Strategies and Struggles with Privacy in an Online Social Networking Community

Katherine Strater* and Heather Richter Lipford+
*Department of Psychology
+Department of Software and Information Systems
University of North Carolina at Charlotte
+1 704-687-8376
{kpstrate, Heather.Lipford}@uncc.edu

ABSTRACT

Online social networking communities such as Facebook and MySpace are extremely popular. These sites have changed how many people develop and maintain relationships through posting and sharing personal information. The amount and depth of these personal disclosures have raised concerns regarding online privacy. We expand upon previous research on users' under-utilization of available privacy options by examining users' current strategies for maintaining their privacy, and where those strategies fail, on the online social network site Facebook. Our results demonstrate the need for mechanisms that provide awareness of the privacy impact of users' daily interactions.

Categories and Subject Descriptors

H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms

Human Factors

Keywords

Privacy, online social networks, Facebook

1. INTRODUCTION

Online social networking has evolved into a social phenomenon on websites such as MySpace.com and Facebook.com, with approximately 110 million and sixty million active users on the sites respectively [9]. Participation on these sites has surpassed participation in all other online activities and the majority of respondents to DeGagne and Wolk's (2006) survey reported Facebook/MySpace as their primary online "addiction" [5]. The benefits of these sites include communicating with and strengthening personal connections, both with friends already known offline and with people known only virtually.

As part of their participation in these online communities, Internet users are revealing a large amount of personal information to manage their identity and build social capital [8, 10, 14]. Users may disclose their interests, contact information, photos, daily activities, associations and interactions with other users and groups, and more. This proliferation of personal data presents a variety of risks for individuals. Users may face embarrassing situations or blackmailing by revealing sensitive or inappropriate data unintentionally [4]. Profiles on MySpace and Facebook have been used by law enforcement [18] and employers [15] for investigation into users' personal histories. Users also inadvertently put themselves at risk for serious physical or online attacks, such as stalking and identity theft. Additionally, with available technology such as face recognition, profiles can be linked across communities or with other databases, thus reducing the privacy of even anonymous data [12]. Due to inexpensive storage and increasingly sophisticated search capabilities, data may be archived for continued accessibility, placing users at risk indefinitely.

Participating in a social community requires the sharing and disclosure of personal information [17]. In this domain, privacy can be thought of as a process of boundary management [2], as individuals alter their behavior to disclose or not disclose information in order to manage their identity and allegiances with others over time [17]. In the physical world, this is a fluid and dynamic process, as the fine line between private and public shifts due to the social context and intentions of an individual [2]. While managing identity and privacy is a continuously negotiated process in face-to-face interaction, online interactions make the case-by-case decision-making process difficult. Users rarely interact with each other synchronously. Instead, decisions of privacy, what to disclose and how, must be made a priori and explicitly.

Despite the risks, many of the privacy and access control mechanisms of online social communities are purposefully weak to make joining the community and sharing information easy. Additionally, there is little awareness of privacy policies and use of existing privacy mechanisms among active users [11]. Research has offered several explanations for this under-utilization of privacy options, including poor interface design and permissive default settings [12], social conformance [11], and inherent trust in the online community [1, 4, 12].

We aim to improve users' privacy management in online social networking communities. In this paper, we present our first formative study, where we explore in detail the concerns and strategies of users in one community, Facebook. Our qualitative study reveals the privacy decisions and strategies utilized by our participants, as well as circumstances under which these strategies fail. We also highlight the need for users to be more aware of the implications of their online actions and encouraged to reflect on their privacy decisions, thus improving their ability to act within their desired boundaries of privacy.

2. FACEBOOK

Launched in November, 2004 by Harvard University undergraduate Mark Zuckerberg, Facebook.com was intended as a forum for student interaction and information flow on college campuses. Approximately 85% of undergraduates in the U.S. maintain a profile [7, 18] and participation on the site increases daily. Facebook has since expanded beyond universities and is now open to the general public. Facebook is unique from similar networking sites because participation and profile accessibility are structured by the user's offline network — their university, workplace or city of habitation. People join the Facebook networks containing only members of their chosen offline contexts. A person outside a user's network may not view his/her full profile unless the two are linked as friends.

Users join Facebook primarily to keep in contact with distant friends and to search for individuals recently met at their current university or workplace. Users also expect that these people are the primary audience for their own profiles [13]. While some networks are small, many university or regional networks have tens of thousands of users. As a result, users often underestimate the accessibility of their own information [1].

Facebook profiles include more disclosure categories than competing sites MySpace and Friendster [18] and in order to create a descriptive and accurate impression on viewers, users often respond honestly and in the majority of disclosure categories [11]. Although the site has extensive privacy controls for limiting the accessibility of any profile feature, large-scale analyses of profiles in college networks indicate a majority (87% on average) of students have default or permissive privacy settings over their personal information [11, 12]. While the majority of users indicate awareness of the privacy concerns and available options, research suggests that users' privacy attitudes do not impact their decisions to disclose sensitive information [1], and less than half of users report altering their default settings [11]. Little research has examined user-generated explanations for these behaviors, including the problems they encounter in managing their privacy over a variety of personal and sensitive information.

