Article

SM+S
social media + society

Social Media + Society
July-December 2015: 1–11

DOI: 10.1177/2056305115612783
sms.sagepub.com
SAGE

Privacy Management on Facebook: Do Device Type and Location of Posting Matter?

Jennifer Jiyoung Suh[1] and Eszter Hargittai[2]

Abstract

People's information sharing on Facebook often happens through mobile devices allowing for posting from different locations. Despite the potential contextual differences in content sharing, the literature on online privacy management rarely takes into consideration the type of device and the type of location from which people post content. Do these aspects of Facebook use affect how people share information online? Analyzing Facebook posts young adults shared from different devices and different locations, this article examines the effectiveness of users' privacy management. By comparing the intended audience with the actual audience of each post, we find considerable mismatch between the two despite most participants expressing confidence in their ability to manage their information on the site. Posts that are accidentally shared with "public"—potentially anyone on the web—are more likely to be shared from non-mobile devices. Interview data reveal that this happens despite the fact that most participants consider non-mobile devices more reliable and convenient to use than mobile devices.

Keywords

privacy, sharing, Facebook, mobile devices, location, social media

Introduction

In the United States, the number of users of mobile devices that provide Internet access has been continuing to grow; as of early 2014, 55% of American adults owned a smartphone, and 42% of American adults owned a tablet computer (Pew Research Center, 2014). These users can engage in many online activities with their mobile devices, and one of the main activities for smartphone and tablet users is accessing social network sites (SNSs) (Keynote Competitive Research, 2012). Indeed, in 2013, 40% of cell phone owners accessed an SNS on their phones (Pew Research Internet Project, 2014). Despite considerable increase in the use of mobile devices for engaging in social media, little research has considered how device type and a user's location may influence people's posting behavior on such sites. It is this gap in the literature that this article addresses.

The largest SNS in the world, Facebook, announced in its 2015 financial report that the number of mobile monthly active users was 1.25 billion out of 1.44 billion total users or over 85% of the user base. As accessing and participating on SNSs have become much more widespread, increasing numbers of people are sharing personal information online using more than one device. Because the mobile Facebook app is integrated into thousands of other apps, it only takes a few clicks for users to upload a photo or share a link on their timelines. As a result, users have shared over 240 billion photos on Facebook, or an average of over 350 million photos per day (Bort, 2013). The number of total posts is far beyond the number of photo uploads. In 2013, users shared an average of 4.75 billion items daily, and this number had increased by 94% in less than 1 year (Constine, 2013).

Privacy issues are of potential concern when it comes to content sharing on SNSs because many employers are using job candidates' profiles before making employment decisions, and half of employers have reported passing up someone for a position due to content found on their online profiles

[1]University of California, Santa Barbara, USA
[2]Northwestern University, USA

Corresponding Author:
Jennifer Jiyoung Suh, Department of Communication, University of California, Santa Barbara, Social Sciences & Media Studies (SSMS), Santa Barbara, CA 93106, USA.
Email: suh@umail.ucsb.edu

(Grasz, 2014; Wortham, 2009). Others have documented the personal costs of privacy mismanagement (Tufekci, 2012). But as work has shown, young adults vary considerably in the extent to which they change their privacy settings, partly due to differences in their general Internet skills and privacy-specific online skills, or due to their past experience of online privacy violations (boyd & Hargittai, 2010; Hargittai & Litt, 2013; Litt, 2013).

With the rise in mobile device usage, people are sharing personal information on SNSs from multiple devices and locations with the potential to further confuse users about the privacy risks of their behaviors. To understand people's approaches to online privacy better, this article examines the factors that influence people's decision-making about sharing their information online from mobile compared to non-mobile devices and from home compared to other locations.

Facebook and Information Sharing

Facebook is the largest and most popular SNS in the world. In addition to offering its services at facebook.com, Facebook's users can interact with the site through the use of various mobile applications. After releasing "Facebook for iPhone" as their first mobile app in 2007, Facebook has gone on to provide several different kinds of mobile apps: Facebook for iPhone, Facebook for Android, Facebook Home, Facebook Messenger, Pages Manager for iOS, and Pages Manager for Android (Facebook, n.d.; Hewitt, 2007).

At the end of 2012, Facebook reported that users were sharing 150 billion "friend" connections in this online community based on "anchored relationships," defined as "offline-based online relationship" (Zhao, Grasmuck, & Martin, 2008, p. 1818). On Facebook, users' family, friends, neighbors, colleagues, and other acquaintances collectively become their "friends," as one of the primary uses of Facebook is to maintain and strengthen pre-existing relationships (boyd, 2008; Ellison, Steinfield, & Lampe, 2007; Vitak, 2012). As a result, people may feel more comfortable sharing information because they have a higher level of trust of their Facebook "friends," and sometimes, they may even feel pressure to share personal information because their "friends" are doing so (Acquisti & Gross, 2006; Gross & Acquisti, 2005; Taddicken, 2014).

Some researchers have compared Facebook to an iceberg because only a small part of user communication is above the surface and visible to users, while the rest is underwater and invisible (Debatin, Lovejoy, Horn, & Hughes, 2009). The visible part of Facebook includes fun social interactions among users, and the invisible part represents a network of personal data that could be mined for targeted marketing and advertising as well as other purposes (Stutzman, Gross, & Acquisti, 2012). While Facebook may seem like a safe space for social networking with pre-existing contacts, users cannot be in complete control of their information on Facebook because of all of the information about their networks invisible to them (Debatin, Lovejoy, Horn, & Hughes, 2009; Gross & Acquisti, 2005; Stutzman et al., 2012).

