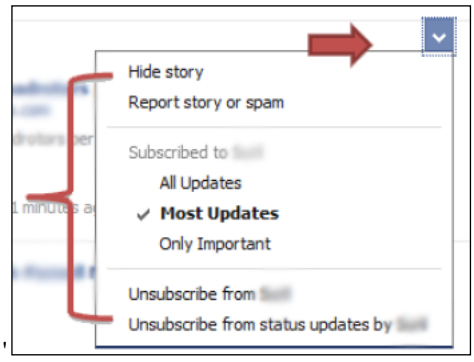


**Figure 1: Privacy Options for Managing Facebook News Feed**

After displaying the directions and screen shot associated with this privacy feature, we asked, "*How often have you done the following to modify posts on your News Feed?*" The privacy behaviors for altering one's News Feed (NWF, see Figure 1) included the frequency (1 = Never, 7 = Always) in which users: 1) Hid a story, 2) Reported Story or Spam, 3) Changed friend subscription settings, 4) Unsubscribed from a friend, or 5) Unsubscribed from status updates from a friend.

If a feature supported multiple behaviors, we asked a separate question for each behavior. Privacy behaviors that were in-situ were measured on a 7-point scale ranging from "Never" to "Always" on how frequently they used a particular privacy feature (similar to the example for **Figure 1**) or by a count of behavior frequency. For instance, we asked users to report how many users they had blocked (BLU), ranging from 1 = None to 5 = More than ten. Privacy behaviors that were tied to a specific privacy setting were measured based on the actual options provided by the Facebook interface. For example, participants were asked to report their Facebook profile settings for their "Basic Info" (BAS in **Table 1**). Possible responses included, "I did not provide this information to Facebook," "Public," "Friends," "Only Me," "Custom," and "Any customized friend list." These responses were coded from 1 = least private to $N$ = most private, given the number of options provided by Facebook.

### *3.2.2 Data Analysis Approach*

We adapted Knijnenburg et al.'s approach to analyzing the privacy behavior items in our dataset [10]. First, using a Confirmatory Factor Analysis (CFA) with a weighted least squares estimator [8, 15], we verified the multidimensionality of our privacy behavior items[1]. We adjusted the resulting factors (i.e. removing items, splitting and combining factors) until we achieved a satisfactory fit of the model to the data. Next, we performed a series of Mixture Factor Analyses (MFAs) with a robust maximum likelihood estimator [14-15]. MFA first establishes a CFA model and then sorts participants into a specified number of classes, where each class is allowed to have a different specific value on each of the factors. Any missing values in the dataset were excluded pairwise. This analysis results in a number of "privacy profiles". The optimal number of classes is determined by inspecting the model fit statistics.

# 4. RESULTS

## 4.1 Descriptive Statistics

We collected a total of 314 survey responses. After screening the data for outliers and excessive missing data, a total of 308 participants remained in the final analysis. The sample included 119 males and 189 females, with an average age of 35.74 (standard deviation: 12 years, range: 18 to 75). About 31% of the sample identified themselves as college students. The majority (91.6%) of the sample reported having a Facebook account for over 2 years with 19.2% having an active Facebook account over 6 years. Overall, the sample is skewed toward a predominantly white and well-educated, adult population who is not new to Facebook. The generalizability of the results may thus be constrained by these sample statistics.

[1] We also performed a series of Exploratory Factor Analyses (EFAs) with a weighted least squares estimator, Geomin rotation, and up to 13 factors on all items. This successfully reproduced the hypothesized dimensionality of the data.

