Computers in Human Behavior 29 (2013) 1649–1656

Contents lists available at SciVerse ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Understanding social network site users' privacy tool use

Eden Litt

Media, Technology & Society, Northwestern University, 2240 Campus Dr., Evanston, IL 60208, USA

ARTICLE INFO

Article history:
Available online 8 March 2013

Keywords:
Social network sites
Privacy
Reputation
Self-presentation
Privacy management
Digital inequality

ABSTRACT

Every day hundreds of millions of people log into social network sites and deposit terabytes of data as they share status updates, photographs, and more. This article explores how background factors, motivations, and social network site experiences relate to people's use of social network site technology to protect their privacy. The findings indicate that during technology-mediated communication on social network sites, not only do traditional privacy factors relate to the technological boundaries people enact, but people's experiences with the mediating technology itself do, too. The results also identify privacy inequalities, in which certain groups are more likely to take advantage of the technology to protect their privacy—suggesting that some individuals' information and reputations may be more at risk than others'.

1. Introduction

Every day hundreds of millions of people log onto social network sites and share their latest updates creating online repositories of accessible self-presentations. While there are many benefits to disclosing information on social network sites, accompanying such disclosures are also risks, as increasingly our digital footprints are also playing an important role in impression formations (Hancock & Dunham, 2001; Stelter, 2012; Tong, Van Der Heide, Langwell, & Walther, 2008). As social network sites increase in popularity and people from a wide variety of life contexts use such services, not only are friends and family forming impressions based on people's self-presentations online, but additional people and entities are also surveying these spaces, including coworkers, current and potential employers, insurance companies, government agencies, advertisers, and law enforcement (Clark & Roberts, 2010; Microsoft, 2010). In 2012, more than 90% of a sample of human resource and recruiting professionals reported that they used social network sites, including Facebook, to recruit potential job candidates—an increase from the prior year and a percentage that is likely to continue to rise (Jobvite, 2012). There are now entire businesses devoted to conducting social media background checks on potential employees (Preston, 2011).

Research indicates that many social network site users engage in a variety of social and technological strategies to help selectively control the flow of their information including refraining from disclosing information altogether and using a service's privacy settings (Boyd & Hargittai, 2010; Marwick, Murgia-Diaz, & Palfrey, 2010; Tufekci, 2008). However, while researchers have explored many aspects of privacy and disclosure on social network sites (e.g., Acquisti & Gross, 2006; Paine Schofield & Joinson, 2008; Waters & Ackerman, 2011), limited work has focused on the technological strategies users implement. Technological privacy strategies describe when users take advantage of a site's features or tools to help maintain their privacy preferences. Such tools include "lists" that allow users to share information with select contacts, buttons that allow for the deletion of posted content, and features that allow users to untag posts and images linked with their identities. Theoretically, individuals use a site's features to tell the technology what they want or do not want shown, and to whom, and then the technology preserves such privacy preferences. For example, if a friend tags a photo of a friend at a bachelorette party, she may decide she does not want any of her contacts on the site to have access to this photo. She can choose to click the untag button so that the social network site no longer links the particular photo with her profile, and it is no longer accessible to her contacts through her profile.

Of the research that has centered on the use of such tools, most has focused specifically on whether individuals use a site's privacy settings (e.g., Boyd & Hargittai, 2010; Lewis, Kaufman, & Christakis, 2008; Madejski, Johnson, & Bellovin, 2011), which can be very important in the privacy management process. However, there are other maintenance and pruning technological strategies users can engage in as well that have been neglected in past studies. These include redaction strategies (Papacharissi & Gibson, 2011), like removing previously presented tags and posts from one's profile or editing one's contact list to alter one's audience. Some may even argue that the pruning strategies that allow users to have more control over the content others contribute to their social network site profiles may be particularly relevant since the content

E-mail address: eden.litt@u.northwestern.edu

0747-5632/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.chb.2013.01.049

others post may be given more prominence when it comes to impression formation (Walther & Parks, 2002; Walther, Van Der Heide, Hamel, & Shulman, 2009). The goal of this paper is to understand these privacy protection behaviors more holistically by looking at a more comprehensive and diverse set of technological privacy behaviors. Grounded in traditional communication theories on privacy behaviors (Altman, 1975; Petronio, 2002) and informed by literature on digital inequality, this study analyzes how people's demographic characteristics, motivations, and social network site experiences impact their use of privacy technology on social network sites. Using a large and diverse sample of social network site users, the results identify another form of digital inequality taking place online in which certain groups of users are more likely to take advantage of privacy tools to protect their personal information than others. The use of privacy tools on social network sites is not randomly distributed among users. Instead factors such as the users' backgrounds (e.g., gender and age), as well as their privacy motivations (e.g., concerns and turbulence), and experiences with social network sites may be indicative of who is more likely to take advantage of the technology to protect their privacy.

2. Research on privacy management

Traditional theories exploring privacy management have theorized many aspects related to how and why people manage their personal information in interpersonal and face-to-face contexts (Altman, 1975; Petronio, 2002). According to such theories, individuals desire "selective control of access to the self" (Altman, 1975, p. 24), so they create imagined or metaphorical boundaries, or barriers, around their information (Petronio, 2002). The boundaries help establish how well protected the information is and who has access, or co-owns, the information. To help signal such boundaries, people use verbal and non-verbal strategies, referred to as privacy markers (Petronio, 2002). For instance, in face-to-face contexts a person might whisper or shut the room's door to indicate that the forthcoming information should be kept private and contained within certain bounds.