2.1 Profile Features

Facebook profiles can be extensive, including a variety of self-reported information (disclosures) as well as details of the user's social environment, including pictures, friends lists, and messages with friends.

Users can disclose a variety of information in their profiles, including the following categories:

- *Basic Information:* Basic descriptive information including gender, birthday, and hometown.
- *Contact Information:* Includes information such as address/dormitory, phone number, email, IM screen name and personal websites.
- *Personal Information:* Descriptive information to convey interests, likes, and personality, such as "About me" and favorite books and movies.

The remainder of the profile reflects social features and the users' activities with their social network, including:

- *Pictures*: Users can upload digital images, identify people in them through "tags," and make comments. Photos "tagged" of another user are viewable on his/her own profile.
- *Friends*: Users request and accept friends, which are then linked through profiles.
- *Wall*: Friends can enter messages that remain posted on the profile for others to read.
- *Minifeed/Newsfeed*: A list of any recent activity on the profile, such as adding a friend or changing personal information. These "stories" are also displayed on friends' homepages.

Users are given granular control over the availability of every profile feature, and by item for contact information. These controls range between "only me" (for some items) to "all networks and all friends." Users can also simply restrict access to their entire profiles to "only friends" through one control. All privacy controls, including those that control the information returned in search results for the user, Newsfeed preferences, and applications are spread out across more than six separate pages.

For purposes of this paper, we also define the following privacy-related aspects of the profile.

- *Public Profiles*: Profiles viewable to all people in a user's network. Users may still restrict access to individual pieces of information in the profile.
- *Private Profiles*: Profiles that can only be viewed by a user's friends.
- *Search Profile:* Profile information returned in search results. Users from separate networks may view full name, profile picture, friends list, and networks.

3. STUDY METHOD

While other studies have examined Facebook profiles and identified the under-utilization of privacy mechanisms, we sought explanations as to how and why users make decisions to share and protect their personal information. We sought to identify how users interact with their profiles and their social networks, how they create their mental models regarding their audience and accessibility, and their strategies for maintaining privacy levels appropriate for these mental models.

3.1 Participants

Eighteen undergraduate students at our university registered for this study through the psychology department's research participation pool and earned class credit towards their general psychology courses for their participation. The UNC Charlotte Facebook network maintained approximately 20,000 users at the time of the study. Six participants were male, 12 female; 7 were freshman, 5 sophomores, 4 juniors, and 2 seniors. The mean age of participants was 21.17 years, with a range of 17 years. Two participants had created profiles on the Facebook site within three weeks of the study and thus had relatively limited profiles. Although they were still learning how to use the site, these participants did alter their privacy settings and disclose information in personal categories, so their data was included in all quantitative analyses. All other participants had maintained active profiles on the site for between six and twenty-four months. All participants maintained profiles that could be found within the university network.

3.2 Procedure

Each interview took approximately one hour and occurred in our usability lab, where the computer screen, audio, and video were recorded by usability software. A participant first completed a demographic survey before logging into his/her own Facebook profile, where we noted the information disclosures and privacy settings. We then interviewed the participant regarding motivations for using the site, reasons for disclosing personal information, opinions about profile features, and decisions regarding social networking. Most questions did not ask specifically about privacy, but focused on issues surrounding privacy management such as sharing, identity, and impression management. The participant then viewed four unfamiliar profiles; two belonging to fellow participants and two under the control of the research team. One of the control profiles was complete and open; the other was partially private, with social performance features restricted but with detailed personal disclosures publicly accessible. For each profile, the participant was interviewed regarding their impressions of the person and the profile.

3.3 Analysis

We first recorded participant's overall disclosure rates and social performances (i.e. friends, Wall posts, photos, etc.) for each profile feature, as well as the use of privacy settings. This data was collected in order to examine overall trends within our sample as well as to profile individual participants when analyzing their interview responses. We transcribed each interview, and analyzed the transcripts using a grounded theory approach, identifying and categorizing common and interesting responses. We also compared interview transcripts with recorded profile data to identify themes as well as possible discrepancies. Additionally, we analyzed the videos of users reviewing other profiles to observe which profile features they viewed in forming their impressions.

4. RESULTS

We summarize the information disclosures and accessibility for our participants in Figures 1 through 3. Five participants maintained private profiles, with the profile only viewable to friends. Similar to other studies, participants disclosed a large amount of information, generally sharing their birthday, hometown, friends, photos, and email. Several also shared sensitive information such as addresses, course schedules, and phone numbers. Participants actively used Facebook's social features and had high numbers of friends (M=75.22, SD=69.58), photos (M=63.72, SD=60.04) and WallPosts from other users (M=211.33, SD=269.69) on their profiles.

The online behaviors of our participants closely resemble those of previous studies, where users primarily join social networking sites to strengthen their relationships [8, 11, 13], regularly engage with other users through features of the site [4, 6], maintain large social networks and disclose high levels of personal information [11, 12, 13, 18], and underutilize the extensive privacy options [12, 18]. Thus, despite our small sample size, we believe that the patterns of behavior identified in our study are representative of college-aged Facebook users.

