Balancing Privacy Concerns and Impression Management Strategies on Facebook

Jessica Vitak
College of Information Studies
University of Maryland
4105 Hornbake Building, South Wing
College Park, MD 20742
jvitak@umd.edu

ABSTRACT

Social network sites like Facebook allow users to engage in self-presentation through a variety of text-based, visual, and interactive features, and numerous studies have examined the various social and technical strategies Facebook users engage in to manage their online persona. That said, few studies have examined how engagement in these impression management strategies varies across users. This paper presents initial findings from a large (N=833) study including three samples to evaluate the relationship between individual factors, network composition and privacy concerns with the use of social and technical features to regulate access to personal information on Facebook. Rather than a straightforward relationship between privacy concerns and impression management, findings suggest that engagement in these strategies involves a number of contextual factors such as age, sex, and Internet efficacy. These complex relationships are discussed with a focus on implications for researchers and designers to consider when evaluating and building these systems.

1. INTRODUCTION

With the explosion in popularity of social network sites (SNSs) in the last decade, researchers have increasingly focused on self-presentation and impression management in digital spaces. SNSs' affordances alter these practices in several important ways. First, one's audience for self-presentation becomes less clear online because of the blurring of public and private spaces [3]; because of this, individuals use an "imagined audience" [14] to guide their sharing behaviors. Second, compared with more ephemeral forms of communication, digital interactions are both highly visible and persist long after the interaction [29]. Even content shared via "ephemeral" platforms (e.g., Snapchat) can be easily captured and disseminated beyond the intended audience. Third, in many of these spaces the technical structure of the site collapses offline relational boundaries between network members (i.e., context collapse) [31]. By labeling all contacts as "friends," individuals become more limited in their ability to vary self-presentation based on audience.

A popular stream of research in this area has focused on the apparent mismatch between users' stated level of privacy concerns and their disclosure habits. The *privacy paradox* occurs when people with high concerns also disclose a lot of personal information. Early research focused on Facebook users' profile disclosures [1, 30], while later research looking at more interactive disclosures (e.g., through status updates) found little or no evidence of a privacy paradox [26, 27, 31].

The present study focuses not on the relationship between privacy and disclosures, but on the social and technical strategies users employ to manage their network's access to their content and to maintain a desired online persona. These strategies range from blocking, unfriending, and denying connections to limiting the audience for content and engaging in self-censorship. Does a paradox exist between privacy concerns and engagement in these strategies, or is the relationship more complex, involving factors such as online skills, age, and network diversity?

Findings from this study provide valuable insights to the SOUPS community on the relationship between users' privacy concerns and their impression management behaviors on SNSs, and offer new factors to consider when designing systems to maximize flexibility, usability, and control.

2. RELATED WORK

2.1 Impression Management (IM) Online

Goffman's [7] seminal research on self-presentation framed the activity as a performance in which individuals alter their performance based on their audience. Everything from style of dress to speech may vary from audience to audience, based on the impressions the individual wants to engender in his audience.

When moving to digital spaces, social media users are encouraged to disclose a lot of personal information as they connect with old and new contacts and share updates, images, and other content. However, these networked spaces have unique affordances and features that users must consider when disclosing personal information. First, when interacting offline, individuals are generally aware of their audience—it could be a single person, or a group of friends, or a packed theater. Online, "invisible audiences" [3] are often present, such as in the case of public tweets, and are complicated by the blurring of public and private spaces, such that it is not always clear who has access to a given piece of content. One's skills at navigating these spaces becomes a critical factor as the platforms add, modify, and delete features related to content visibility and control.

Even when posting publicly, individuals share content with an audience in mind [18]. These "imagined audiences" [14] may differ significantly from the actual audience for a piece of content. For example, Bernstein and colleagues [2] found that Facebook users significantly underestimate the audience for content they shared on the site. This underestimation may become problematic when combined with the technical structure of these spaces, such

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22-24, 2015, Ottawa, Canada.

that the boundaries separating network groups and contexts is flattened into a homogeneous group of contacts [31]. While sites like Facebook and Google Plus have built-in features to allow users to segment their audiences, these features are generally under-utilized; even those who use the features describe them as cumbersome [34]. Other sites like Twitter have only two dissemination settings: public or private.