Managing privacy boundaries requires a dynamic and dialectical process of rulemaking, negotiating, and coordinating as people take into account both the benefits and risks that come from sharing information (Petronio, 2002). Such processes do not always go seamlessly though. When information disseminates beyond a person's desired or perceived boundaries because of misunderstood rules or intentional betrayal, turbulence results (Petronio, 2002). Turbulent experiences are often accompanied with "minor flare-ups, confusion, misunderstandings, mistakes, embarrassments, and full-fledged uproars" (Petronio, 2002, p. 177). Although these privacy management theories focus on the development and coordination of private information between people in face-to-face contexts, they have more recently been applied to online environments including blogs (Child, Pearson, & Petronio, 2009) and electronic commerce sites (Metzger, 2007). Communication Privacy Management theory has also been applied to the social network site environment to look at university students' disclosure practices on Facebook (Waters & Ackerman, 2011), and has been identified as "the most valuable privacy theory for understanding interpersonal computer-mediated communication" (Margulis, 2011, p.12).

This research uses Communication Privacy Management theory as a framework to understand how people are using social network site technology to help maintain their overall privacy boundaries. Rather than create metaphorical boundaries like people do during everyday communication in face-to-face contexts, people can use a site's technological tools, or "markers" in Petronio's terms, to help technologically enforce their boundaries. For example, if a user removes an individual from his or her contact list, the site creates a virtual boundary between the two people so that these individuals no longer have access to each other's information. Communication Privacy Management theory serves as a useful framework to begin considering what influences people to impose technological boundaries on social network sites by first considering what influences people's privacy boundaries more generally. Below, I review what the theory and more traditional literature states, and, where applicable, I discuss what research on social network sites explicitly finds.

2.1. Traditional privacy criteria as predictors of privacy management

2.1.1. Gender

Communication Privacy Management theory suggests that because of differing socialization processes and cultural expectations, men and women vary in how they delineate their boundaries and how they understand privacy and disclosure practices (Petronio, 2002). While some more traditional communication research suggests that women tend to disclose more than men (see Dindia and Allen (1992) for a meta-analysis), many factors, such as status and context, influence these gender dynamics (e.g., Brooks, 1974; West, 1970). Research on social network sites specifically has found associations between gender and disclosure (Hoy & Milne, 2010; Tufekci, 2008; Waters & Ackerman, 2011). For example, one study found that college women were less likely to reveal their phone numbers online, but more likely to reveal their movie and book preferences than college-aged men (Tufekci, 2008). Although an earlier study on marketing and advertising found that females engaged in fewer privacy protection behaviors online (Sheehan, 1999), more recent research focused on social network site use found that women were more likely to set their profiles' privacy settings to "private" on both Facebook (Lewis et al., 2008; Stutzman & Kramer-Duffield, 2010) and MySpace (Thelwall, 2008). Hoy and Milne's (2010) study, focused specifically on gender, also found that females were more likely to monitor their Facebook privacy settings, untag photos, selectively friend, and use Facebook's "Friend lists" feature than males. Similarly, in a study on college students' use of Facebook privacy settings, Boyd and Hargittai (2010) found that women were more likely to adjust their privacy settings and tended to do so more often than men. While Communication Privacy Management theory suggests a relationship between gender and privacy rules, it does not predict how gender might relate to one's use of technological privacy tools. To understand this relationship better while simultaneously taking into account other criteria influencing privacy behaviors, this article proposes the following research question:

RQ1: What is the relationship between gender and technological privacy tool use on social network sites?

2.1.2. Age

As people age, their metaphorical privacy boundaries expand and contract throughout various life stages (Petronio, 2002). Children start off managing small amounts of information with highly permeable boundaries so that information can flow between family members. Then for adolescents, and next adults, boundaries expand with information as people develop new relationships and take on more life responsibilities. However, the boundaries begin to contract for the elderly, as they have to balance privacy desires with other health and safety concerns. Currently, a majority of the literature on privacy management and social network sites focuses on university students (e.g., Boyd & Hargittai, 2010; Lewis et al., 2008; Young & Quan-Haase, 2009), making age comparisons difficult. While popular media portray young adults as apathetic to privacy online, studies that have included multiple age groups find that teens and young adults may actually be stricter in their general privacy behaviors online than older adults (Caverlee & Webb, 2008; Park, 2011). While Communication Privacy Management theory might predict that middle-aged adults would engage the most privacy behaviors because they have to manage the most information and relationships, there seems to be conflicting evidence on how younger and older adults manage privacy online. Thus, this article explores the following research question:

RQ2: What is the relationship between age and technological privacy tool use on social network sites?