Perceived Importance of Privacy

While over a billion users share information each day on Facebook, research suggests that users do care about privacy and have become more aware of their public information disclosure on Facebook (boyd & Hargittai, 2010; boyd & Marwick, 2011; Marwick & boyd, 2014; Stutzman et al., 2012). A survey conducted after the revelation about the National Security Agency (NSA) tracking people's phone records also supports this result. Young people between the ages of 18 and 29 years were most likely to say that the government should not "intrude on personal privacy, even if that limits its ability to investigate possible terrorist threats" (Pew Research Center for the People & the Press, 2013, p. 5). Some teens take different structural and social strategies, such as blocking people or encoding their messages, to share information online and maintain a desired amount of privacy at the same time (boyd & Marwick, 2011).

Influence of Location and Type of Device

As the value of privacy may differ depending on social contexts and norms, a single definition may not be applicable in all cases (boyd & Marwick, 2011; Nissenbaum, 2011; Solove, 2007). People's sense of privacy may vary across different locations. Some researchers have suggested that the number of unique visitors influences people's sense of privacy about different locations. Toch and colleagues (2010) found that users feel more comfortable sharing their location when in higher entropy places, such as on campus or at work, and less comfortable about sharing location information when in lower entropy places. Using the unit of "location entropy" as a predictor of people's sense of privacy, people's perceived level of privacy will be lower in more public places, but higher in places with less unique visitors (e.g., home or friend's house) (Cranshaw, Toch, & Hong, 2010; Toch et al., 2010). Home can be expected to be the most private place for most people because it would usually have the lowest number of unique visitors.

However, location entropy may not account for everyone's sense of privacy in a particular location because it may vary from person to person. While older adults consider home their private places, teenagers who live with their parents may not feel the same way as they see their caretakers at home as people who take away their autonomy (boyd & Marwick, 2011), a feeling that may extend to young adults sharing their living space with roommates. This study explored whether users' sense of privacy at home, a location with presumably the lowest location entropy, and that in other locations with higher location entropy affect their use of SNSs.

In addition, people's sense of privacy may differ depending on the device they are using as they may relate one kind of device with more positive values than another. Research has argued that portability and interface design of mobile devices can positively influence users' perception of their usability (Okazaki & Mendez, 2012). However, portability comes at the expense of precise task completion that is supported using keyboards and mice with larger screens on non-mobile devices. Given multiple options of devices, people feel more in control when using a device with an input mechanism that results in less error (Jonsson, Nass, & Lee, 2004). This may partly explain why people may still prefer to use devices like desktop or laptop computers in contrast to more mobile handheld devices. In a study about mobile education, comparing students' sensitivities to different devices in South Korea and the United States, researchers (Sung & Mayer, 2012) found that the American students had more "positive beliefs" about desktop computers by describing them as "fast, sharp, meaningful, good, and realistic" (p. 1333). Varying perceptions of different devices may affect the ways people use them to share information.

Privacy Settings and Management

On Facebook, privacy settings give users some control over others' access to the information they share. These settings continue to change, and whenever they do, users need to re-learn how to manage their information. A previous version of Facebook's Data Use Policy clearly advised users to think carefully about the content they are sharing each time they post something: "Always think before you post. Just like anything else you post on the web or send in an email, information you share on Facebook can be copied or re-shared by anyone who can see it" (Facebook, 2013). Effective privacy management requires consistent attention to changes, as Facebook's privacy policy was updated again in January 2015 and was renamed, "Data Policy" (Facebook, 2015).

However, some people do not even change their privacy settings and leave it as default for different reasons (boyd & Hargittai, 2010; Debatin et al., 2009; Vitak, 2012). First, some users do not know that they can manage their privacy settings. Second, even when they are given the tools to customize their privacy settings, some users do not know where to find them or how to use them (Hargittai, 2015). Third, some users perceive privacy risks as not their own problems but those of others. Because users usually hear about others' experiences of privacy violation, they do not believe that they are personally subject to the same privacy risks (Debatin et al., 2009). Users believe that they are not as vulnerable to privacy risks as other users, and when they believe that they have more control over their information, they become more optimistically biased (Xu, 2012). Some users believe that they know how to protect themselves from online privacy risks, but their privacy knowledge may be equally inadequate compared to that of people who believe otherwise (Debatin et al., 2009).

In particular, young adults tend to be more proactive about changing their privacy settings and restricting access to their information compared to users in other age groups (Madden & Smith, 2010; Rainie, Kiesler, Kang, & Madden, 2013). Due to their privacy concerns, some young adults manage their online reputation by deleting comments, removing photo tags, and unfriending their contacts, and they express more confidence in controlling their privacy settings than those in other age groups (Madden, 2012). Despite their efforts to protect their online privacy, they continue to share personal data and are most likely to report that they have regretted the content they posted on SNSs (Madden, 2012). This contradicting pattern in their privacy behaviors suggests that young adults' privacy perception and management deserve further investigation.

There are a number of explanations for the privacy paradox of sharing personal information despite having concerns about privacy (Barnes, 2006). Users may continue sharing their information based on privacy calculus of comparing the benefits and risks of information disclosure online (Dinev & Hart, 2006; Smith, Dinev, & Xu, 2011; Xu, 2012). Others have suggested that taking protective action is not enough to protect the information the way users intended. Control paradox suggests that having control over publication of content online may lead users to neglect thinking about others' access and use of their information, that is, their ability to share information may seem more salient than others' ability to see the same information (Brandimarte, Acquisti, & Loewenstein, 2012). Moreover, users may make decisions not based on their actual audience, but their imagined audience, "mental conceptualization of the people with whom we are communicating" (Litt, 2012, p. 331). The reality of misalignment between imagined audience and actual audience was suggested in research analyzing the audience logs of 222,000 users (Bernstein, Bakshy, Burke, Karrer, & Park, 2013). Findings suggested that there is a significant difference between the sizes of users' perceived audience and actual audiences with users underestimating the number of people who are exposed to their content.