**Table 1: Privacy Behavior CFA Results. Items with no factor loading were removed.**

| Factor | Code | Item | Loading |
|---|---|---|---|
| **Altering News Feed (NWF)** | NFH | Hid a story (*See **Figure 1***) | 0.845 |
| AVE: 0.777 | NFS | Changed friend subscription | 0.872 |
| | NFN | Unsubscribed to a friend | 0.908 |
| | NFP | Unsubscribed to status updates | 0.900 |
| **Timeline/Wall Moderation (WAL)** | CWD | Deleted content from Timeline/Wall | 0.783 |
| AVE: 0.638 | CWS | Reported/marked content as spam | 0.796 |
| | CWH | Hid a story | 0.817 |
| **Reputation Management (REP)** | UNT | Untagged a photo or post | 0.800 |
| AVE: 0.671 | TAK | Requested friends to take down posts or photos | 0.838 |
| **Limiting Access Control (LIM)** | TAG | Tag visibility privacy setting | 0.683 |
| AVE: 0.734 | SEE | Wall/Timeline post visibility privacy setting | 1.012 |
| | DEF | Default privacy level | *Removed* |
| **Blocking people (BLP)** | BLU | Blocked a user | 0.892 |
| AVE: 0.838 | RES | Added a user to restricted list | 0.938 |
| **Blocking apps/events (BLA)** | BLE | Blocked an event invite | 0.746 |
| AVE: 0.621 | BLA | Blocked an app invite | 0.828 |
| **Restricting Chat (CHA)** | SCF | Gone "offline" on Facebook chat | 1.013 |
| AVE: 0.777 | SCH | Default chat visibility | 0.744 |
| **Selective Sharing (SEL)** | POS | Posted a status to a custom friend list | 0.867 |
| AVE: 0.829 | PIC | Posting a photo to a custom friend list | 0.952 |
| **Friend Management (FRM)** | LIN | Categorized new friends into friend lists | 0.915 |
| AVE: 0.910 | LIO | Categorized existing friends into friend lists | 0.991 |
| **Withholding Contact Info. (CON)** | CIB | Withheld/restricted cell phone number | 0.742 |
| AVE: 0.780 | CIP | Withheld/restricted other phone number | 0.946 |
| | CIM | Withheld/restricted IM screen name | 0.880 |
| | CID | Withheld/restricted street address | 0.949 |
| **Withholding Basic Info. (BAS)** | BAD | Withheld/restricted "Interested In" | 0.750 |
| AVE: 0.700 | BAE | Withheld/restricted religion | 0.878 |
| | BAO | Withheld/restricted political views | 0.876 |
| **Concealing Network** | FRL | Hid Friend list from profile | *Removed* |
| **Denying Connection** | HID | Hidden a friend request | *Removed* |
| | UNF | Unfriended (frequency) | *Removed* |

## 4.2 Privacy Behavior CFA

We measured a total of 32 individual privacy behaviors that Facebook users could perform using the native Facebook interface. We performed a CFA to confirm that the respective privacy behaviors conceptually grouped with the higher-level privacy controls as provided by the Facebook interface (i.e. hiding a story in one's News Feed loaded with other privacy options for managing one's News Feed). The factor loadings of the final CFA solution for privacy behavior are presented in **Table 1** and the factor correlations between the different privacy behaviors are presented in **Table 2**. The final 11-factor model shows a good fit ($\chi^2(295) = 432.59$, $p < .001$; *CFI* = .987, *TLI* = .983; *RMSEA* = .039, 90% CI: [.031, .047]), as well as good convergent and discriminant validity.

The eleven dimensions of privacy behaviors are: 1) Altering one's News Feed; 2) Moderating one's Timeline/Wall; 3) Reputation management through untagging or asking a friend to take down an unwanted photo or post; 4) Limiting access control or visibility of information shared through one's Timeline/Wall; 5) Blocking people; 6) Blocking apps or event invitations; 7) Restricting chat availability; 8) Selective sharing through customized friend lists; 9) Custom friend list creation and management; 10) Withholding contact information; and 11) Withholding basic information. Four items were dropped because they did not load well with any of the factors: default Facebook privacy level (DEF), changing friend list visibility (FRL), hiding friend requests (HID) and unfriending (UNF). The remaining privacy behaviors loaded on factors that were consistent with specific Facebook interface features.

**Table 2: Privacy Behavior Factor Correlations***

| | NFW | WAL | REP | LIM | BLP | BLA | CHA | SEL | FRM | CON |
|---|---|---|---|---|---|---|---|---|---|---|
| **WAL** | .62 | | | | | | | | | |
| **REP** | .46 | .78 | | | | | | | | |
| **LIM** | .21 | .21 | .26 | | | | | | | |
| **BLP** | .42 | .41 | .35 | .23 | | | | | | |
| **BLA** | .46 | .55 | .54 | - | .65 | | | | | |
| **CHA** | .35 | .32 | .32 | .20 | .26 | .33 | | | | |
| **SEL** | .44 | .55 | .59 | .28 | .50 | .47 | .25 | | | |
| **FRM** | .45 | .49 | .35 | .23 | .44 | .40 | .21** | .76 | | |
| **CON** | .17 | .30 | .34 | - | .27 | - | - | .40 | .26 | |
| **BAS** | .15* | .29 | .27 | - | .25 | - | - | .27 | .16* | .67 |

**All listed correlations are significant at $p < .001$, except: * $p < .05$ and ** $p < .01$*

## 4.3 Classifying Facebook Users

Next, we used these factors to create classes of users based on their different privacy behaviors. The Mixture Factor Analysis (MFA) was run with an increasing number of classes; the optimal

number of classes at a point where subsequent models do not fit significantly better ($p$-value > .05), where the BIC (Bayesian Information Criterion) is at a minimum, where the entropy is highest, or where the loglikelihood levels off.