2.1.3. Privacy concerns

Privacy concerns, or the worries and concerns people have about the accessibility and control of their personal information, are influenced by culture and norms, and can impact people's privacy behaviors and boundaries (Petronio, 2002). Communication Privacy Management theory predicts that individuals who have more privacy concerns will engage in stricter rules and boundaries. Although some empirical research on online disclosures supports this (Young & Quan-Haase, 2009), other research finds no significant connections between privacy concerns and disclosure practices online (Acquisti & Gross, 2006; Metzger, 2007; Tufekci, 2008). For example, a study on Facebook adoption found that people's privacy attitudes played a role in who initially signed up for the service, but among Facebook members such concerns had no impact on how much information users revealed (Acquisti & Gross, 2006). However, the aforementioned studies looked at whether information had been disclosed or not, rather than which strategies people use to protect their already released information. It is possible that privacy concerns may be more likely to prompt users to employ the technology to help protect their already-released information. Thus, the following hypothesis is proposed:

H1. Individuals with online privacy concerns will be more likely to use more technological privacy tools than individuals without privacy-related concerns.

2.1.4. Turbulence

When privacy turbulence, or an incoordination of boundaries, occurs and information leaks beyond one's desired boundaries, Communication Privacy Management theory predicts that the person will be motivated to adjust or change boundaries. Through qualitative in-depth interviews, Debatin, Lovejoy, Horn, and Hughes (2009) found that a person who experienced a "privacy invasion" on Facebook (such as public humiliation from another member) was more likely to adjust his or her privacy settings than someone who had only heard about such occurrences, but had not experienced them personally. Other qualitative research has exposed similar relationships in which turbulent experiences have led individuals to reconsider their disclosure habits and increase their privacy settings strategies (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011; Strater & Lipford, 2008). Relying on survey data of a larger sample, this article tests the following hypothesis:

H2. Users who have had an online turbulent experience will use more technological privacy tools on social network sites than those who have not had such an experience.

2.2. Social network site experiences as potential predictors of privacy management criteria

While Communication Privacy Management theory offers a conceptual framework for studying the processes underlying privacy management on social network sites, it does not address a potential relationship that may exist between the individual and the technology that is facilitating the privacy management. However, digital inequality research consistently shows that people vary in how they use Internet services based not only on background factors like race and socioeconomic status, but also on online experiences and Internet skills (Hargittai, 2010). For example, scholars have found that individuals with higher Internet skills are more likely to share content online (Correa, 2010; Hargittai & Walejko, 2008) and adopt newer social media services (Hargittai & Litt, 2011).

Networked environments, like social network sites, afford characteristics that are different from what everyday individuals experience during privacy management in face-to-face settings. More explicitly, privacy management online is complex not only because users rely heavily on their imagination to navigate environments in which their audiences are invisible and hard to discern due to limited nonverbal cues, but also because of the potential for asynchronous communication, the persistence of one's information, and the ability to replicate and share digital information easily (Boyd, 2007; Litt, 2012; Walther, 1996). This complexity is further compounded by the fact that many social network site users are interacting with larger audiences that "collapse" or merge social groups and contexts that were once physically distinct in the offline realm (Boyd, 2010). Users not only have to manage the boundaries of their information socially through decisions on what to disclose, but they also have to manage their technological boundaries successfully to make sure the system does not over- or underexpose their personal information beyond their desired boundaries (Altman, 1975). To negotiate all of this, a user must know not only what tools exist, but also have the experience and skills to utilize them.

Although limited research in the area exists, several studies suggest that there may be a connection between people's technological strategies and their experiences with the mediating technology (Boyd & Hargittai, 2010; Lewis et al., 2008; Yao & Linz, 2008). For example, a survey on young adults' Internet uses found a positive association between Facebook privacy settings changes and Facebook use frequency and Internet skill (Boyd & Hargittai, 2010). Lewis et al. (2008) also found that students who used Facebook more frequently were more likely to adjust their profiles' visibility to private. In one of the most well-developed studies on online privacy management as it relates to protecting oneself from institutional surveillance, Park (2011) found that one's technical familiarity and online experience, in terms of years of usage and daily Internet use, impacted individuals' privacy strategies. Based on past digital inequality literature, this article proposes the following hypothesis:

H3. Individuals with more social network site experiences will engage with more technological privacy tools on social network sites than those with fewer experiences.

3. Method

The analyses in this paper are based on Pew Internet's "Reputation Management and Social Media" data set (Madden & Smith, 2010). These data are from cell phone and landline interviews conducted during August and September of 2009 using random digit dialing. The original sample consisted of 2253 adults age 18 and older, and surveyed both Internet users and non-users. The response rate for the surveys conducted via landline was 19% and 16% for the sample of cell phone users. Since the focus of this study is on social network site users, the data used in this paper are restricted to those who reported that they had created their own profile on a social network site. The question wording was "Have you ever created your own profile online that others can see on any social networking site like MySpace, Facebook or LinkedIn?" Individuals with missing response items were not included in the descriptive statistics or analyses. The final sample size consisted of 490 social network site users. To help control for the wide variety of social network sites and variation in privacy tool availability, I verified all participants used at least MySpace and/or Facebook, which both have all the privacy features looked at in this study. For more details on the overall sampling method, see Madden and Smith (2010). Since these data are cross-sectional no causal claims can be made. Further, like any self-report data, when interpreting the analysis of these data, researchers must keep in mind social desirability and validity concerns as people's self-reported behaviors may not always reflect their actual behaviors. Future work will need to explore this more thoroughly.