Research Questions

In light of earlier scholarship, we seek answers to the following research questions:

1. What are young adults' attitudes about using non-mobile versus mobile handheld devices for posting on Facebook?
2. How does young adults' location—home versus elsewhere—influence posting practices on Facebook?
3. How does the intended audience of a Facebook post match up with its actual audience?

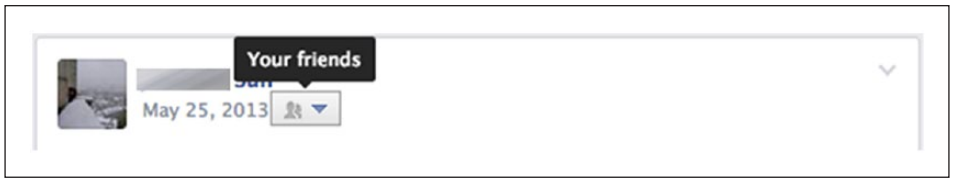

Figure 1. Checking the actual audience of the post by putting the cursor over the audience icon.

3a. How does young adults' sense of privacy in different locations (home vs elsewhere) affect the privacy level with which they share information on Facebook?
3b. How do young adults' attitudes toward different devices (non-mobile vs mobile handheld) influence the privacy level with which they share on Facebook?
3c. Do device and location influence whether people post publicly unintentionally?

Method

Data Collection

We conducted 30 interviews (17 female, 13 male) with young adults between the ages of 18 and 25 years in Summer 2013.[1] Their experience with Facebook ranged from 3 to 8 years. A third of the participants (33.3%) checked Facebook less than five times a day; another third (30.0%), between 5 and 10 times a day; and the rest (36.7%), more than 10 times a day.

We recruited participants by posting flyers on a university campus and in multiple establishments such as libraries and cafés in the nearby urban area. The interviews lasted up to an hour and were held in local cafés. Participants were required to have an active Facebook account, which they accessed using at least two different devices—one non-mobile device (laptop or desktop computer) and one mobile handheld device (smartphone, iPod Touch, or tablet computer).

During the first part of the interview, participants answered questions without looking at a personal device. We created the interview questions based on prior literature to reflect that the definition of privacy may vary from person to person and across different contexts. To address the location-related research question, we asked participants to provide their own definition of privacy, list the locations where they feel they have privacy, and describe whether a strong sense of privacy in those locations affects the content they share or activities they do on Facebook.

During the second part of the interview, participants logged into their Facebook account on the laptop computer provided by the researcher. We asked respondents to describe four different types of posts they had created in the recent past: (1) the last post updated from home, (2) the last post updated from elsewhere, (3) the last post updated from a non-mobile device, and (4) the last post updated from a mobile handheld device. As some participants understood "home" as the one in their hometown, it was qualified as their current residence when asked. These posts included any type of content that was originally created by the participant. We asked participants to scroll far back through their timeline to ensure that they were commenting on posts while looking at them rather than relying on their memory. As two participants did not have one of the types of posts of interest, we analyze a total of 118 posts by 30 participants.

Data Coding

After asking participants to choose the posts described above, the researcher asked respondents to identify the intended audience for each post. Here, the intended audience refers to the people whom the participants had in mind as their audience of the post when they posted it. Then, we asked participants to put their mouse cursor over the audience icon of the post to check the actual audience, which is the privacy setting of each post (see Figure 1).

After completing 30 interviews, the first author transcribed the audio files to begin coding the data. For all 118 posts, we coded whether they had been posted at home or elsewhere and whether they had been updated using a non-mobile device or mobile handheld device. Then for each post, we compared the intended audience to the actual audience. If the actual audience of each post included even one more person than the intended audience, the participant's intended audience and actual audience were coded as not a match. In other words, the "non-match" posts are those accidentally shared with a larger audience than the participants had intended. To allow for the largest possible group of intended audiences for each post, we included everything the participants said verbatim as the intended audience and then compared it to the actual audience. We also coded in which instances the actual audience was "public" because it may expose participants to greater privacy risks than sharing their posts with other types of audiences. To ensure inter-coder reliability, we trained a third-party independent researcher to code just over 10% of the data set. The coding matched for 11 out of 12 posts (91.67%).

By examining whether posts were correctly shared with the intended audience, we were able to assess the effectiveness of the participants' privacy management when updating

Facebook with different devices (non-mobile vs mobile handheld) and in different locations (home vs. elsewhere).

Results

Before addressing our research questions about how type of device and location of posting may influence the privacy of one's posts, we start by reporting on respondents' experiences with Facebook's official privacy policy and with changing the privacy settings of their Facebook accounts.

Experiences with Facebook's Privacy Policy and with Changing Privacy Settings

While most of the participants had not read what was then Facebook's "Data Use Policy", all participants reported that they had changed their privacy settings before. In all, 27 out of 30 participants said that only their Facebook "friends" could view their posts, and the other three participants said that their Facebook "friends" and their "friends of friends" could view their posts. As adjusting privacy settings is an act that shows interest in protecting their information from certain audiences, all participants seemed to care about privacy to some extent, supporting findings from previous research (boyd & Hargittai, 2010; boyd & Marwick, 2011).