Because of the time and energy associated with re-creating offline boundaries on social media, researchers have highlighted a wide range of social and technical strategies to manage one's online persona. For example, Lampinen and colleagues [12] distinguish between preventive (e.g., through settings, self-censorship, careful crafting of content) and corrective (e.g., deleting or untagging content) strategies. Vitak et al. [33] group strategies based on the mechanism for achieving control: network, platform, content, and multiple profiles. Multiple researchers [4, 10, 25] describe variations on self-censorship as a strategy, whereby an individual chooses to not post a message or alters a message to avoid turbulence. Researchers have also distinguished between individual-level and collective or group impression management, highlighting how a significant amount of impression management is in the hands of friends, network members, and sometimes strangers [6, 12, 16].

2.2 The Role of Privacy Concerns

The conceptualization of privacy concerns in SNS research has evolved over the past decade, from a broad focus on general concerns [1] to technology-specific concerns [26] and, more recently, to concerns related specifically to the content and networks with whom individuals interact in these spaces [31]. For example, research examining location-sharing technologies found that users expressed concern about how sharing location information in their social media updates might change their relationship with network members [20]. This shift in the focus on privacy concerns reflects Helen Nissenbaum's [19] work on the role of context in managing one's privacy. Nissenbaum argues that we must evaluate both access control as well as contextual norms. As she notes when defining "contextual integrity":

> *Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation. … the social phenomenon of distinct types of contexts, domains, spheres, institutions, or fields is firmly rooted in common experience (p. 119).*

The norms guiding use of SNSs are often unclear and shift quickly with the technology. Uncertainty about one's ability to control access to information increases privacy-related concerns [22]; with Facebook, the frequent modifications to the privacy policy and privacy settings, as well as new features that shift control from the individual to the network (such as tagging updates and photos) is likely to increase privacy concerns among some users.

2.3 Relationship Between Privacy Concerns Impression Management Behaviors

Situating Nissenbaum's [19] work on contextual integrity within SNSs, it becomes clear that context plays a significant role in individuals' attitudes and behaviors. It is likely that individual users' decisions on how to manage their online personas are guided by a number of factors.

This exploratory study focuses on the relationship between users' privacy concerns and their engagement in strategies to manage access to their personal information.

RQ1: How do concerns about privacy on Facebook vary across demographic and site-based factors?

H1: Concerns about one's online privacy will positively correlate with engagement in impression management strategies on Facebook.

H1a: This relationship will be moderated by the skill of the user.

H1b: This relationship will be moderated by the diversity of a user's network.

3. METHOD

Data were collected in fall 2014 from three samples: (1) American adult Mechanical Turk workers recruited through a HIT, (2) a random sample of 2000 university staff, and (3) a random sample

Table 1: Descriptive Statistics for Three Samples With ANOVA Comparison

Variable	F-test	Mechanical Turk (N=577)	University Staff (N=258)	Undergrads (N=279)	Full Sample (N=1112)
Sex: Female	15.03***	45%[a]	64%[b]	57%[b]	52%
Age	326.37***	33.56[b]	40.47[c]	19.99[a]	31.70 (*SD*=12.05)
Education[1]	265.21***	2.46[b]	3.36[c]	2.00[a]	2.56 (SD=.85)
Race: White	5.52**	73%[b]	68%[ab]	62%[a]	69%
Internet Efficacy	20.19***	3.59[b]	3.30[a]	3.16[a]	3.42 (*SD*=1.02)
Facebook User	35.96***	66%[a]	75%[b]	92%[c]	74%
Use Other Social Media Platforms	9.00***	82%[a]	78%[a]	91%[b]	83%
Privacy Concerns	4.73**	3.10[a]	3.28[ab]	3.35[ab]	3.22 (*SD*=1.06)
Content-Based IM Strategies	2.29 *ns*	2.41[a]	2.35[a]	2.51[a]	2.43 (*SD*=.82)
Network-Based IM Strategies	2.08 *ns*	2.50[a]	2.50[a]	2.63[a]	2.54 (*SD*=.82)

[1] In streamlining the education measure to be applicable to all survey populations, the undergraduate sample all fall into the same category (i.e., some college or post-secondary training, no degree).