**Table 3** compares the different MFAs. Beyond a 2-class solution, no marginally significant improvements were made. However, the BIC is at a minimum for the 6-class solution, which is also where the entropy reaches its maximum value, and where the loglikelihood levels off. Therefore, we adopted the 6-class solution.

**Table 3: Privacy Behavior MFA Model Fit Statistics**

| | BIC | Entropy | LL | N | *p*-value |
|---|---|---|---|---|---|
| 1 class | 21998 | | -10534.652 | 162 | |
| 2 classes | 20829 | 0.915 | -9916.195 | 174 | < .001 |
| 3 classes | 20479 | 0.915 | -9706.503 | 186 | 0.1032 |
| 4 classes | 20324 | 0.880 | -9594.600 | 198 | 0.7248 |
| 5 classes | 20183 | 0.905 | -9489.752 | 210 | 0.1774 |
| **6 classes** | **20104** | **0.922** | **-9415.822** | **222** | **0.4441** |
| 7 classes | 20163 | 0.904 | -9411.090 | 234 | 0.7039 |

**Figure 2** shows the distribution of participants over the six privacy behavior classes. The largest class is "*Privacy Balancers*" (36%) followed by "*Privacy Minimalists*" (22%); the smallest class is "*Selective Sharers*" (5%).

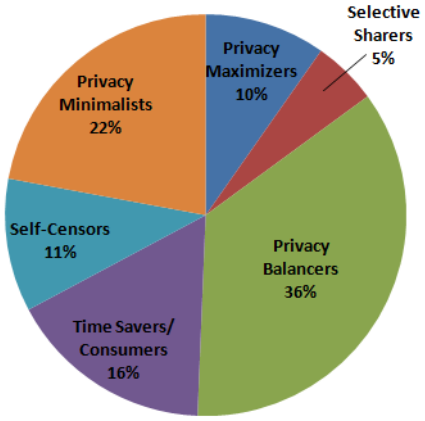


**Figure 2: Percent of Participants by Privacy Behavior Class**

To aid in comparisons, we use the same colors to represent each of the user classes in **Figures 3-6** as we do in **Figure 2**. **Figure 3** uses a stacked bar chart to show how the privacy behavior factors are distributed across users of different classes. This chart is weighted to account for the total number of users that belong to each class. Limiting access control by setting Timeline/Wall tagging and post visibility to "Friends Only" is the most common privacy strategy while blocking people, apps, and events is the least frequently employed strategy overall. Facebook users alter their News Feed privacy settings more frequently than moderating the posts to their Timeline/Wall. We also observed that a fair share of users tend to create and manage friend lists, but that they are actually less likely to use these lists to selectively share content with subsets of Facebook friends.

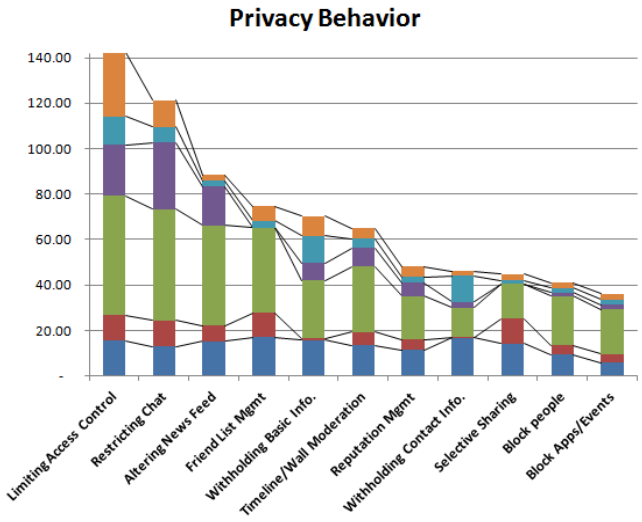


**Figure 3: Privacy Behavior by Behavior and User Class**

**Figures 4-6** illustrate how the different user privacy profiles vary based on the behavioral dimensions; all charts are drawn to the same scale to aid visual comparisons between classes.