Although we did not directly ask participants to discuss their perceived importance of privacy management, 15 participants volunteered that strangers' access to their information motivates them to manage their information. Overall, 14 participants reported that future employers' access to their information was a source of their concern for privacy. One participant said, "mostly for the benefit of future employers, I don't want them to be able to just sift through my photos in case there is anything—there shouldn't be—but in case there is something unflattering" (19-year-old male). Participants with this particular concern assumed that their potential employers could somehow gain access to their information on Facebook. One participant directly pointed to companies using consumers' data for marketing as her main reason for managing her online privacy:

> It's not really anyone else's business—what you do online or anywhere else for that matter. Companies don't really have the right to track your data, and use marketing based on that, or like tracing all your things even though it's your decision to buy them or not. I just don't feel right that companies have access to your data without your permission. (19-year-old female)

Although all participants had shared information from at least two different devices, only three participants had attempted to read Facebook's "Data Use Policy," which outlines how the data users share can be used or collected by Facebook and other third-party stakeholders. In all, 14 out of the 27 participants who had not read the policy thought text was too long and thus too time-consuming to read it. One participant said, "Too long, too technical, and at the end of the day, even if I disagree with what they're doing, it's kind of, I feel like socially [bound] where I have to agree anyways" (22-year-old male). Four participants said that they have nothing to hide on Facebook and thus they do not need to know what Facebook could do with their data. The responses from two other participants seemed to show that they engage in privacy calculus (Dinev & Hart, 2006; O'Brien & Torres, 2012; Smith et al., 2011; Xu, 2012) as one of them said, "the value of Facebook for me outweighs the fact that I don't like this practice. I'm not gonna stop using Facebook because I don't like that they do that" (19-year-old male). Another said, "they provide a, you know, pretty satisfactory service for free. And in exchange for that, advertising is just an unnecessary evil of the type of society we live in" (20-year-old male). The remaining participants had other reasons for not reading the privacy policy.

Two of the three participants who reported to have read the policy did not remember the content of the privacy policy, and one participant claimed that the document was not easy to read:

> I mean, they purposefully made it very, very long so that they could slip in things there that you might not necessarily be into. Um, language-wise, it probably was pretty dense; that would also discourage you from reading the whole thing, I guess. (22-year-old female)

Attitudes about Posting from Non-Mobile versus Mobile Handheld Devices

Participants mainly had two reasons for using Facebook on their mobile handheld devices. First, they could check Facebook when their laptops were not available. Due to its size and weight, participants considered their phones and iPod Touches to be more portable than their laptops. Second, they used their mobile devices because these allowed them to access Facebook more quickly than on their laptops. The mobile app sends notifications to users' mobile devices, which they bring with them everywhere at all times.

Despite the advantages of using Facebook on their mobile device, with the exception of one participant, everybody expressed preference for using Facebook on their non-mobile device when the two were both available and ready to go. When comparing their experience of using Facebook on mobile and non-mobile devices, participants mainly considered two factors: convenience and reliability. The participants reported that a laptop is usually more convenient to use because the screen is bigger, and it is easier to type on a keyboard. For those who considered reliability when using different devices, they said Wi-Fi on a laptop feels much faster than an Internet connection on their mobile devices and that their mobile devices are more likely to crash while completing a task.

While most of the participants preferred using non-mobile devices to mobile devices, the interviews revealed that 29

participants still make mobile posts for three reasons: (1) uploading photos from their mobile device, (2) checking in to share location with others, and (3) using mobile apps that are connected to their Facebook accounts, such as Instagram.

Attitudes about Posting from Home versus Another Location

As 22 out of 30 participants were undergraduate students, who usually share their living space with others, most participants referred to their current residence as their "room" instead of their "home." In all, 22 out of 30 participants reported that they feel most private in their room, and 5 of them used the word "home" and "my room" interchangeably. Four participants specifically said they feel most private at home. The remaining four had different answers. While one's current residence may not be the most private place for everyone, these data suggest that the participants feel most private in a place with the lowest location entropy. Only one participant said that she would feel most private both at home and in a place where she can be anonymous: "in a place where there's people I don't know or where no one know me . . . like my house or downtown Chicago" (19-year-old female).

Many users made a clear distinction between their online and offline spaces. When asked whether varying senses of privacy in different locations affect the content of information he shares on Facebook, one participant said, "I hope that I have a good understanding that there's a difference between privacy online and privacy offline" (20-year-old male). In most cases, users' perceptions of the privacy level of their physical location did not seem to affect significantly the content they share on Facebook. Only 5 of the 30 participants responded that being in private locations made them more likely to post more private content. Two of them did not feel comfortable posting private content because of the people around them when in public. One participant said, "I think [being in private] just makes me more likely to share things over messenger or like my status than I would in public just in case like some sort of wandering eyes saw 'em or something like that" (22-year-old female). Two other participants said that they would be more willing to share their emotions online in locations where they feel private. One participant said, "Because at that time, there would be more, [I would feel] more sentimental just [to] express [my] emotions or feelings" (25-year-old female). Another said,

> going back to the feeling of comfortability, I think that translates into some confidence or maybe something that I was a bit unsure of posting in public that I can talk myself into in privacy . . . maybe not more emotional, but maybe more vulnerable. (22-year-old male)

The remaining participant of the five initially claimed that being in private locations did not affect the content he shares on Facebook: "Even if I'm alone and not interacting with anybody else, something I post on the Internet could be seen by however many people" (20-year-old male). Later, when he was commenting on one of his posts, he admitted that being in a private location, in fact, affected the content of the posts he shared on Facebook. When describing the time he posted photos on Facebook at home, he said, "definitely more comfortable, or it's just something that I would rather do at home in private" (20-year-old male).