While previous research has shown that users of online social networking sites underutilize their privacy options, this study reveals more details of users' strategies as well as several factors that inhibit users' choices regarding their online privacy. While all of our participants were aware of privacy concerns involved in online networking and did make attempts to protect themselves, their strategies for achieving privacy were often prone to failure due to individual and interface issues.

4.1 Privacy Strategies

In Facebook, as in many other social networking sites, users are responsible for deciding what information to disclose and whether or not to protect any of that information with privacy settings. From the time they join the community, users are challenged to create a mental model of their online audience and desired levels of privacy, and then determine how to best match the disclosures and accessibility of their personal information to these mental models. Unfortunately, most sites also offer little explanation about the choices users have and the impacts of their decisions, and users are forced to develop their own strategies for achieving an appropriate balance of privacy and self-expression.

Figure 1. Example Basic and Personal Information Disclosures.

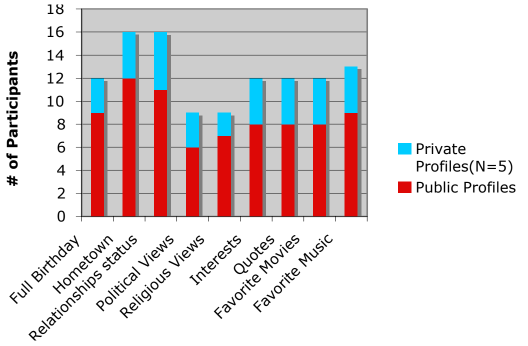
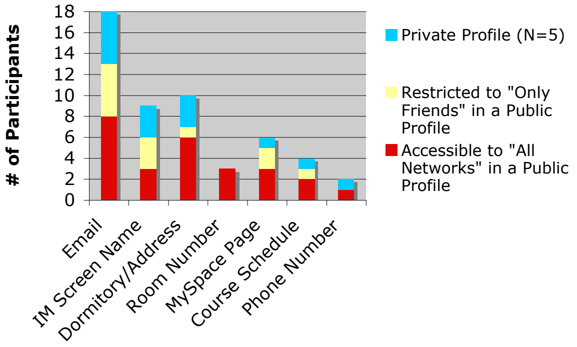
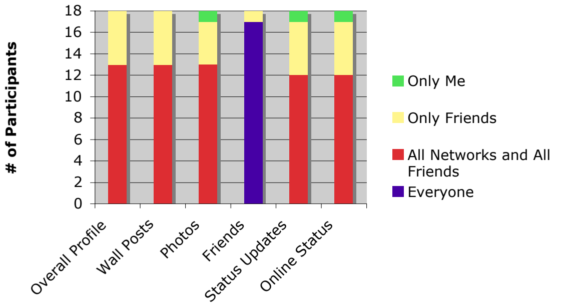


Figure 2. Disclosure Rates and Privacy Usage for Contact Information.

Figure 3. Accessibility of Profile and Social Features.





4.1.1 All or Nothing

In general, users can approach their privacy management in one of two ways: either by controlling what information they enter on the site, or by managing privacy settings to restrict information accessibility to certain audiences. The default and initial settings in Facebook are completely open: all information is shown to all users (within the network).

For our participants, these two strategies often exhibited an all-or-nothing approach. Users who desired privacy utilized a simple setting on the privacy pages to restrict the entire profile to only their friends (5 participants). While Facebook users are given granular control over the accessibility of almost every profile feature, only five participants with public profiles used these controls to limit the accessibility of some of their disclosed information (including the mandatory disclosure of one's email address) (Figure 3), and only one participant with a public profile limited the accessibility of social features to "only friends" (Figure 2). Furthermore, when these controls were utilized, it was in a similar, all-or-none fashion, with all controls set to "only friends" regardless of whether the information was even disclosed or the feature was used.

Our participants also approached disclosures as an all-or-nothing process, choosing either to leave all information fields blank, or fill in most information fields (and what was omitted was often considered redundant, or had been added by Facebook later).

4.1.2 One Time Event

Participants reported that many of their privacy or disclosure decisions were made early in profile creation and rarely reconsidered and altered. Although participants reported occasionally adding items of information to their profiles, there were instances during each interview when participants noted items that were no longer accurate or forgot what they had disclosed. Participants often neglected to review the information already disclosed when making changes to their profiles.

> *"I might add something every once in a while, but I never go through everything on my profile." P[15]*

Furthermore, almost all participants had to review their profiles when asked about the accuracy of their information and their decisions to disclose items, reporting that, *"they were things I could think of at the moment, I'm not sure what I wrote." P[6]*. The privacy settings pages were also rarely revisited. Participants reported forgetting what their privacy settings were, or whether they had even changed their default settings.

Thus, users' privacy management decisions were often made upon joining the social networking community, and were not modified based upon ongoing use. This is problematic because the social norms and pressure of disclosure that early users face prompt them to disclose a good deal of information. Participants reported the impression that disclosures were mandatory when they activated their profiles. And while users did seem aware of the broad audience for their information, they also reported filling out their personal information hastily.