Notes: Superscript letters show groupings based on Tukey's B post hoc tests. * $p < .05$ ** $p < .01$ ***$p < .001$

of 2000 university undergraduates. The student and staff samples were provided by the university's registrar and human resources departments, respectively. In each case, participants were invited to complete an online survey about their online communication practices and were compensated with direct payment (in the case of Turkers) or entry into a raffle for one of 10 $50 Amazon gift cards (for the university samples). A total of 1119 usable responses were received[1]. For the subsample of Facebook users (N=833), 56% were female and the average age was 30 (median=27, *SD*=11.54). See Table 1 for details.

3.1 Measures

3.1.1 Privacy Concerns

Participants were asked to rank their level of concern regarding 11 Facebook-specific privacy concerns used in a previous study [32]. The 11 items formed a reliable scale (α=.92, *M*=3.22, *SD*=1.06) and includes both site-based and network-based concerns. See Table 2 for items, means, and standard deviations.

3.1.2 Impression Management Strategies

Participants were also asked about the frequency with which they engaged in 14 impression management strategies. These items were developed based on findings from previous studies (e.g., [4, 12, 34] and reflect both individual vs. collaborative strategies as well as social vs. technical strategies.

Exploratory factor analysis using Varimax rotation was conducted on the 14 items; after removing three items a two-factor solution was obtained. The first factor includes six items and is labeled "content-based impression management strategies" (α=.83, *M*=2.43, *SD*=.82) and reflects ways in which individuals control the content they share on the site. The second factor, "network-based impression management strategies" (α=.79, *M*=2.54, *SD*=.82) reflects individuals' decisions about who has access to content. All items are included in Table 3.

3.1.3 Facebook Network Diversity

Participants were asked to select all groups of people present in their Facebook Friend network from a list of 17 options plus an open-ended "other" category. Sample groups included current romantic partner, former romantic partner, friends from high school, friends from college, friends from a former job, friends from a current job, and online-only friends. Participants reported, on average, that their Facebook network included 8.9 categories of friends (median=9, *SD*=3.03, range: 0-16).

3.1.4 Online Skills/Efficacy

This study includes two measures to capture individuals' ease of navigating the Web. First, the 10-item version of Hargittai and Hsieh's [9] Web-use Skills measure asks participants to rate their familiarity of various Web-related terms (e.g., PDF, cache, malware) on a 1-5 scale. Higher scores indicate higher levels of perceived familiarity. Analysis led to the removal of one item (weblog), resulting in a nine-item scale (α=.91, *M*=3.94, *SD*=.89). Second, an abridged Internet efficacy scale [12] was included. One item was dropped from the final scale, leading to a reliable, three-item measure (α=.89, *M*=3.42, *SD*=1.02).

Table 2. Privacy Concerns Scale Items

Items	*M*	*SD*
Privacy Concerns	**3.22**	**1.06**
Your account being hacked.	3.44	1.41
Your picture being used in a Facebook ad.	3.07	1.52
Unwanted contact from another user.	2.84	1.37
Your account information being compromised.	3.62	1.36
Private messages becoming publicly visible.	3.33	1.46
A Facebook friend posting mean, unflattering, or factually incorrect content about you.	2.66	1.43
Being tagged in a photo you don't want linked to your account.	3.19	1.32
Your employer viewing content (text or photos) that might negatively impact your job.	2.85	1.50
Your personal information becoming publicly visible.	3.57	1.39
Your personal information being sold to other companies for marketing purposes.	3.51	1.38
Being tagged in an update that identifies your current physical location.	2.96	1.38

Item prompt: "Indicate your level of concern about the following things that might happen when you use Facebook." (Five-point scale, range: Not at all Concerned to Very Concerned)