**Figure 4** compares our user class "*Privacy Maximizers*" (10% of participants) with our "*Selective Sharers*" (5%—the minority of our participants). The *Privacy Maximizers* tend to report the highest levels of privacy behaviors across the majority of the privacy features, including completely withholding personal information (something no other users do to such a large extent). In contrast, the *Selective Sharers* leverage more advanced privacy settings: they create and manage customized friend lists, and use these to post content to selective groups of friends (something they do more often than the *Privacy Maximizers*). They are also more likely to share personal profile information, such as basic and contact information; this may be related to their selective sharing (e.g. their selective sharing allows them to share more personal information, or their tendency to share more personal information entices them to share more selectively).

In **Figure 5**, the "*Privacy Balancers*" (36%—the largest profile) exhibit moderate levels of privacy management behaviors, showing fewer privacy behaviors overall than *Privacy Maximizers* but more than "*Privacy Minimalists*." In contrast, the "Self-Censors" (11% of participants) use Facebook's privacy features and settings fairly infrequently but compensate by protecting their privacy through self-censorship, such as withholding basic and contact information from Facebook (i.e. opposite to the selective sharers).

In **Figure 6**, the *Privacy Minimalists* (22% of participants) report the fewest overall privacy strategies across all the user classes, managing their privacy only using the most common methods, such as limiting their Facebook profile so that they only share with friends by default. The "*Time Savers/Consumers*" (16% of participants) are similar to the *Privacy Minimalists*, however, they use privacy strategies that enable them to be passive consumers on Facebook without being bothered by unwanted others. For instance, they often restrict their chat availability so that others cannot initiate chat conversations with them and alter their News Feeds so that they can more effectively consume updates from their friends that are of most interest to them.