> *"When I was filling it out I didn't put a whole lot of thought into it, I just kind of answered it, and I don't update it very often. When you get on, it's right there, I didn't think twice." P[13]*

4.2 What to Share and Protect

While in general users showed an all-or-nothing, one time strategy, users did still choose to not share or restrict some information. They judged their disclosures based on what they deemed safe and appropriate, as well as what seemed to be socially acceptable and normal within their networks.

4.2.1 Appropriate Information

The most reported privacy concern of our participants was being stalked or physically located by a stranger. This was indeed a realistic concern, as 4 participants reported being contacted outside of Facebook by an unknown person due to information on their profile (and as we did not specifically ask this question, this may be underreported). Thus, participants were careful about disclosing contact information, addresses, and course schedules, and reacted negatively towards users who did disclose such information. All but one participant with a public profile reported being comfortable with the possibility of a large audience, however, as Figures 1 and 3 show, several public participants did still release sensitive information to their large networks, such as addresses and phone numbers.

Users also seemed to completely overlook other sensitive disclosures that could lead to identification, location, or identity theft. For example, Facebook requires a user to disclose his/her full birthday during the account activation process, however this information is automatically available on the profile unless the user specifically alters the privacy preferences for this item. Indeed, 75% of our participants shared their full birthday on their profiles. Similarly, a user's hometown was a common disclosure, as were email addresses and IM screen names.

Based on this primary privacy concern, users then considered many of the other information categories, such as interests and favorite movies, to be safe to disclose.

> *"You don't want to give out too much information so people can hunt you down… But they can't really stalk you knowing what kind of TV shows you like." P[8]*

Participants' disclosures in these less sensitive information categories depended significantly on how they intended to utilize the site. Decisions regarding whether to disclose information at all related to participants' motivations; four participants reported using the site for practical purposes, such as locating classmates and finding local events, and therefore considered personal information irrelevant. These users disclosed less information in all categories.

On the other hand, 12 participants reported that they used Facebook to keep in touch with friends from home and/or new friends from college and thus considered personal information important as a way for people to get to know them and keep up with their interests. For them, the personal information fields were judged appropriate if they were something the user would consider sharing with newly met people, such as school major and activities. Religious and political views were sometimes considered too personal for this audience, and were thus disclosed less frequently than other pieces of basic and personal information.

Our results reflect previous research into online impression management; users actively considered the reactions that others might have to their personal information and social ties [4]. This concern was strongest for photos, where users do not have complete control over what pictures get linked to their profiles. The majority of photos for all participants were reportedly posted by friends. Photos were considered one of the most important features in participant's strategies of self-expression and impression-making. While this need for impression management did affect what users chose to share, no one reported modifying their privacy settings, even for photos, because of these concerns. Two participants who were concerned over inappropriate pictures on their profiles were not even aware of the ability to un-tag themselves from photos or limit photo accessibility

4.2.2 Social Norms

As expected, social norms also impact users' choices to disclose or protect information. Participants in our study were familiar with the layout of Facebook profiles, and took notice when information was lacking or a profile contained sections they were not used to seeing. For example, participants responded favorably to profiles that were completely restricted to "only friends." Although very limited information was available in the search profiles of these restricted users, participants often made relatively detailed, albeit tentative, comments about the user.

However, participants reacted differently when viewing the controlled, partially private profile. In this case, the profile had most basic and personal information viewable, but the social information such as friends and the Wall was restricted to friends only. When viewing this profile, participants reacted with confusion, even negatively, and were more reluctant to comment on the user's personality.

> *"I'm used to seeing all of it. Profiles are either none or all, I don't see this. It makes it really hard to tell anything." P[13].*

Interestingly, these reactions to partial profiles did not apply when users omitted their personal information. When personal disclosures were lacking, participants instead examined the social aspects of their profiles to form impressions. Thus, users may be inclined to not customize their privacy settings if the resulting profile is not like others they have seen, or if the settings restrict information they or others find important, and may be more inclined to disclose information they have seen in other profiles.

4.3 When Privacy Strategies Fail

Although the privacy strategies adopted by our participants may have initially achieved desired privacy protection and matched their initial mental models of audience and accessibility, these strategies often failed over time as participant's motivations, actions, and profiles evolved with use.

4.3.1 A Shrinking Audience

Users who are new to Facebook do appear to consider the possibility of a broad and public audience and take into consideration the range of people who might access their profiles when making decisions regarding their disclosures and privacy. However, as users continue to explore the Facebook interface, enlarge their social networks, and interact with their friends through the site, their perception of their online audience appears to shrink.

As discussed previously, once a user's profile information is filled in, users rarely revisit and update. Instead, they spend time messaging friends, organizing groups or events, and sharing photos. For example, in reviewing the updates on participants' MiniFeeds, we observed 20 stories for new friends, and 29 stories for Wall posts, but none for modifying profile information. Our participants indicated that they were interacting with their friends fairly regularly, both online and offline. They also indicated that they did not search for unknown users or browse profiles, thus having little interaction with users outside of their friends.