Table 3. Impression Management Scale Items

Items	M	SD
Content-Based Impression Management	**2.43**	**0.82**
Spend time thinking about who can see a piece of content you're sharing.	2.81	1.17
Delete a status update before posting.	2.63	1.10
Change the wording of a status update to avoid angering some of your Facebook friends.	2.37	1.12
Delete a status update you've already posted.	2.35	1.00
Delete a photo or photo album you've already shared.	2.19	1.06
Post a status update to a subset of your Facebook friends so that it will not be visible to a specific user or group of friends.	2.22	1.18
Network-Based Impression Management	**2.54**	**0.82**
Defriended someone because of the content they share on the site.	2.43	1.10
Defriended someone you no longer talk to.	2.61	1.12
Refuse a friend request from someone you know.	2.67	1.08
Block another Facebook user.	2.31	1.07
Hide a Facebook friend (so their posts no longer appear in your News Feed).	2.03	1.16

Item prompt: "How often do you engage in the following behaviors when using Facebook?" (Five-point scale, range: Never to Very Often)

[1] Sixty-one participants' responses were removed because of missing data (See Section 3.2).

3.1.5 Controls

Lampe et al.'s [11] Facebook Appropriateness Scale was included to control for individual users' attitudes about sharing content through the site. One item ("Facebook is an appropriate place to coordinate events") was removed to increase the scale's reliability, leading to a four-item scale (α=77, *M*=2.95, *SD*=.79). Rosenberg's [23] seven-item Self-Esteem measure (*M*=4.09, *SD*=68) was included as a control because of its significance in previous studies of Facebook use.

3.2 Data Analysis

Each case was examined closely using Missing Value Analysis in SPSS v21. Criteria for removal of a case from analysis was missing data for 10% or more of the total items in the survey or missing data for more than 25% of items in a scale. This led to the removal of 23 cases from Mechanical Turk sample, 22 cases from the university staff sample, and 16 cases from the university undergraduate student sample. No single item had more than 2% of total cases missing, so missing data for the remaining cases were imputed using the Expectation-Maximization (EM) algorithm [24].

Because significant differences emerged between the three samples on some measures, all analyses control for this factor.

4. FINDINGS

4.1 Predicting Privacy Concerns

As seen in Table 2, participants' privacy concerns, on average, fell slightly above the midpoint, with a scale average of 3.22, suggesting that Facebook users have some concerns about content they share and corporate practices of the site. The highest level of concerns related to users' accounts being compromised, while the lowest concerns related to actions by other users.

To determine how privacy concerns varied across individual factors and site-specific behaviors, an OLS regression was run with users' privacy concerns as the dependent variable (see Table 4 for results). Women reported slightly higher concerns than men (β=.08, p<.05), but no differences were observed across age, education, or Internet efficacy. In addition, engagement in content-based impression management strategies positively predicted privacy concerns (β=*.40,* p<.001) while network-based strategies were unrelated.

In a separate set of analyses, those with the greatest privacy concerns were compared to those with the fewest privacy concerns. In a series of independent samples t-tests comparing the first (*M*<2.4) and fourth (M>4.1) quartiles, only engagement in impression management strategies varied significantly between groups. In both cases, those with the greatest concerns reported engaging in more content-based (*M*=2.72, *SD*=.86 vs. *M*=1.98, *SD*=.66; *t*(430)=-10.08, *p*<.001) and network-based (*M*=2.78, *SD*=.91 vs. *M*=2.23, *SD*=.74; *t*(430)=-6.89, *p*<.001) strategies.

4.2 Predicting IM Strategy Engagement

Two OLS regressions were run with the impression management scales as dependent variables (see Table 4 for results).[2]

[2] Both online skills and Internet efficacy were tested separately, but because they were strongly correlated (*r*=.60), only Internet efficacy was significant, so it was included.