When asked whether their perception of their location affected the kind of activities they do on Facebook, 22 out of 27 participants responding to that question reported that it did, especially when they are viewing other people's photos. "I think I go through more people's pictures when I'm, you know, in my room on Facebook, versus when I'm in public, then I'm looking at articles or something like that," said 22-year-old female participant. While physical location did not affect the posting practices, it seemed to have affected how they consume information on Facebook. Being in private locations made participants more likely to engage in "mediated voyeurism" (Calvert, 2000; Su, 2012), as 18 out of 22 participants mentioned viewing others' photos or profiles as one of the activities they were more likely to do in private locations. While SNS users can only view content that has been made available by other SNS users who may have had a different intended audience in mind, mediated voyeurism on SNSs seems to be considered a private activity reserved to be done in private locations. When asked why she would not view others' photos in public, the woman quoted above said, "'Cause I would look like a creeper. I wouldn't want someone to see me seeing someone else."

The Intended versus the Actual Audience

When discussing their own privacy settings before describing their posts on Facebook, the participants seemed confident about the security level of their Facebook profiles. Claiming that he wanted to appear "transparent" online for potential employers, one participant said, "I'm not careless about what I post. So that's why I don't have a problem making things public" (19-year-old male). Another participant discussed privacy management as part of an adult's responsibilities: "Because I'm like an adult now, and I just feel like I should be at a point where I'm protecting my information" (20-year-old female). Nevertheless, as the results in the following sections will reveal, there seemed to be considerable discrepancy between participants' intended online privacy management and its actual effectiveness.

All of the participants had changed their privacy settings on Facebook at least once in the past. By changing their general privacy settings, users are choosing their intended audience for all of their future posts. However, the intended audience may vary across posts, so they could take an extra step of customizing the privacy setting of individual posts to share information with the correct audience. Despite the available options

to share their information only with their intended audience, the posts they shared were not as protected as they thought. After examining 118 posts that these participants had created on their timelines, only 34 posts (28.8%) had privacy settings that corresponded exactly to users' intended audiences. For six posts, the size of the intended audience was greater than that of the actual audience; in all other cases, the actual audience was larger than intended. In other words, the participants shared about two of every three posts with people who were not part of their intended audience.

The size of the discrepancy between the intended and actual audience varied. One participant (20-year-old male) described the intended audience of his post as his friends from his hometown, but he did not customize the setting of that post, so it was being shared with all of his Facebook "friends," which was his general privacy setting. Another participant (17-year-old male) specified his intended audience for a post as people who are in the pictures he posted, his college friends, and his friends in the same city, but later realized that the post was being shared with "public," which was different from his privacy setting ("friends only") he reported before being able to see his profile on the computer. Both participants had a specific group of people in mind as their intended audience for their posts, but by checking the privacy setting of the posts during the interview, the first participant realized that he had shared it with all of his Facebook "friends" by accident, and the second participant, with potentially anyone online.

Although there was low age variation among the participants as a whole, age nonetheless seemed to have an influence on the likelihood of selecting the correct privacy setting for the intended audience of each post. Younger participants were more likely to share posts with the correct privacy setting. None of the 24- and 25-year-old participants shared posts with actual audiences that matched their intended audiences (see Table 1).

This pattern in participants' information sharing was consistent regarding both types of devices and physical locations. When examining the posts based on the type of device from which they were uploaded, 38 out of 60 posts (63.33%) from non-mobile devices and 38 out of 58 posts (65.52%) from mobile devices were shared with the incorrect actual audience (see Table 2). The type of device participants used did not seem to have much influence on information sharing behavior as they created similar percentages of non-match posts from both devices. In addition, different physical locations also did not seem to have affected the likelihood of selecting the correct privacy setting before sharing posts. When examining the posts based on the location from which they were shared, 40 out of 64 posts (62.50%) updated at home and 34 out of 49 posts (69.39%) updated elsewhere ($p = .445$) were shared with the incorrect actual audience (see Table 3). Regardless of the location or device, the participants often made the mistake of not selecting the correct privacy setting that corresponded to their intended audience.

Table 1. Intended Audience versus Actual Audience of the Posts Shared from Participants of Different Ages.

Age	Match	Non-match	
18	2 (50.00%)	2 (50.00%)	4 (100.00%)
19	11 (45.83%)	13 (54.17%)	24 (100.00%)
20	10 (28.57%)	25 (71.43%)	35 (100.00%)
21	11 (39.29%)	17 (60.71%)	28 (100.00%)
22	8 (53.33%)	7 (46.67%)	15 (100.00%)
24	0 (0.00%)	8 (100.00%)	8 (100.00%)
25	0 (0.00%)	4 (100.00%)	4 (100.00%)
	42 (35.59%)	76 (64.41%)	118 (100.00%)
		$\chi^2 = 11.0701$	Pr = .086

Table 2. Intended Audience versus Actual Audience of the Posts Shared from Different Devices.

	Match	Non-match	
Non-mobile	22 (36.67%)	38 (63.33%)	60 (100.00%)
Mobile	20 (34.48%)	38 (65.52%)	58 (100.00%)
	42 (35.59%)	76 (64.41%)	118 (100.00%)
		$\chi^2 = 0.0614$	Pr = .804

Table 3. Intended Audience versus Actual Audience of the Posts Shared from Different Locations.