As users begin to interact more with the individuals on their friends lists, either directly through the site or in a physical setting, they begin to perceive these individuals as the primary and often solitary audience for their Facebook profiles. For example, P[16] had allowed all users within his networks to view his profile because he had originally been cautious about his disclosures. Although he maintained a relatively small number of friends on Facebook, he was active with these friends, uploading pictures and sending and receiving Wall posts. At the time of study, P[16] had disclosed his mobile phone number and current apartment number and complex through his profile. *"I got a new cell phone and apartment, it's for friends to stay in touch."* Although he reported being uncomfortable with strangers viewing his profile, this information remained accessible to his entire network. When asked about this discrepancy, P[16] replied *"Wow, that's really not a good idea. I didn't even think about that. I guess I should take that down."* Immediately following the study, P[16] blocked access to his profile to "only friends."

The Wall is also a potential source of accidental disclosures. Users reported that they used the feature to make plans with friends, such as lunch with classmates at the campus coffee shop or what party they planned to attend that weekend. Participants did not consider this sensitive information, despite the potential implications of being used as a feared stalking mechanism. Users averaged 211.33 posts from other users on their Walls (SD=269.69), and reported that they rarely deleted them. As we did not read the Wall posts of our participants, we do not have any specific examples of over-disclosures from our study, but have experienced them ourselves. For example, one of the authors had a friend post his cell phone number on her Wall, yet this information was not disclosed on the friend's profile!

Thus the privacy strategy of limiting information disclosures fails due to a shrinking perceived audience. As users interact more with their friends, they begin to see this smaller social network as their primary audience and forget that their profile and any new disclosures, even those made through Wall posts, remain publicly accessible. Although users continue to make decisions that impact their privacy, such as adding new information or accepting new friends, users rarely re-consider their privacy options and instead maintain profiles where the perceived audience no longer matches the real one.

These results partly explain the appeal of restricting the entire profile to only friends, as this simple setting reflects a better match between the perceived and actual audience for most of the users' activities. However, even this setting may be problematic. Several participants did complain about the actions of individuals on their friends lists.

> *"There's this girl that I used to be friends with, and she kept harassing me. Eventually I took her off my list." P[18]*

Participants required minimal offline interaction to accept a friend request, and rarely removed friends, resulting in large friends lists (M=75.22, SD=69.58) that function more like a Rolodex [3]. Thus, even when information is restricted to this friends list, the perceived audience for users may still be smaller than the real one.

4.3.2 *Interface Problems*

Our participants also reported a variety of problems due to the complexity and lack of usability of the Facebook privacy settings. In many cases, the users' expectations of the outcome of their privacy settings did not match what actually happened, resulting in accidental disclosures that would be very difficult for users to detect. Additionally, as users continue to expand their profiles by downloading new applications, joining new networks, or disclosing new information, they rarely revisit their privacy pages to ensure their settings appropriately cover the growing profile.

One major issue is that as users grow their profile or Facebook adds new features, these new features often default back to their "all networks" settings. This goes against the expectations of users who had already restricted their profiles to "only friends." For example, P[13] had originally joined Facebook under her university network and set her profile's accessibility to "only friends," citing that *"I've had problems with weird guys messaging me, so I make everything private."* Since then, she had joined a regional network, and due to Facebook's privacy defaults, her profile was fully accessible to this new and larger network. Because P[13] had never returned to her privacy settings to discover these default settings, she believed that her profile remained accessible to "only friends" in both her university and regional network.

Another serious interface failure was discovered regarding residence information. During data analysis, we realized that P[4] had set her overall profile privacy to "only friends", however her current dormitory was displayed in her search profile and was viewable by all people within her network. Upon further investigation, we realized that the privacy settings for the search profile did not contain a control for residence information, despite checkboxes for other information. A user's residence must be individually restricted through the contact information settings, located on a separate settings page. This setting effected how the residence was displayed on both the full and search profiles. So if a user maintained a private profile, as P[4] did, but did not specifically restrict the residence field to "only friends," this information appeared in search results for the user's entire networks.

We did not discover this intricacy of the privacy settings until after P[4]'s interview, and so could not ask her directly about it. Based on her other responses, we strongly believe that she was unaware of this problem and would consider it a serious privacy violation. Searches into our own Facebook networks revealed that this was a relatively common disclosure in search profiles, where otherwise private users were releasing their residence and even room number to a large audience. Since our analysis, Facebook has stopped displaying residence information on Search profiles (although the user can still appear in search results for a specific dormitory or apartment complex). However, we have discovered similar intricacies between the search profile settings and regular profile settings involving friends and status updates.

Even adjusting and remembering the most basic of settings is challenging. For example, one participant believed she was accessible to "only friends" when in fact she was accessible to all of her networks, while another believed he was public to all of his networks but was actually available to "only friends." Users commented on their confusion and general lack of knowledge about their privacy settings.