3.1. Measures for traditional privacy management criteria

3.1.1. Background factors

The interviewer asked respondents typical demographic questions related to race and ethnicity, gender, age, and income. Education, race and ethnicity, and income were included in the regression analyses since these factors have often been associated with Internet and social network site use (Bonfadelli, 2002; Hargittai, 2007, 2010; van Deursen & van Dijk, 2011). First participants were asked if they consider themselves to be "Hispanic or Latino origin or descent, such as Mexican, Puerto Rican, Cuban, or some other Latin American background," then they were asked about their race. These two questions were combined to create the following mutually exclusive categories: Hispanic; White, non-Hispanic; Black or African–American, non-Hispanic; Asian or Pacific Islander, non-Hispanic; Native American/American Indian, non-Hispanic; and mixed race, non-Hispanic. The majority of the restricted sample identified as non-Hispanic, White (79%). There were no individuals who identified as Native American/American Indian, non-Hispanic or mixed race, non-Hispanic. There were slightly more females (56%) than males (44%). Participants ranged in age from 18 to 76 years old (see Table 1 for more details). For household income, the instrument asked participants to pick from several categories ranging from less than $10,000 per year to more than $150,000. The midpoints were taken from each category and the variable was treated as continuous in the regression models (the midpoint for the lowest category was $5000 and $175,000 for those who fell in the highest category).

Table 1
Participant background.

	Percent	*N*
Women	55.71	273
Men	44.29	217
Age	36.62 (13.46)[a]	490
Race and ethnicity		
White, non-Hispanic	78.98	387
Black or African–American, non-Hispanic	9.18	45
Asian or Pacific Islander, non-Hispanic	2.45	12
Hispanic	9.39	46
Education		
Less than high school degree	4.29	21
High school degree	25.10	123
Some college	30.41	149
College graduate	25.71	126
Advanced degree	14.49	71
Household income	66, 683.67 (45, 585.51)[a]	490

[a] Reporting mean and standard deviation.

3.1.2. Privacy concerns

To measure attitudinal concerns related to online privacy, participants were asked, "Do you ever worry about how much information is available about YOU on the Internet, or is that not something you really worry about?" and then they chose between two response items indicating that either they worry about it or they do not. Roughly a third of the participants expressed having concerns about their information online.

3.1.3. Online turbulence

To inquire about turbulent experiences, the survey asked participants a yes-or-no question about whether they had ever had any bad or embarrassing situations occur because of online information posted about them or if they had ever posted content online that they later regretted sharing. If participants responded yes to either of these questions, then they were considered in the analyses as having experienced turbulence. The majority of participants had not experienced turbulence online (85%).

3.2. Measures for social network site experiences

Two variables were used to investigate social network site experiences: (1) the frequency with which one uses social network sites and (2) the number of social network sites one uses. Pew measured the former by asking participants "how often" they visited the site they use most frequently and participants chose between the following response items: "several times a day," "about once a day," "every few days," "once a week," or "less often." To measure the number of sites one uses, Pew asked, "How many social networking web sites do you currently have a profile on?" Users could then pick from "one," "two," "three," or "four or more." Due to the small proportion of individuals in the latter categories, the variable was recoded as binary with people using either one or two or more sites. When it comes to participants' social network site use, more than 45% used such services at least once a day, but still more than a fifth used them less than once a week (see Table 2).

3.3. Technological privacy tools measure

While most privacy-related studies have focused on individuals' use of privacy settings (e.g., Boyd & Hargittai, 2010; Lewis et al., 2008; Waters & Ackerman, 2011), the following analysis takes on a more expansive and diverse understanding of technological privacy tools. This variable is composed of an index that sums the number of technological privacy tools an individual reported using. This index is composed of responses (yes = 1, no = 0) to a set of five questions that asked participants if on social network sites they ever: (1) change their privacy settings; (2) delete people from network/friends lists; (3) untag photos; (4) limit certain updates to certain people; and (5) delete others' comments from their profile. The index ranged from 0 to 5 and had a Cronbach's alpha of 0.72

Table 2
Communication privacy management motivators and social network site experiences.

	Percent	*N*
Expressed privacy concern	32.04	157
Experienced turbulence online	14.69	72
Social network site frequency		
Less often than once a week	21.63	106
Once a week	12.04	59
Every few days	19.80	97
Once a day	22.65	111
Several times a day	23.88	117
Uses two or more social network sites	53.27	261

Table 3
Technological privacy tools.

	Percent	*N*
Number of technological privacy tools used	2.46 (1.63)[a]	490
Popularity of individual privacy tools		
Changed the privacy settings for one's profile to limit what's shared	65.31	320
Deleted people from one's network or friends' list	58.57	287
Kept some people from seeing certain updates	52.86	259
Deleted comments that others have made on one's profile	33.88	166
Removed one's name from photos that have been tagged	30.00	147

[a] Reporting mean and standard deviation.

(see Table 3 for the breakdown of privacy tool types by popularity). Participants averaged using a little less than two and a half of these tools. More than 16% of the sample did not use any technological strategy. Roughly 16% used one, 21% used two, 19% used three, 14% used four, and roughly 14% used all five privacy tools. The most common strategy used among the sample was adjusting one's privacy settings (65%), while the least was removing or untagging photos (30%).