	Match	Non-match	
Home	24 (37.50%)	40 (62.50%)	64 (100.00%)
Elsewhere	15 (30.61%)	34 (69.39%)	49 (100.00%)
	39 (34.51%)	74 (65.49%)	113 (100.00%)
		$\chi^2 = 0.5825$	Pr = .445

Unintentional public sharing. In all, 12 out of 30 participants unintentionally shared at least one post with "public"—anyone on Facebook, or potentially anyone on the web depending on whether their privacy settings allowed their profiles to appear on search engines. The finding about the influence of age on the likelihood of sharing "public" posts was statistically significant (see Table 4). Older participants were more likely to share "public" posts. All but one "public" posts (17 out 18, 94.44%) were accidentally shared with the wrong audience, and this finding was statistically significant (Table 5). In other words, only one of these posts was actually meant to be shared with the "public."

Categorizing and comparing 18 posts that were mistakenly shared with "public" seems to suggest that what users think they do may differ from what they actually do on Facebook. First, most of the participants considered their laptop more convenient and reliable than their mobile device and thought they were more familiar with using the website version of Facebook, which is easier to navigate. However, more posts shared using a laptop or a desktop (13 out of 60, 21.67%) than mobile handheld devices (5 out of 53, 8.62%) were shared

Table 4. "Public" Posts from Participants of Different Ages.

Age	"Public"	Non-"public"	
18	0 (0.00%)	4 (100.00%)	4 (100.00%)
19	3 (12.50%)	21 (87.50%)	24 (100.00%)
20	7 (20.00%)	28 (80.00%)	35 (100.00%)
21	4 (14.29%)	24 (85.71%)	28 (100.00%)
22	0 (0.00%)	15 (100.00%)	15 (100.00%)
24	1 (12.50%)	7 (87.50%)	8 (100.00%)
25	3 (75.00%)	1 (25.00%)	4 (100.00%)
	18 (15.25%)	100 (84.75%)	118 (100.00%)
		$\chi^2 = 15.2829$	Pr = .018

Table 5. Intended Audience versus Actual Audience of the "Public" Posts.

	Match	Non-match	
Public	1 (5.56%)	17 (94.44%)	18 (100.00%)
Non-public	41 (41.00%)	59 (59.00%)	100 (100.00%)
	42 (35.59%)	76 (64.41%)	118 (100.00%)
		$\chi^2 = 8.3596$	Pr = .004

Table 6. "Public" Posts Shared from Different Devices.

	Public	Non-public	
Non-mobile	13 (21.67%)	47 (78.33%)	60 (100.00%)
Mobile	5 (8.62%)	53 (91.38%)	58 (100.00%)
	18 (15.25%)	100 (84.75%)	118 (100.00%)
		$\chi^2 = 3.8828$	Pr = .049

with "public" setting ($p = .049$; Table 6). Furthermore, participants' answers from the first part of the interview seemed to indicate that being in private locations, home being the most private location for most of the participants, does not affect the way they share information on Facebook. Although not statistically significant, more posts from home (10 out of 64, 15.63%) than elsewhere (6 out of 49, 12.24%) were shared with "public" (see Table 7). Two participants could not identify where the remaining 2 of the 18 "public" posts were shared because they updated those posts too long ago.

Overall, there was only one participant who said he did not mind sharing his posts with anyone during both parts of the interview. Although he did not mind having his privacy setting as "public," he still adjusted the setting as "friends except restricted," which was applied consistently to the four posts he shared. Other participants, when realizing that some of their posts were shared with more people than they had intended, had different reactions. The majority (21 out of 30 participants) said that they do not care that additional people who were not part of their intended audience for the post could view the information in the post. This group of participants included those who were initially confident about the security of their Facebook profiles and had shown interest in online privacy management by adjusting their privacy settings. Even after finding out that two of his posts were being shared with "public," instead of his specific intended audience, one participant said, "I post things to Facebook that I'm prepared for the world to see, I guess. I'm not that concerned" (21-year-old male).

Table 7. "Public" Posts Shared from Different Locations.

	Public	Non-public	
Home	10 (15.63%)	54 (84.38%)	64 (100.00%)
Elsewhere	6 (12.24%)	43 (87.76%)	49 (100.00%)
	16 (14.16%)	97 (85.84%)	113 (100.00%)
		$\chi^2 = 0.2609$	Pr = .610

The remaining nine participants reacted differently. Three of them changed the privacy setting of the post during the interview, immediately after learning that anyone on Facebook could view their post. One of them wanted to review her settings after the interview. After seeing the difference between the sizes of her intended audience and actual audience, she said, "it definitely does encourage me to maybe go take a look at my privacy settings when I go home" (19-year-old female). Two participants took it as an opportunity to learn about Facebook privacy settings, as one of them learned that tagging people allowed Facebook "friends" of anyone tagged to view the posts, and another asked, "What does it mean when it says 'public'?" to better understand her mistake (20-year-old female). The rest of the participants did not know how to explain their feelings as two of them vaguely said they did not feel good about it, and one of them kept repeating, "I don't know" (20-year-old female).

Limitations

As with all studies, this one has its limitations. First, the participants in this study were not fully representative of the people between the ages of 18 and 25 years. All of the participants had some level of higher education as they were either currently enrolled in a university or had graduated with at least a bachelor's degree. Moreover, because participating in this study required an in-person interview in the researcher's vicinity, all of the participants were current residents of an urban area.