> *"I really didn't know how to do it at first, I was stuck. I didn't even know where to look for it. P[18]*

Other participants were unaware of more detailed privacy features, such as the ability to "untag" photos to remove them from the profile. Furthermore, it is difficult to experiment with the privacy settings and determine the outcome of the controls since they do not affect the appearance of the user's own profile. As users stated, *"I didn't know who could and couldn't see what I was doing." P[12].*

One participant reported attempting to test her profile's privacy by changing settings and viewing it from other profiles. However, her description of her perceived privacy still did not reflect the actual outcome of her privacy settings. The authors themselves spent hours doing this same exercise, trying to understand the outcomes of our own and participants' privacy settings.

4.4 Privacy Reflection

While users' privacy decisions are generally an all-or-nothing, one-time process, many participants in our study reported events that prompted a reflection of their disclosures and privacy strategies. These reflections resulted in participants either readjusting their mental models of accessibility, online appropriateness, and perceived audience to better match the reality of online social networking; or altering their privacy options to better match their original and/or desired mental models. Our participants reported several of these events, where being "creeped out" in some way prompted a privacy reflection and adjustment or restriction of the profile. We also observed this reflection occurring due to participation in our own study, which we also discuss below.

4.4.1 *Contact from Strangers*

A major type of reflection event that occurred for our participants was the personal experience of a privacy intrusion, usually in the form of unwanted contact from an unknown person. Three participants with private profiles reported that they had restricted their profiles due to previous privacy intrusions on either Facebook or MySpace.

> *"I've done the whole phone number thing but had to change my number because someone kept calling, they got my number off Facebook."* P[6]

Two participants had received phone calls and text messages from unknown users while several more reported annoyance over Facebook messages from strangers. Several users also reported modifying their profile rather than adjust their privacy settings to deal with this annoyance. For example, three female participants reported switching their relationship status to items such as "married" or "engaged" to discourage strangers from sending messages.

4.4.2 *The Newsfeed*

Facebook has also introduced new features and applications that many users deemed intrusive. The largest of these was the introduction of the Newsfeed, where users' activities on their profiles were broadcast to their friends. When launched in 2006, privacy settings were not even available to control information flow and spawned a Facebook revolt of online petitions and subsequent media frenzy over privacy concerns.

While the frenzy has died down, users still reported dislike for this feature:

> *"I was creeped out when they started the stalker-ticker… I don't think it's necessary to know everything a person does on their profile." P[9]*

Note that the Newsfeed does not change the accessibility of any profile feature or disclosure, it instead increases users' awareness of that information by more directly informing them of changes made on their friends' profiles. Users responded to this awareness with additional privacy management. Seven participants altered their privacy settings for the Newsfeed to control which stories were "published" on their own profile and sent to friends. Additionally, 3 participants reported manually removing stories from their MiniFeed, which subsequently prevents the Newsfeed from publishing them.

However, while many users did adjust their Newsfeed privacy settings, users did not report that the Newsfeed application resulted in modifying any other profile settings or information. This is despite the fact that although the privacy settings prevent some information from being posted on the Newsfeed, they do not prevent the user from appearing on the "recently updated" sections of their friends' lists. Thus, the Newsfeed seemed to prompt reflection about just the Newsfeed feature, and not about the accessibility of the profile overall.

4.4.3 Elicited Reflection

The process of participating in our study prompted participants to reflect on their own mental models of appropriateness and perceived audience, many of whom reported that they planned to alter their privacy settings or remove information from their profile after the interview.

Searching for and viewing profiles of fellow students whom they had never met prompted many participants with public profiles to reconsider their perceived audience and the accessibility of their own profiles, realizing that their own profiles could be similarly accessed. When sensitive information was disclosed in the profiles they were viewing, participants rebuked the owners. It is interesting to note that this type of reflection is rarely possible in users' daily lives and online activities. When users search for or view the profiles of fellow users, this is usually done for a purpose, such as to develop a relationship; learn more about the user; contact the user for legitimate purposes, etc. In such cases, disclosures are seen as useful and appropriate; and since the users are often already acquainted somehow, knowledge of this information is not considered a privacy intrusion. However, when participants were asked to view profiles of strangers with no personal goal in mind, and someone looking over their shoulders, the sensitive information within the profile was more apparent and considered more intrusive.

> *"The way I just looked her up, anyone else could have done that. They have her class schedule and dorm room. And knowing when she is in and out of her room, anyone could be stalking her." P[8]*

> *"I have no clue who he is, but I can look up all this about him." P[3].*

Furthermore, viewing the profiles of strangers caused participants to reflect on the information within their own profiles. For example, P[9] rebuked a profile for having a course schedule posted, then added "*well I probably shouldn't have done that either.*"

Surprisingly, this trend did not extend to participant's viewing of pictures from profiles of unknown users. All participants examined pictures on the profiles they viewed and although the majority of photos contained appropriate content, participants commented negatively on pictures with a sexual nature, those that gave the impression of too much partying, or those that were not the "usual" group or solo shot. However, no participants considered re-visiting their photos to delete similar pictures from their own profiles.