4. Results

4.1. Explaining privacy tool usage

4.1.1. Background factors

In order to understand how background factors, privacy motivators, and social network site experiences relate to the diversity of people's technological privacy strategies, three linear regression models were run (see Table 4). To help establish a baseline and address questions related to privacy and background factors, Model 1 includes only the demographic variables age, gender, education, race, and household income. Model 2 then incorporates the factors that Communication Privacy Management theory hypothesizes will impact people's privacy decisions adding privacy concerns and turbulence experience to the baseline. Lastly, Model 3 combines factors that Communication Privacy Management theory suggests impact privacy behaviors with those that digital inequality literature also find relevant by looking at how experiences with the mediating technology relate to the way people manage their privacy on social network sites while controlling for people's background factors and motivations. Variance inflation factors were calculated and no indication of multicollinearity was detected in any model.

RQ1 asked about the relationship between gender and technological privacy tool usage. The negative gender coefficient from Models 1, 2, and 3 (in Table 4), suggests that males engaged with a less diverse set of technological privacy tools than females. Even when privacy concerns and social network site experiences are included in Models 2 and 3, the relationship between gender and privacy tool use remains.

Looking across all three models, the negative coefficient for the age variable provides evidence of a negative linear relationship between age and technological privacy tool use. This suggests that in response to RQ2, older individuals were less likely to use technological strategies than younger individuals. Even when potentially mediating variables between age and privacy tool use are included in the models, such as one's social network site use and privacy concerns (see Models 2 and 3), the systematic age difference remains. However, beyond age and gender, there were no significant differences in privacy tool use based on the demographics education, income, or race and ethnicity in any of the models. It is possible that part of the effect for race and ethnicity may be due to the small sample size, since the majority of the sample was White (roughly 79%).

4.1.2. Motivational predictors

H1 hypothesized that people with privacy concerns related to information online would engage with more technological privacy

Table 4
Technological privacy tool use as a function of background, motivations, and social network site experiences (standard errors).

	Model 1 (*N* = 490)	Model 2 (*N* = 490)	Model 3 (*N* = 490)
Age	−0.038 (0.0056)***	−0.032 (0.0054)***	−0.029 (0.0055)***
Male	−0.38 (0.15)**	−0.39 (0.14)**	−0.39 (0.14)**
Race (White omitted)			
Black, non-Hispanic	−0.27 (0.25)	−0.18 (0.24)	−0.22 (0.24)
Asian, non-Hispanic	0.72 (0.46)	0.63 (0.44)	0.61 (0.45)
Hispanic	0.43 (0.25)	0.30 (0.24)	0.25 (0.24)
Education (Advanced degree omitted)			
Less than high school degree	−0.15 (0.41)	0.0040 (0.39)	−0.0088 (0.39)
High school degree	−0.19 (0.24)	−0.20 (0.23)	−0.20 (0.23)
Some college	−0.27 (0.23)	−0.25 (0.23)	−0.21 (0.22)
College graduate	0.011 (0.23)	−0.032 (0.22)	−0.074 (0.23)
Household income	0 (0)	0 (0)	0(0)
Motivational predictors			
Privacy concern		0.38 (0.15)*	0.39 (0.15)**
Online turbulence		1.15 (0.20)***	1.06 (0.20)***
Social network site frequency (Less than weekly omitted)			
Once a week			0.14 (0.25)
Every few days			0.28 (0.21)
Once a day			0.33 (0.21)
Several times a day			0.50 (0.21)*
Uses more than one social network site			0.29 (0.14)*
Constant	3.93 (0.34)***	3.45 (0.34)***	2.94 (0.37)***
R^2	0.11	0.19	0.21

* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

tools than those who do not report such concerns. Models 2 and 3 provide support for H1 while controlling for demographics and social network site experiences. Model 3 suggests that social network site experiences do not impact the relationship of privacy concerns and privacy tools use as this relationship remained significant even in the third model. There is also support for H2 in Models 2 and 3 indicating that those users who have had turbulent experiences use more technological privacy tools than those who have not experienced such regret or negativity online. As judged by the *r*-squared measure, including privacy concerns and online turbulence into the model greatly improves the models fit (from $r^2 = 0.11$ to $r^2 = 0.19$).

4.1.3. Social network site experiences

Finally, Model 3 focuses on technological privacy tool use with the addition of social network site experience variables. The findings suggest some support for H3. While controlling for motivational and background factors, those who use social network sites the most often in comparison to those who use them the least often, engage with more technological privacy tools. The general trend is that as users' social network site frequency increases so does the diversity of their privacy tool use; however, the only significant difference is between those who use social network sites several times a day and those who use them less often than once a week. Furthering the evidence that there may be a relationship between experience with the social network site medium and use of privacy tools is the finding that individuals who use more than one social network site in comparison to those who only use one seem to engage with more privacy tools overall (see Model 3).

5. Discussion

The goal of this paper was to investigate what factors relate to people's use of privacy tools on social network sites. Overall, we see that such protection strategies are not randomly distributed throughout the population, but certain groups of people are more likely to engage such strategies than others. More specifically, we see evidence that people's background, motivations, and social network site experiences are related to the diversity of their privacy management strategies in monitoring their reputation online.