Second, the method of collecting information about intended audience and actual audience may have prevented the participants from giving more honest answers in some cases. For this study, we checked the actual audience of the post immediately after asking the participants to describe their intended audience for a particular post. As the researcher repeated this process four times with the participants to help them smoothly go back in time on their timelines, they may have figured out the continuing pattern of the questions. As a result, the participants may have consciously or unconsciously described the sizes of their intended audiences as

larger than the actual sizes to match those of actual audiences. Future research will have to implement other methods to determine the match between intended and actual audiences. That said, given the relatively large number of mismatches, the method did capture at least a portion of unintended audience sharing. In that sense, the findings are likely to be conservative compared to audience mismatches that may be present among young users.

One of the findings suggested that users are more likely to share information accidentally with "public" on non-mobile devices than on mobile devices, but the study did not consider additional factors that could account for the difference in users' experiences of using Facebook on non-mobile and mobile devices. For example, as accessing Facebook on mobile devices depends on users' access to wireless Internet or individual data plans, users may be more conscious of their information sharing behaviors on mobile devices. As we cannot dive deeper into the data with this limitation, future research should address various factors that could explain the reasons behind this finding.

Future work should also consider other factors that may be relevant, such as general Internet skills (Litt, 2013) or privacy-specific skills (Hargittai & Litt, 2013; Park, 2013). While the in-depth qualitative approach was able to shed light on certain questions, it makes large-scale data collection difficult. Future work should develop methods that can measure the outcome variable of interest (the match between intended vs. actual audience) in a way that allows for collecting more representative and larger data sets.

Conclusion

Although only a few of the participants had read Facebook's Data Use Policy, all of the participants expressed at least some concern for online privacy by having adjusted their privacy settings. When consciously thinking about information sharing on Facebook, many participants seemed to echo the idea that information they share may be seen by people who they did not think might see it (Debatin et al., 2009). Regardless, participants made posts from at least two devices on Facebook. As suggested by Madden (2012), most of the participants felt confident about their online privacy management on Facebook, and at least a few participants seemed to use SNSs based on privacy calculus (Dinev & Hart, 2006), seeing more value in being active and sharing information on Facebook than protecting their information.

Users can preserve the "contextual integrity" of Facebook by adjusting their privacy settings (Nissenbaum, 2011). When done properly, using privacy settings lets users share the right amount of information with the audience they had intended. Despite participants' perceived high level of knowledge and skills of online privacy management on Facebook, the majority of the posts collected for this study was shared with more people than the participants had intended.

While most participants reported that non-mobile devices were more reliable and more convenient to use than mobile devices, more posts shared via non-mobiles device were shared unintentionally with "public" than ones shared via mobile devices. Control paradox suggests that participants' perceived confidence and familiarity of using non-mobile devices may have focused their attention to their control of sharing information, thereby neglecting to control others' access to their information (Brandimarte et al., 2012).

Furthermore, most participants claimed that varying sense of privacy in different physical locations does not influence the way they share information online, but more posts shared from home—the most private place for most participants—were shared with "public" than the ones shared elsewhere. This result may indicate that being in different locations adds another context to participants' online information sharing. In order to share the right information with their intended audiences in double-layered contexts, users need to differentiate their sense of privacy on Facebook and the one that comes from a particular physical location.

In about two out of three cases, what the participants thought they did was different from what they actually did. Future research should further explore why people's concern for privacy does not lead to effective online privacy management. Also, it would be helpful to know whether knowing about the mismatch between intended versus actual audiences changes people's Facebook uses moving forward.

Acknowledgments

The authors thank Dr. Robert Hariman, Dr. Eden Litt, and two anonymous reviewers for their insightful feedback that helped improve this paper.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The study resulting in this publication was assisted by a grant from the Undergraduate Research Grant Program of Northwestern University's Office of Undergraduate Research.

Note

1. The first author was the interviewer at all of the sessions. The second author participated actively in the development of the questionnaire and its pretesting.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies* (Vol. *4528*, pp. 36–58).

Berlin, Germany: Springer. Retrieved from http://link.springer.com/chapter/10.1007/11957454_3

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312

Bernstein, M. S., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the invisible audience in social networks. In *CHI 2013*. Paris, France: ACM.

Bort, J. (2013, January). Facebook stores 240 billion photos and adds 350 million more a day. *Business Insider*. Retrieved from http://www.businessinsider.com/facebook-stores-240-billion-photos-2013-1

boyd, d. (2008). *Taken out of context: American teen sociality in networked publics*. Berkeley: University of California, Berkeley.

boyd, d., & Hargittai, E. (2010, July 27). Facebook privacy settings: Who cares? *First Monday*. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589

boyd, d., & Marwick, A. (2011). Social privacy in networked publics: Teens' attitudes, practices, and strategies. In *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society* (pp. 1–29). Oxford, UK. doi:10.1037/0003-066X.63.2.111

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. *Social Psychological & Personality Science*, *4*, 340–347. doi:10.1177/1948550612455931

Calvert, C. (2000). *Voyeur nation: Media, privacy, and peering in modern culture*. Boulder, CO: Westview Press.