Table 4. OLS Regressions Predicting Engagement in Impression Management Strategies on Facebook

	IM Content Strategies	IM Network Strategies	Privacy Concerns
Variables	Standardized Betas (t-score)		
Sample[1]	*	*	**
Sex: Female	.12 (3.53)***	.10 (2.92)**	.08 (2.17)*
Age	-.19 (-5.24)	-.21 (-5.65)***	.05 (1.37)
Facebook Appropriate	.10 (3.22)***	-.03 (-.74)	-.07 (-2.09)*
Internet Efficacy	.10 (3.07)**	.08 (2.14)*	.00 (-.02)
Network Diversity	.09 (2.701)**	.13 (3.87)***	-.06 (-1.65)
Self-Esteem	-.07 (-2.17)*	.01 (.40)	.01 (.26)
Privacy Concerns	.39 (12.33)***	.26 (7.87)***	n/a
IM Content Strategies	n/a	n/a	.40 (9.15)***
IM Network Strategies	n/a	n/a	.02 (.34)
F-test	30.98***	17.19***	20.52***
Adjusted R^2	.23	.14	.18

[1] A variable for the three samples is included as a control only.

* p<.05 ** p<.01 *** p<.001

In the regression predicting frequency of engagement in content-based impression management strategies, all included variables were significant, whereas Facebook Appropriateness and self-esteem (included as controls) were not significant in the regression predicting engagement in network-based strategies.

Overall, the findings indicate that women, younger users, and those more skilled at using the Web reported engaging in both types of impression management strategies more often. Likewise, diversity of one's network and privacy concerns were positively correlated with engagement in both strategies. This provides support for H1: As one's privacy concerns related to Facebook increase, so does one's engagement in strategies to manage network access and content visibility.

To test H1a and H1b, interaction terms were created crossing privacy concerns by (1) the network diversity measure and (2) the user's age. When added to the regression, the first interaction term (network diversity by privacy concerns) was significant for both impression management strategies (content: β=.08, p<.05; network: β=.07, p<.05); the second (Internet efficacy by privacy concerns) was not.

Plotting these variables reveals the nature of the interaction (see Figure 1); as one's privacy concerns increased, the increase in engagement in impression management strategies narrowed between those with very diverse and less diverse networks. In other words, the diversity of one's Facebook friend network only

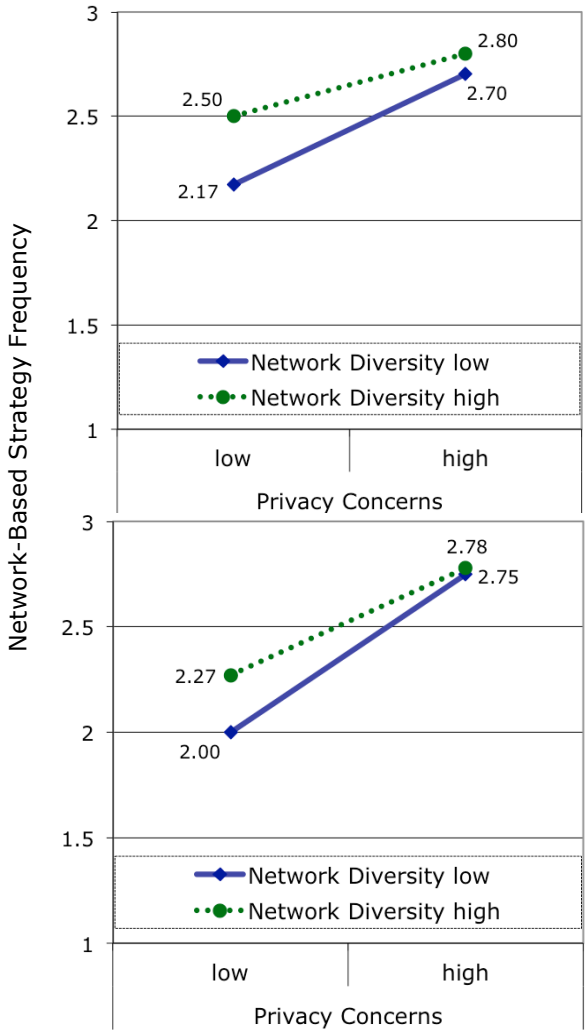

Figure 1. Network Diversity and Privacy Concerns Interaction Effect Predicting Impression Management Strategies.

matters for those with low privacy concerns. When privacy concerns are high, there is little difference in engagement in network- and content-based strategies.