Consistent with Communication Privacy Management theory, the results indicate gender is related to privacy and reputation management on social network sites as well. While some studies on online privacy find no relationship between gender and boundary formation (e.g., Metzger, 2007), similar to other studies that focused strictly on privacy settings use among university students (Lewis et al., 2008; Stutzman & Kramer-Duffield, 2010; Thelwall, 2008), these results suggest that females among all age groups are more likely to use a more diverse set of technological privacy tools than males. The Social Web Gendered Privacy Model suggests that because women have more general (offline) privacy concerns related to safety (e.g., stalking and harassment), they transfer their protective practices into the social network site realm as well (Thelwall, 2011). Relatedly, popular rhetoric, moral panics, and public messaging about potential social network site dangers (e.g., predation and cyberbullying) were originally targeted at women (Cassell & Cramer, 2007). Boyd and Hargittai (2010) hypothesized that this might also explain why females were so engaged with adjusting the privacy settings of their Facebook accounts in their study. Interestingly however, the relationship between gender and privacy tool use seems to go beyond one's worry or concern for privacy, as such gender effects remained significant even while controlling for privacy concerns (see Models 2 and 3 in Table 4). This expresses the importance of researchers carefully outlining their conceptualization and operationalization of variables related to privacy concerns. For example, in this study, privacy concerns referred to one's worries about having information available on the Internet. It is possible that variables measuring privacy concerns more generally or concerns related specifically to social network sites would reflect a different outcome or one in which such concerns mediated the relationship between gender and tool use.

Future studies will need to investigate the construct of privacy concerns more thoroughly, and perhaps in a more nuanced fashion, as the overall findings on its relationship with privacy-related behaviors are mixed. The results in this report suggest that individuals who are concerned about their personal information online are more likely to take action to protect this information. It is worth noting though that other work (e.g., Patil & Kobsa, 2010) has found that individuals with lower privacy concerns also tend to have lower understandings of the technology itself. So, it is possible that some users are not as concerned as they should be because they are not aware of their susceptibility and the potential dangers of disclosing information in these spaces. This may also explain why some individuals have learned this the hard way through turbulent experiences, such as those in this study who had regretful or bad experiences online. These individuals were more likely to be concerned about their personal information and more likely to engage in more technological privacy strategies. While the causal relationship from this study is not known, evidence from others' interviews indicates that such negative events triggered the protective behaviors (Ellison et al., 2011; Strater & Lipford, 2008). For example, Strater and Lipford (2008) reported that some participants modified their Facebook privacy settings after they received a phone call or text message from a stranger. Similarly, a female participant in Young and Quan-Haase's (2009) study reported a negative experience related to a tagged photo on Facebook and stated that now she is more likely to untag photos or ask others to remove tagged photos to prevent future turbulent experiences. The results from this study complement the aforementioned results by demonstrating the relationship between turbulence and privacy behaviors on a larger and more diverse sample.

Even while controlling for a variety of factors, the results suggest an age divide persists in which younger adults are more likely to engage in a wider use of technological privacy tools than older adults. While Communication Privacy Management theory suggests a relationship between age and privacy behaviors, it provides no explanation for why this negative relationship might exist. Although some studies have found older adults engage in other social privacy strategies not measured in this study, such as using nicknames while posting on public sites (see Maaß (2011) for more), most studies have not included a wide enough age range to determine people's privacy protection strategies in comparison to one another. While these data allow a closer examination of the age and privacy-tool relationship, future studies will need to investigate other mediating and intervening relationships that help better understand why such age inequalities persist.

For example, potential influential factors could be users' knowledge and awareness of privacy tools, as well as their skill in using the mediating technology itself. While in face-to-face contexts, the accessibility of one's personal information is not mediated by technology, in networked environments it is. While no measures of tool awareness or skill were captured in this data set, the results in this paper begin to support a relationship between the individual and the mediating technology. Regardless of other motivating factors like privacy concerns or turbulent experiences, the frequency with which people use social network sites impacts how they manage their privacy online. Individuals who use social network sites more often may be at an advantage because they have more time to experiment and gain familiarity with the site and its affordances. For example, young adult Facebook users who spend more time on the site also have higher levels of confidence in using Facebook's privacy settings (Boyd & Hargittai, 2010). It may also be that individuals who use social network sites more often are also disclosing more information so they have more information to protect, and thus engage in a wider array of privacy practices. More use of social network sites may also lead to more exposure of other users engaging in such strategies. It may also lead to a hyperawareness of one's own self-presentation as one judges others' self-presentations. While age remained significant even when controlling for social network site experiences, its effects did diminish a little, suggesting that part of the variation in age may be due to related factors. There are likely better measures though to capture this. Future research will need to investigate concretely the relationship between these privacy inequalities and other kinds of social network site experiences including social media skills, privacy tool awareness, and self-efficacy in using such tools.

6. Conclusion

The findings of this study demonstrate that criteria that have traditionally influenced privacy management in face-to-face contexts, like age, gender, and motivation, also relate to the technological privacy boundaries people create in networked environments, like social network sites. However, the findings also extend traditional theories like Communication Privacy Management theory, by suggesting that when communicating through mediated environments, overall boundary regulation is also related to one's experience and relationship with the mediating technology itself. Another major contribution of these findings is evidence of a continuing second-level digital divide (e.g., Hargittai & Walejko, 2008; Park, 2011) related to privacy on social network sites. Such privacy inequality based systematically on age, gender, and medium experiences are particularly disconcerting as online self-presentations are increasingly playing an important role in impression formation and offline reputation and life chances. In spaces where we are managing our information with larger and more diverse audiences than we are used to in face-to-face interactions (Boyd, 2010), those not taking advantage of the technological tools indicate whose data and reputation may be most vulnerable to unintentional disclosure and turbulence. However, it is worth pointing out that this may be an area in which most users could use training. Even when considering the whole sample, more than a third engaged with none or only one of these technological tools. The most common strategy, changing one's privacy settings, was used by less than two-thirds of the sample. The findings from this study also showcase the importance of expanding our understanding of privacy management beyond privacy settings use by studying other ways individuals try to manage access to their personal information on social network sites. Future work will need to continue in this direction by exploring use of additional privacy tools as well as social strategies people are also implementing.