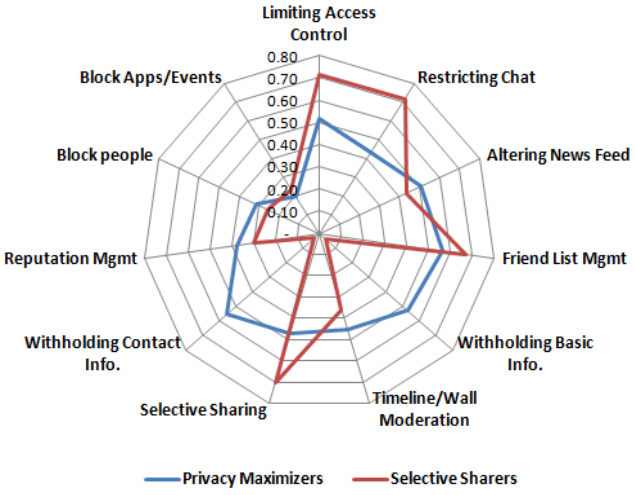


**Figure 4: Privacy Maximizers vs. Selective Sharers**

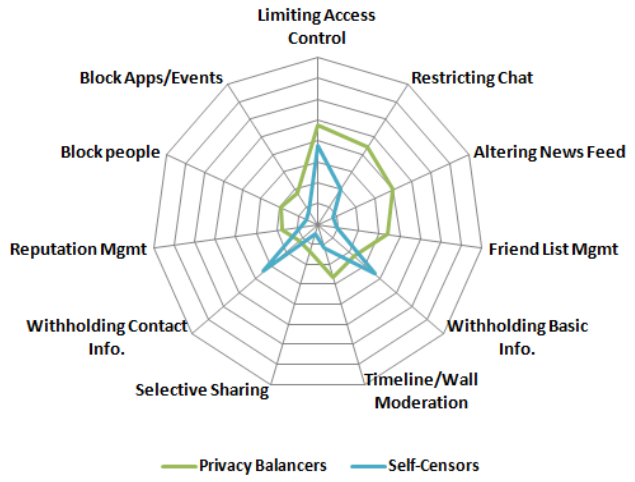


**Figure 5: Privacy Balancers vs. Self-Censors**

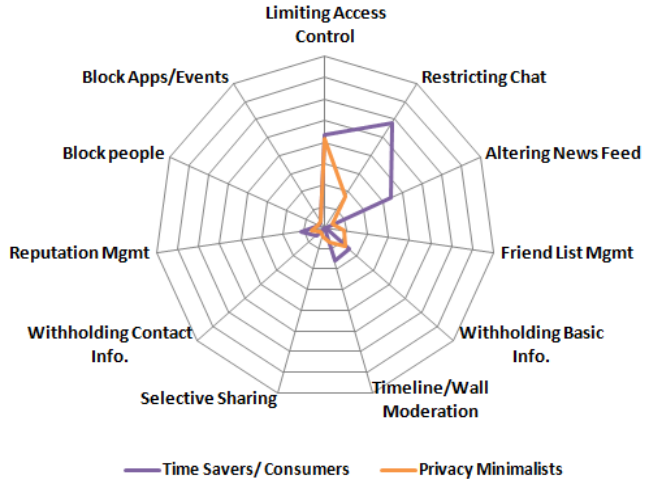


**Figure 6: Time Savers vs. Privacy Minimalists**

# 5. DISCUSSION AND CONCLUSION

Our results show first and foremost that most SNS users use a *subset* of Facebook's privacy features. In our analyses we uncover several interesting facts about this type of heuristic privacy management behavior. As our analysis demonstrates, users did not simply employ more or fewer privacy behaviors. Instead, their strategies show a distinctly multidimensional pattern. In other words, certain behaviors co-occur more frequently than others, resulting in unique privacy management strategies. Additionally, the dimensionality of privacy behaviors on Facebook is driven by physical groupings in the Facebook user interface. Our results thus suggest that conceptually grouping privacy settings and features by the privacy functionality that they support should be a crucial element of design.

Our work moves beyond Knijnenburg et al. [10] by addressing privacy behaviors other than information disclosure that can be used in various combinations to manage one's interpersonal privacy boundaries. For example, *Self-Censors* could arguably be leveraging a coping strategy to protect their personal privacy by reducing self-disclosures [22] in lieu of using privacy settings or features. It is possible that these users either are not aware of other privacy management strategies or find them too burdensome to employ. However, as a result, these users may be missing out on some of the social benefits that may be associated with sharing some level of personal information with some subset of their social networks [18]. In contrast, *Selective Sharers* take the opposite approach by using advanced privacy settings to facilitate self-disclosures to specific audiences. In future work, we are interested in exploring whether or not these different privacy strategies result in more optimal or sub-optimal user outcomes.

As it is, understanding the underlying dimensionality of privacy behaviors and interpreting these privacy profiles enables a number of theoretical and practical contributions. First, our work highlights privacy behaviors that are most common and most infrequent across all users. From a design perspective, privacy features that are used infrequently may present an opportunity for redesign or user education. For instance, our findings uncovered that users often create customized friend lists and group friends into these lists, but that that it is less common for them to actually *use* these lists to selectively share content. We initially expected for these two privacy behaviors (friend list management and selective sharing) to load on the same factor because they supported the same privacy strategy. However, this was not the case. Therefore, it would be interesting to understand why users go through the process of creating customized friend lists and categorizing friends if not to leverage this exercise as a privacy management strategy. It is possible that friend list management supports a different purpose; however, it is also possible the link between these two behaviors is disjointed because they are not physically grouped within Facebook's user interface.

Second, determining a user's privacy profile can be useful in personalizing settings, notifications, advice, and recommendations. For example, Facebook has recently introduced a "Privacy Dinosaur" that gives users timely tips on how to manage their privacy settings. To be effective, such tips need to relate to privacy mechanisms that fit users' personal privacy management strategies. The advice of the Privacy Dinosaur thus needs to be *personalized* [9]. Utilizing techniques similar to our privacy profiles may be one way this personalization may occur. One

approach would be to personalize the advice to support privacy strategies that are *congruent* with a user's current privacy profile; yet, another approach would be to nudge users toward alternative privacy management strategies by recommending strategies that are *different* from their current profile. For example, suggesting the use of friend list management and selective sharing may encourage *Self-Censors* to transform into *Selective Sharers*. An ethical consideration is to ensure that any potential behavior modification benefits SNS users, as opposed to (only) benefiting the SNS at users' expense.

Additional questions naturally arise as to why users develop certain privacy management strategies; is it related to certain privacy concerns, goals of Facebook use, or other demographic variables? How do these strategies change and evolve over time? How are these profiles related to other interactions with Facebook and other people? For example, we are currently examining how these behavioral strategies relate to users' awareness of the particular interface features for privacy regulation. Thus, investigating how these privacy management profiles relate to a variety of other factors will provide a deeper understanding of privacy and behavior on sites such as Facebook.