5. DISCUSSION

Findings from these preliminary analyses provide useful insights into factors that influence active engagement in impression management online. Increasingly, our digital footprints are being used to make important decisions ranging from hiring and firing by employers to acceptance at universities; therefore, it is critical for researchers and designers to understand how users interact with these systems and incorporate features that encourage profile curation without being too complex or time-consuming.

As found in both the regressions and moderation analyses predicting engagement in impression management, concerns about who can see personal information, how that personal information is used, and the security that information from unwanted access play a significant role in predicting engagement in behaviors to manage one's online persona. This finding provides empirical support to a number of qualitative studies that have linked privacy concerns to these strategies [12, 25, 34]. Beyond this, the findings regarding age and gender support previous privacy research [17, 21, 28], whereas the non-significant findings for online skills (not included in the final regressions) were somewhat surprising.

Understanding the relationship between privacy concerns and impression management behaviors provides an important piece in evaluations of the privacy paradox. Many of the strategies users may engage in on SNSs are invisible, so standard measures of disclosures [1, 26, 30] may not capture a users' overall strategy. At the same time, the low engagement across behaviors (with all falling blow the midpoint in the scale) and the non-significant relationship between network strategies and privacy concerns suggests additional factors at play. In a qualitative study by Vitak and Kim [24], some participants said that impression management strategies like using the Friend List to segment one's network were too time consuming or tedious, which often led to self-censorship rather than employing strategies to define the audience. It is unsurprising that any "cost" associated with preventative or protective behaviors would decrease engagement; this is often seen in technology adoption and usability research.

The low values for impression management strategies are somewhat at odds with the privacy concern item that merited the highest levels of concern, i.e., that of private information becoming publicly visible. On Facebook especially, users never have full control over information that might conflict with their desired self-presentation because of the various ways in which individuals and content are connected. While the items that factored into the two impression management strategy variables used in this study reflect user-centered behaviors, other studies have begun to explore system- and other-behaviors that factor into self-presentation (e.g., [6, 16]). Future research needs to incorporate the complexities of friendship, interaction, and privacy on these sites.

The biggest challenge for designers is developing usable, flexible, and low-cost features that facilitate impression management. Over the past year, Facebook's Privacy Team[3] has released a number of new features to help users' quickly check and update their privacy settings on the site, most notably through the Privacy Checkup Feature [5]. This development represents significant progress on making privacy features more accessible, but additional research needs to be conducted focusing on the most vulnerable users, including adolescents and seniors. These groups face additional challenges of low skills (in the case of seniors) and distinct sharing norms (in the case of adolescents) that may put them at a higher risk of negative outcomes ranging from identity theft to loss of employment or educational opportunities.

6. CONCLUSION

As more people join SNSs and begin sharing personal information, the need for creating customized privacy features becomes paramount to ensure users can safely navigate these spaces. Therefore, it is important to assess the most salient concerns users have as well as their current knowledge and practices to protect their information. The present study highlights the complexity in this relationship and provides some directions

[3] https://research.facebook.com/security

for future researchers and designers to consider when working with SNSs. Future researchers should work to better map the role of normative and contextual factors to this relationship, as this will help advance both theory and design in this area.

7. REFERENCES

[1] Acquisti, A. and Gross, R. Imagined communities: awareness, information sharing, and privacy on the Facebook. *Proc. PET 2006,* Springer (2006), 36-56.

[2] Bernstein, M.S., Bakshy, E., Burke, M. and Karrer, B. Quantifying the invisible audience in social networks. In *Proc. CHI* (2013), ACM Press, 21-30.

[3] boyd, d. Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi, ed., *Networked Self: Identity, Community, and Culture on Social Network Sites*. 2010, 39–58.

[4] Das, S. and Kramer, A. Self-censorship on Facebook. In *Proc. ICWSM*, AAAI Press (2013).

[5] DeAmicis, C. It's time for a "privacy checkup" from your Facebook doctor. GigaOm. September 4, 2014. Available: https://gigaom.com/2014/09/04/its-time-for-your-privacy-checkup-from-your-facebook-doctor/

[6] De Wolf, R., Willaert, K. and Pierson, J. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior 35* (2014), 444-454.