5. IMPLICATIONS

This study highlights several factors which are inhibiting the use of privacy mechanisms in online social networking. While some of the challenges that were found may be specific only to Facebook due to its particular structure and interface, we believe many issues may be applicable to social networking in general.

One challenge is that users learn what to disclose and what to protect over time, both through the social norms of the community and through their own experiences. Our small sample indicates that perhaps privacy utilization increases over time. Participants with private profiles had maintained accounts on Facebook longer than other participants in this study. Yet, as this and other research has demonstrated, users are not fully aware of the accessibility of their information and underestimate the risks of disclosure. Many privacy decisions are made one time, at initial profile creation. Users are rarely reminded of or given an opportunity to reflect upon their disclosures and privacy after initial profile creation, and these issues are not a concern in their daily social communications with their friends. Users write Wall posts and upload pictures without much thought as to the consequences and reach of that information. This can result in users disclosing information to a broader audience than really intended.

Only noticeable and disturbing events, such as a privacy intrusion, induced users to modify their settings. Being phoned by a stranger led users to restrict access to their profiles. The perceived intrusiveness of the Newsfeed led many to use the privacy controls of that feature. Participating in our study also led to such reflection. Participants were generally unaware of the actual impact of their own disclosures until confronted with similar information in an unfamiliar profile and asked to consciously make impressions. Participants became more acutely aware of their role as the audience, subsequently altering how they considered the appropriateness of their own profiles.

The goal of our study is to inform future research on improving privacy management in order to reduce the risks of participation on social network sites. Our results have several implications for potential requirements, and shed light on important issues and challenges in designing new privacy mechanisms for Facebook and other communities.

The most basic solution to over-disclosures would be to enforce, or at least default to, more restrictive settings, particularly for sensitive and risky information. This would help new users by providing immediate protection; and, as users rarely modify their settings, protect even experienced users while still letting them customize their settings to share information when desired. Yet, this will not help users understand and use the privacy controls, nor understand the impact of any changes they do make to their profile or settings. Also, potentially sensitive information can appear in many profile areas, so new defaults may still not accurately reflect the users' privacy needs and desires.

A key goal in privacy management is that users must always be made aware of what information is being shared with whom to prevent accidental disclosures. Improved interfaces need to be developed that provide a more accurate mental model of the outcomes of the various privacy controls. The complexity of the Facebook profile leads to a large number of privacy controls, spread out over multiple pages. In the end, this complexity was incredibly confusing and time consuming. Privacy controls also need to be highly visible, making them accessible while users are modifying their profile instead of located on separate pages. If the user ignores these privacy pages, they will never see their options for modifying the privacy settings. While Facebook has some of the most complex privacy controls and its own idiosyncratic problems, more sites may face similar problems as they expand their features as well.

Making privacy controls more usable still does not address users' confusion over how and when they want to use them. For example, many privacy experts are concerned about releasing a full birthday as this can be used in identity attacks. Yet users often disclose this information, despite the very visible controls on Facebook for restricting this disclosure to month and day or to hide it completely. Designers need to consider ways to educate users to protect themselves while still allowing them to socially interact.

We also need to promote a clearer understanding of the audience of the information. This is another mental model that users must maintain, with little help from the current interface. This mental model can only be created through participation within the community, as opposed to interaction with the user's own profile. Thus, there seems to be a need for mechanisms that improve users' awareness of their profile accessibility initially, and continues that awareness and promotes reflection over time. These mechanisms need to be attached to the regular activities of the users, so privacy does not remain a separate and rare consideration as the user's audience perceptions change.

However, the impact of any privacy management interfaces and mechanisms need to be considered carefully. Social networking sites are popular for a reason. People naturally disclose and protect information to form and strengthen social bonds [2]. If too much of this information is restricted, those bonds will not be created or maintained within the community. For our users, increasing privacy meant completely restricting the profile to just friends instead of selectively disclosing and protecting individual pieces of information. On an individual level, this was not as negative as we expected. Users looked positively on private profiles, and still made remarkably detailed, albeit tentative, impressions from very little information. However, if many more profiles become private, the overall impact on the community may be more profound, leading to decreased participation. For example, Facebook users can search for others in their classes or with similar interests only if that information is not restricted. We would like to achieve increased privacy that is not at the expense of reduced social communication and participation on Facebook or other online social networking communities.

Partially restricting information may better balance privacy and accessibility. Yet doing so currently requires significant effort by the user to choose the desired settings for individual pieces of information. Additionally, as few users currently do this, others are not sure how to interpret this kind of profile. Perhaps privacy solutions could more automatically suggest a reasonable balance. For example, our participants highly valued pictures and personal information, particularly shared interests, in forming impressions and getting to know other people. This implies that solutions should seek to still provide access to some amount of this information, but could restrict other aspects of the profile. How to usably achieve this kind of balance while still providing customizable privacy controls is an important and challenging issue.