While this study demonstrates several factors related to technological privacy boundaries, future research will need to investigate more closely why and how such inequalities persist by exploring additional technological, social, and psychological factors like Internet or social media skills (Boyd & Hargittai, 2010; Litt, 2012), audience size (e.g., Ellison et al., 2011; Lewis et al., 2008; Madejski et al., 2011), and social skills, like one's self-monitoring ability (Child & Agyeman-Budu, 2010) as well as incorporating more nuanced measures related to privacy concerns, turbulence, and medium experience. With the ever-evolving social media sphere, more work is needed to help account for the many changes that have occurred on the social network site services themselves and among the users. For example, older adults' social network site use continues to rise. Currently, 43% of older adults use social network sites daily up from 27% in 2009 (Madden & Zickuhr, 2011). More new users and added complexities to the social network site technologies, however, may mean an even greater number of less experienced individuals, and thus the results from this study may be conservative.

Future research in this area will not only provide scholars with insight into who is benefitting from such actions and why, but it will also provide information to social network services and policymakers to create tools that are more user-friendly and policies that are more relevant in helping people protect their information and reputations. Since "the burden of online privacy protection is primarily shouldered by an individual's own conscious effort" (Yao, 2011, p. 112), engaging with the social network site's privacy features is becoming an imperative literacy for users. Thus, we need to do a better job of training individuals to personalize their privacy management strategies so that they can make informed decisions about sharing their information in desired ways. Users should not have to experience turbulence to realize they need to adjust their practices. They should learn how to use these tools to reap the benefits from *selectively* sharing content on social network sites, while at the same time minimizing the potential damage and harm to their reputations and relationships that may result from unintentional disclosures.

Acknowledgements

The author gratefully acknowledges the feedback and insight from Professor Eszter Hargittai, Professor James S. Ettema, Professor Lincoln Quillian, and an anonymous reviewer.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Paper presented at the proceedings of privacy enhancing technologies workshop (PET)*, Cambridge, UK.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole Publishing Company.

Bonfadelli, H. (2002). The Internet and knowledge gaps: A theoretical and empirical investigation. *European Journal of Communication, 17*, 65–84. http://dx.doi.org/10.1177/0267323102017001607.

Boyd, D. (2010). *Social network sites as networked publics: Affordances, dynamics, and implications*. London: Routledge.

Boyd, D. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media* (pp. 119–142). Cambridge, MA: MIT Press.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8).

Brooks, L. (1974). Interactive effects of sex and status on self-disclosure. *Journal of Counseling Psychology, 21*(6), 469–474. http://dx.doi.org/10.1037/h0037288.

Cassell, J., & Cramer, M. (2007). High tech or high risk: Moral panics about girls online. In T. McPherson (Ed.), *Digital young, innovation, and the unexpected* (pp. 53–75). Cambridge, MA: MIT Press.

Caverlee, J., & Webb, S. (2008). A large-scale study of MySpace: Observations and implications for online social networks. *Paper presented at the proceedings from the 2nd international conference on weblogs and social media*, Seattle, WA.

Child, J. T., & Agyeman-Budu, E. A. (2010). Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior, 26*(5), 957–963. http://dx.doi.org/10.1016/j.chb.2010.02.009.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology, 60*(10), 2079–2094. http://dx.doi.org/10.1002/asi.21122.

Clark, L. A., & Roberts, S. J. (2010). Employer's use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics, 95*(4), 507–525. http://dx.doi.org/10.1007/s10551-010-0436-y.

Correa, T. (2010). The participation divide among "online experts": Experience, skills and psychological factors as predictors of college students' web content creation. *Journal of Computer-Mediated Communication, 16*, 71–92. http://dx.doi.org/10.1111/j.1083-6101.2010.01532.x.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of*

Computer-Mediated Communication, 15(1), 83–108Springer. http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x.

Dindia, K., & Allen, M. (1992). Sex differences in self-disclosure: A meta-analysis. *Psychological Bulletin, 112*(1), 106–124. http://dx.doi.org/10.1037/0033-2909.112.1.106.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 19–32). Heidelberg and New York: Springer.

Hancock, J. T., & Dunham, P. J. (2001). Impression formation in computer-mediated communication revisited: An analysis of the breadth and intensity of impressions. *Communication Research, 28*(3), 325–347. http://dx.doi.org/10.1177/009365001028003004.

Hargittai, E. (2007). Whose space? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication, 13*(1). http://dx.doi.org/10.1111/j.1083-6101.2007.00396.x.

Hargittai, E. (2010). Digital na(t)ives? Variation in Internet skills and uses among members of the ''Net Generation''. *Sociological Inquiry, 80*(1), 92–113. http://dx.doi.org/10.1111/j.1475-682X.2009.00317.x.

Hargittai, E., & Walejko, G. (2008). The participation divide: Content creation and sharing in the digital age. *Information, Communication & Society, 11*(2), 239–256. http://dx.doi.org/10.1080/13691180801946150.