[7] Goffman, E. *The Presentation of Self in Everyday Life*. Doubleday Anchor, New York, 1959.

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

[9] Hargittai, E. and Hsieh, Y. P. Succinct survey measures of web-use skills. *SSCR, 30* (2012)*,* 95-107.

[10] Hogan, B. The Presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society 30*, 6 (2010), 377–386.

[11] Lampe, C., Vitak, J., and Ellison, N. Users and nonusers: Interactions between levels of Facebook adoption and social capital. In *CSCW*, ACM Press (2013), 809-820.

[12] Lampinen, A., Lehtinen, V., Lehmuskallio, A. and Tamminen, S. We're in it together: Interpersonal management of disclosure in social network services. In *Proc. CHI*, ACM Press (2011), 3217–3226.

[13] Larose, R., Mastro, D. and Eastin, M.S. Understanding Internet Usage. *SSCR*, *19* (2000). 395-413.

[14] Litt, E. Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media*, *56*, 3 (2012), 330-345.

[15] Litt, E. Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29* (2013), 1649-1656.

[16] Litt, E., E. Spottswood, Birnholtz, J., Hancock, J.T., Smith, M.E. and Reynolds, L.Awkward encounters of an "other" kind: collective self-presentation and face threat on Facebook. In *Proc CSCW,* ACM Press (2012), 449-460.

[17] Maab, W. (2011). The elderly and the Internet: How senior citizens deal with online privacy. In *Privacy Online* (pp. 235-250). Berlin: Springer.

[18] Marwick, A.E. and boyd, d. I tweet honestly, I tweet passionately: Twitter users, context collapse, & the imagined audience. *New Media & Society, 13* (2011), 114–133.

[19] Nissenbaum H.F. *Privacy in Context: technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA, 2010.

[20] Page, X., Kobsa, A. and Knijnenburg, B.P. Don't disturb my circles! Boundary preservation is at the center of location-sharing concerns. In *Proc ICWSM*, AAAI (2012), 266-273.

[21] Peter, J., and Valkenburg, P. M. Adolescents' online privacy: Toward a developmental perspective. In *Privacy Online* (pp. 221-234). Berlin: Springer, 2011.

[22] Petronio, S. *Boundaries of Privacy.* State University of New York Press, Albany, NY, 2002.Page Kobsa

[23] Rosenberg, M. *Society and the Adolescent Self-image*. Wesleyan University Press, Middletown, CT, 1989.

[24] Schlomer, G. L., Bauman, S., & Card, N. A. Best practices for missing data management in counseling psychology. *Journal of Counseling Psychology* (2010)*, 57,* 1-10.

[25] Sleeper, M., Balebako, R., Das, S., McConahy, A.L., Wiese, J., and Cranor, L.F. The post that wasn't: Exploring self-censorship on Facebook. *In Proc. CSCW,* ACM Press (2013), 793–802.

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

[27] Stutzman, F., Vitak, J., Ellison, N., Gray, R., & Lampe, C. Privacy in interaction: Exploring disclosure and social capital in Facebook. In *Proc ICWSM* (pp. 330-337)*.* Washington, DC: AAAI, 2011.

[28] Thelwall, M. Privacy and gender in the social web. In S. Trepte and L. Reinecke, eds., *Privacy Online*. Springer, Heidelberg and New York, 2011, 251–266.

[29] Treem, J.W. and Leonardi, P.M. Social media use in organizations: Exploring the affordance of visibility, editability, persistence, and association. *Communication Yearbook 36* (2012), 143-189.

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

[31] Vitak, J. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting and Electronic Media, 56,* 4 (2012), 451- 470.

[32] Vitak, J. *Keeping connected in the Facebook age*. Doctoral dissertation, Michigan State University, East Lansing, MI, 2012.

[33] Vitak, J., Blasiola, S., Patil, S., and Litt, E. Balancing audience and privacy tensions on social network sites. *iJOC, 9* (2015)*,* 1485-1504.

[34] Vitak, J. and Kim, J. "You can't block people offline": Examining how Facebook's affordances shape users' disclosure process. In *Proc. CSCW,* ACM Press (2014), 461-474.