## 6. ACKNOWLEDGMENTS

We would like to thank Dr. David C. Wilson who co-advised the original dissertation work, which subsequently contributed to this research collaboration.

## 7. REFERENCES

[1] Acquisti, A. and Grossklags, J. What Can Behavioral Economics Teach Us About Privacy? *Digital Privacy: Theory, Technologies, and Practices* (2008 2008), 363–377.

[2] Altman, I. *The environment and social behavior*. Brooks/Cole Monterey, CA, 1975.

[3] Babbie, E. *The Practice of Social Research*. Wadsworth Publishing Company, Belmont, CA, 2004.

[4] Compañó, R. and Lusoli, W. The Policy Maker's Anguish: Regulating Personal Data Behavior Between Paradoxes and Dilemmas. In T. Moore, D. Pym and C. Ioannidis (eds.) *Economics of Information Security and Privacy*, (2010), 169-185.

[5] Ellison, N. B., Vitak, J., Steinfield, C., Gray, R. and Lampe, C. Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environments. In *Privacy Online*, (2011).

[6] Gross, R. and Acquisti, A. Information revelation and privacy in online social networks. In *Proc. Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, ACM (2005), 71-80.

[7] Kairam, S., Brzozowski, M., Huffaker, D. and Chi, E. Talking in circles: Selective Sharing in Google+. In *Proc. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM Press (2012), 1065-1074.

[8] Kline, R. B. *Principles and Practice of Structural Equation Modeling*. The Guilford Press, New York, 2011.

[9] Knijnenburg, B. P. Simplifying Privacy Decisions: Towards Interactive and Adaptive Solutions. In *Proc. Proceedings of the Recsys 2013 Workshop on Human Decision Making in Recommender Systems (Decisions@ RecSys'13)* (2013), 40-41.

[10] Knijnenburg, B. P., Kobsa, A. and Jin, H. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies*, *71* (2013 2013), 1144-1162.

[11] Lampinen, A., Lehtinen, V., A., L. and Tamminen, S. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. In *Proc. Proceedings of the annual conference on Human factors in computing systems* (2011).

[12] Lipford, H. R., Besmer, A. and Watson, J. Understanding Privacy Settings in Facebook with an Audience View. In *Proc. Usability, Psychology, and Security 2008 (UPSEC 2008)* (2008 ).

[13] Madden, M. *Privacy management on social media sites*. Pew Research Internet Project, 2012, http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/.

[14] Muthén, B. Latent variable hybrids: Overview of old and new models. In G. R. Hancock and K. M. Samuelsen (eds.) *Advances in latent variable mixture models*, (2007).

[15] Muthen, L. K. and Muthen, B. O. *Mplus Statistical Analysis with Latent Variables User's Guide*, 2010.

[16] Stutzman, F., Capra, R. and Thompson, J. Factors mediating disclosure in social network sites. *Computers in Human Behavior*, *27*, 1 (2011), 590-598.

[17] Stutzman, F. and Kramer-Duffield, J. Friends Only: Examining a Privacy-Enhancing Behavior in Facebook. In *Proc. ACM Conference on Human Factors in Computing Systems* (2010).

[18] Stutzman, F., Vitak, J., Ellison, N. B., Gray, R. and Lampe, C. Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook. In *Proc. Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media* (2012).

[19] Tufekci, Z. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, *28*, 1 (February 1, 2008 2008), 20-36.

[20] Watson, J., Besmer, A. and Lipford, H. R. +Your circles: sharing behavior on Google+. In *Proc. Proc. of the 8th Symposium on Usable Privacy and Security*, ACM (2012).

[21] Wisniewski, P. *Understanding and Designing for Interactional Privacy Needs within Social Networking Sites*. Dissertation, University of North Carolina at Charlotte, Charlotte, NC, 2012.

[22] Wisniewski, P., Lipford, H. and Wilson, D. Fighting for My Space: Coping Mechanisms for SNS Boundary Regulation. In *Proc. ACM Conference on Human Factors in Computing Systems* (2012).

[23] Wisniewski, P., Lipford, H. R. and Wilson, D. C. A New Social Order: Mechanisms for Social Network Site Boundary Regulation. In *Proc. Americas Conference on Information Systems* (2011).