6. CONCLUSION AND FUTURE WORK

Our study demonstrates that users of Facebook are aware that their profiles are public and are attempting to disclose appropriate and safe information. Yet users are making privacy decisions based on that awareness only initially or when problems occur, and are overlooking the accessibility of their information during everyday interactions with their friends. Additionally, users are confused by the existing and extensive privacy settings, and are not utilizing them to customize their accessibility. We are currently designing and prototyping a new privacy settings interface for Facebook that attempts to provide awareness and better mental models of the profile audiences, as well as improve users' ability to modify and understand their privacy settings [15].

Our study also highlights a need for more investigation in several areas. Our questions did not examine issues of trust and privacy within friends. The discomfort with the Newsfeed demonstrates that users may not wish to be fully accessible to their entire (and often large) friends list. Recently, Facebook modified the privacy options, allowing users to restrict pieces of profile information from groups of friends. While this allows for more privacy control, it has further complicated the settings. Research is needed to examine how these changes impact users' behaviors, and whether it is possible to simplify this interface while still providing high levels of granular control and encouraging usage.

Although we believe that many of our results are applicable to other social network sites, the unique structure of Facebook's networks, the popularity among college students, and the site's complexity may significantly impact users' attitudes and choices regarding trust and privacy. It is important to examine the differences and similarities in user behaviors and perceptions among these sites. Facebook is also no longer restricted to college users. We are currently investigating whether the disclosures and privacy issues of other user populations differs from college students. Additionally, Facebook and other popular sites now have the ability for 'add-on' applications, written by a third party yet displayed on the profile. These applications have access to profile information, may gather and display new personal information, and have additional privacy settings that users must configure and understand. This raises additional serious privacy concerns and design and interface issues that we intend to explore.

7. ACKNOWLEDGMENTS

This research was conducted with the support of the National Science Foundation (NSF) Grant Number SES-0552160.

8. REFERENCES

1. Acquisti, A. and Gross, R. Imagined communities: awareness, information sharing, and privacy on the

Facebook. In the *Proceedings of Privacy Enhancing Technology (PET 2006)*, Cambridge, June 28-30, 2006.

2. Altman, I. *The environment and social behavior—privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing Company, 1975.
3. boyd, d. Friendster and publically articulated social networking. In the *Extended Abstracts of the Conference on Human Factors and Computing Systems (CHI 2004)*. Vienna, Austria, 2004, pp1279-1282.
4. boyd, d. and Heer, J. "Profiles as Conversation: Networked Identity Performance on Friendster." In *Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39)*, Persistent Conversation Track. Kauai, HI: IEEE Computer Society, 2006.
5. DeGagne, M. and Wolk, R. Unwired : student use of technology in the ubiquitos computing world. In *Proceedings of ISECON 2006.*
6. Donath, J. and boyd, d. Public displays of connection. *BT Technology Journal, 22*, (2004) 71-82.
7. Ellison, N., Steinfield, C., Lampe, C. Spatially bounded online social networks and social capital: the role of Facebook. In *Proceedings of Conference of the International Communications Association (ICA 2006)*, Dresden, Germany, June 19-23, 2006.
8. Ellison, N., Steinfield, C. and Lampe, C. The benefits of Facebook "friends:" social capital and college students' use of online social networking sites. *Journal of Computer-Mediated Communication, 12,* (2007), 1143-1168.
9. Facebook Statistics. http://www.facebook.com/press/info.php?statistics. Accessed January 20, 2008.
10. Gosling, S., Gaddis, S. and Vazire, S. Personality impressions based on Facebook profiles. In *Proceedings of the International Conference on Weblogs and Social Media (ICWSM)*, Boulder, CO, 2007.
11. Govani, T. and Pashley, H. Student awareness of the privacy implications when using Facebook. Unpublished manuscript retrieved September 2007 from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf.
12. Gross, R. and Acquisti, A. Information revelation and privacy in online social networks (the Facebook case). In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society,* Alexandria, VA, USA, November 7, 2005, pp 71-80.
13. Lampe, C., Ellison, N., Steinfield, C. A face(book) in the crowd: social searching vs. social browsing. In the *Proceedings of the Conference on Computer Supported Cooperative Work*, Banff, Alberta, Canada, 2006.
14. Lampe, C., Ellison, N., Steinfield, C. A familiar Face(book): profile elements as signals in an online social network. In the *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* San Jose, CA, 2007.
15. Lipford, H. R., Besmer, A., and Watson, J. Understanding Privacy Settings in Facebook with an Audience View. In the *Proceedings of the USENIX Workshop on Usability, Psychology, and Security (UPSEC 2008)*, April 14, 2008.
16. Palank, J. Face it: 'Book' no secret to employers. *The Washington Times*, July 17, 2006.
17. Palen, L. and Dourish, P. Unpacking "privacy" for a networked world. *CHI Letters*, 5(1), 129-136, 2003.
18. Romano, A. Walking a New Beat: Surfing MySpace.com helps cops crack case. *Newsweek*, April 24, 2006.
19. Stutzman, F. An evaluation of identity-sharing behavior in social network communities. In the *Proceedings of iDMAa and IMS Code Conference*, 2005.