Constine, J. (2013). *Facebook's growth since IPO in 12 big numbers*. Retrieved from http://techcrunch.com/2013/05/17/facebook-growth/

Cranshaw, J., Toch, E., & Hong, J. (2010). Bridging the gap between physical location and online social networks. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing* (pp. 119–128). Copenhagen, Denmark: ACM Press. doi:10.1145/1864349.1864380

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*, 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Dinev, T., & Hart, P. (2006). An extended privacy calculus transactions model for E-commerce transactions. *Information Systems Research*, *17*(1), 61–80. doi:10.1287/isre.l060.0080

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "Friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*, 1143–1168. doi:10.1111/j.1083-6101.2007.00367.x

Facebook. (n.d.). *Facebook mobile*. Retrieved from https://www.facebook.com/mobile/

Facebook. (2013). *Data use policy*. Retrieved from http://web.archive.org/web/20150120065528/https://www.facebook.com/full_data_use_policy

Facebook (2015, January 30). *Data policy*. Retrieved from https://www.facebook.com/policy.php

Grasz, J. (2014). *Number of employers passing on applicants due to social media posts continues to rise, according to New CareerBuilder Survey*. Retrieved from http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on privacy in the electronic society* (pp. 71–80). Alexandria, VA: ACM.

Hargittai, E. (2015). *Who cares about privacy?* Paper presented at the Annual Meeting of the International Communication Association, San Juan, Puerto Rico.

Hargittai, E., & Litt, E. (2013). New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security and Privacy*, *11*(3), 38–45. doi:10.1109/MSP.2013.64

Hewitt, J. (2007). *Facebook for iPhone is here*. Retrieved from https://www.facebook.com/notes/facebook/facebook-for-iphone-is-here/5353402130

Jonsson, I., Nass, C., & Lee, K. M. (2004). Mixing personal computer and handheld interfaces and devices: Effects on perceptions and attitudes. *International Journal of Human-Computer Studies*, *61*, 71–83. doi:10.1016/j.ijhcs.2003.11.005

Keynote Competitive Research. (2012). *2012 Mobile User Survey*. Retrieved from http://www.slideshare.net/keynote_systems/keynote-mobile-user-survey-1-h2012

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

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, *29*, 1649–1656. doi:10.1016/j.chb.2013.01.049

Madden, M. (2012). *Privacy management on social media sites*. Washington, DC: Pew Internet & American Life Project.

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

Marwick, A., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*, 1051–1067. doi:10.1177/1461444814543995

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*, 32–48. doi:10.1162/DAED_a_00113

O'Brien, D., & Torres, A. (2012). Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, *31*(2), 63–98. Retrieved from http://aran.library.nuigalway.ie/xmlui/handle/10379/4059

Okazaki, S., & Mendez, F. (2012). Exploring convenience in mobile commerce: Moderating effects of gender. *Computers in Human Behavior*, *29*, 1234–1242. doi:10.1016/j.chb.2012.10.019

Park, Y. J. (2013). Digital literacy and privacy behavior online. Communication Research, 40, 215–236. doi:10.1177/0093650211418338

Pew Research Center. (2014). *Device ownership over time*. Retrieved from http://www.pewinternet.org/data-trend/mobile/device-ownership/

Pew Research Center for the People & the Press. (2013). *Public says investigate terrorism, even if it intrudes on privacy: Majority views NSA phone tracking as acceptable anti-terror tactic*. Washington, DC. Retrieved from http://www.people-press.org/files/legacy-pdf/06-10-13 PRC WP Surveillance Release.pdf

Pew Research Internet Project. (2014). *Social networking fact sheet*. Retrieved from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online*. Washington, DC: Pew Research Center.

Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*, 989–1015. Retrieved from http://dl.acm.org/citation.cfm?id=2208950

Solove, D. J. (2007) 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, 44, 745 (GWU Law School Public Law Research Paper No. 289). Retrieved from http://ssrn.com/abstract=998565

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7–41. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1098&context=jpc

Su, P. J. (2012). *Mediated voyeurism on social networking sites: The possible social needs and potential motivations of the voyeurs on Facebook*. The Rochester Institute of Technology. Retrieved from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=4097&context=theses

Sung, E., & Mayer, R. E. (2012). Students' beliefs about mobile devices vs. desktop computers in South Korea and the United States. *Computers and Education*, *59*, 1328–1338. doi:10.1016/j.compedu.2012.05.005

Taddicken, M. (2014). The "Privacy Paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*, 248–273. doi:10.1111/jcc4.12052

Toch, E., Cranshaw, J., Drielsma, P. H., Tsai, J. Y., Kelley, P. G., Springfield, J., & Sadeh, N. (2010). Empirical models of privacy in location sharing. In *UbiComp '10* (pp. 129–138). Copenhagen, Denmark: ACM Press. doi:10.1145/1864349.1864364

Tufekci, Z. (2012, June 14). Facebook, youth and privacy in networked publics. In *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media* (Vol. 148, pp. 36–37).

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*, 451–470. doi:10.1080/08838151.2012.732140

Wortham, J. (2009). *More employers use social networks to check out applicants*. Retrieved from http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/?_r=1

Xu, H. (2012). Reframing Privacy 2.0 in online social network. *Journal of Constitutional Law*, *14*, 1077–1102. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/upjcl14&section=34

Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, *24*, 1816–1836. doi:10.1016/j.chb.2008.02.012

Author Biographies

Jennifer Jiyoung Suh (BS, Northwestern University) is a student of Communication at the University of California, Santa Barbara. Her research interests include privacy perceptions and information sharing behaviors. This article is based on her honors thesis work at Northwestern University.

Eszter Hargittai (PhD, Princeton University) is Delaney Family Professor of Communication Studies and Faculty Associate of the Institute for Policy Research at Northwestern University. Her research looks at how people may benefit from using the Internet in their everyday lives with particular focus on how Web-use skills may play a role in this process. She has looked at these questions in the domains of information seeking, health content, political participation, job search, the sharing of creative content, and privacy management.