Hargittai, E., & Litt, E. (2011) The tweet smell of celebrity success: Explaining variation in Twitter adoption among a diverse group of young adults. *New Media & Society, 13*(5), 824–842. http://dx.doi.org/10.1177/1461444811405805.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 22–45.

Jobvite (2012). *The jobvite social recruiting survey 2012*.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*, 79–100. http://dx.doi.org/10.1111/j.1083-6101.2008.01432.x.

Litt, E. (2012). Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media, 56*(3), 330–345. http://dx.doi.org/10.1080/08838151.2012.705195.

Maaß, W. (2011). The elderly and the Internet: How senior citizens deal with online privacy. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 235–250). Heidelberg and New York: Springer.

Madden, M., & Smith, A. (2010). *Reputation management and social media: How people monitor their identity and search for others online*. Washington, DC: Pew Internet & American Life Project.

Madden, M., & Zickuhr, K. (2011). *65% Of online adults use social networking sites*. Washington, DC: Pew Internet & American Life Project.

Madejski, M., Johnson, M., & Bellovin, S. (2011). *The failure of online social network privacy settings (D.o.C. Science, Trans.) Technical report CUCS-010-11*. Columbia University.

Margulis, S. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 9–17). Heidelberg and New York: Springer.

Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. (2010). *Youth, privacy and reputation (literature review)*. Berkman Center Research Publication: Berkman Center for Internet & Society.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335–361. http://dx.doi.org/10.1111/j.1083-6101.2007.00328.x.

Microsoft (2010). *Research shows online reputations matter*. <http://www.microsoft.com/privacy/dpd/research.aspx>.

Paine Schofield, C. B., & Joinson, A. N. (2008). Privacy, trust, and disclosure online. In A. Barak (Ed.), *Psychological aspects of cyberspace: Theory, research, applications* (pp. 13–31). Cambridge, UK: Cambridge University Press.

Papacharissi, Z., & Gibson, P. L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75–90). Heidelberg and New York: Springer.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*. http://dx.doi.org/10.1177/0093650211418338.

Patil, S., & Kobsa, A. (2010). Enhancing privacy management support in instant messaging. *Interacting with Computers, 22*(3), 206–217. http://dx.doi.org/10.1016/j.intcom.2009.10.002.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Preston, J. (2011). *Social media history becomes a new job hurdle*. <http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?pagewanted=all>.

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13*(4), 24–38. http://dx.doi.org/10.1002/1520-6653.

Stelter, B. (2012). *CNN suspends Roland Martin for remarks on Twitter*. <http://mediadecoder.blogs.nytimes.com/2012/02/08/cnn-suspends-roland-martin-for-remarks-on-twitter/?emc=eta1>.

Strater, K., & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *Paper presented at the BCS-HCI '08 proceedings of the 22nd British HCI group annual conference on people and computers: Culture, creativity, interaction*, Swinton, UK.

Stutzman, F., & Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in Facebook. *Paper presented at the CHI 2010*, Atlanta, GA.

Thelwall, M. (2008). Social networks, gender, and friending: An analysis of MySpace member profiles. *Journal of the American Society for Information Science and Technology, 59*(8), 1321–1330. http://dx.doi.org/10.1002/asi.20835.

Thelwall, M. (2011). Privacy and gender in the social web. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 251–266). Heidelberg and New York: Springer.

Tong, S. T., Van Der Heide, B., Langwell, L., & Walther, J. B. (2008). Too much of a good thing? The relationship between number of friends and interpersonal impressions on Facebook. *Journal of Computer-Mediated Communication, 13*(3), 531–549. http://dx.doi.org/10.1111/j.1083-6101.2008.00409.x.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36. http://dx.doi.org/10.1177/0270467607311484.

Van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2011). Internet skills and the digital divide. *New Media & Society, 13*(6), 893–911. http://dx.doi.org/10.1177/1461444810386774.

Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research, 23*(3). http://dx.doi.org/10.1177/009365096023001001.

Walther, J. B., & Parks, M. (2002). Cues filtered out, cues filtered in: Computer mediated communication and relationships. In M. L. Knapp, J. A. Daly, & G. R. Miller (Eds.), *The handbook of interpersonal communication* (3rd ed., pp. 529–563). Thousand Oaks, CA: Sage.

Walther, J. B., Van Der Heide, B., Hamel, L., & Shulman, H. (2009). Self-generated versus other-generated statements and impressions in computer-mediated communication: A test of warranting theory using Facebook. *Communication Research, 36*(2), 229–253. http://dx.doi.org/10.1177/0093650208330251.

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*(1), 101–115. http://dx.doi.org/10.1111/j.1083-6101.2011.01559.x.

West, L. W. (1970). Sex differences in the exercise of circumspection in self-disclosure among adolescents. *Psychological Reports, 26*(1), 226. http://dx.doi.org/10.2466/pr0.1970.26.1.226.

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior, 11*(5), 615–617. http://dx.doi.org/10.1089/cpb.2007.0208.

Yao, M. Z. (2011). Self-protection of online privacy: A behavioral approach. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 111–126). Heidelberg and New York: Springer.

Young, A. L., & Quan-Haase, A. (2009). Information revelation and Internet privacy concerns on social network sites: A case study of Facebook. *Paper presented at the C&T 2009*, University Park, PA.