Understanding Privacy Settings in Facebook with an Audience View

Heather Richter Lipford, Andrew Besmer, Jason Watson
Department of Software and Information Systems
University of North Carolina at Charlotte
9201 University City Blvd., Charlotte, NC
{Heather.Lipford, arbesmer, jwatso8}@uncc.edu

Abstract

Users of online social networking communities are disclosing large amounts of personal information, putting themselves at a variety of risks. Our ongoing research investigates mechanisms for socially appropriate privacy management in online social networking communities. As a first step, we are examining the role of interface usability in current privacy settings. In this paper we report on our first iterative prototype, where presenting an audience-oriented view of profile information significantly improved the understanding of privacy settings.

1. Introduction

Online social networking communities have undergone an explosion in recent years, as both the kinds and numbers of sites has grown and membership increased. As part of their participation in online communities, Internet users are revealing a large amount of personal information. This proliferation of personal data presents a variety of risks for individuals, such as identify theft, stalking, embarrassment, and blackmail. As participation in online communities increases, so does the necessity for flexible privacy mechanisms to protect user data.

Despite these risks, many privacy mechanisms of online social communities are purposefully weak to facilitate joining the community and sharing information. Additionally, there is little awareness and use of existing privacy mechanisms among active users [6]. Research has offered several explanations for this under-utilization of privacy options, including poor interface design, permissive default settings [7], social conformance [6], and inherent trust in the online community [1, 2]. In many cases, users are unwilling or unable to put forth the effort to modify and manage their privacy settings to protect their personal information. By improving usability, we believe we can address some of these issues and help users become more comfortable with modifying privacy options.

Our ongoing research examines privacy in online social networking sites, aiming to improve the security and privacy management of personal information. As a first step, we are examining and proposing improvements to current privacy mechanisms. This addresses one aspect of the problem: improving the ability of users to manage their privacy if they desire. In order to do this, we are currently focusing on one particular social networking site, Facebook. Facebook is extremely popular and has numerous information disclosure categories and also has more extensive privacy settings than similar sites.

We are designing a new interface for managing privacy settings in Facebook focused around an audience point of view. In this paper we discuss our first iterative prototype and evaluation that demonstrates that interface improvements can impact users' understanding of their privacy settings. These results will inform the design of a more functional prototype that will examine the role of audience and visual feedback in privacy management.

2. Motivation and Background

Facebook was intended as a forum for student interaction and information flow on college campuses. Since Facebook opened to the general public, it has grown to 62 million active users [4]. A number of studies have examined Facebook and similar sites to demonstrate the wide-scale disclosures of personal information such as dorm rooms and phone numbers, and the general lack of alteration of the default and permissive privacy settings [1, 7]. To guide our own research, we first performed a formative study where we interviewed 18 undergraduate students about their use of Facebook and privacy concerns and management [8]. We learned that users do have privacy concerns, but often struggle with privacy management and can accidentally and unintentionally disclose personal information.

One problem we discovered in Facebook is the usability of the current privacy settings. In our formative study, users reported that the privacy interface was confusing and time consuming [8]. The current interface has limited visual feedback, confusing language, and promotes a poor mental model of how the settings affect the profile. Even after modifying settings, users can experience difficulty in ensuring that their settings match the actual desired outcome. We used these findings as motive to develop a new privacy settings interface.

In real world interactions, users present different facets of their identity to different audiences [5]. Online, users attempt this same identity management task by tailoring their profile for various and broad audiences [2]. Our formative work also revealed the importance of the audience in users' conceptions of their information sharing. Users' awareness of the broad audience of their information did influence them initially in profile creation as they explicitly decided what they were comfortable sharing publicly. However, that awareness was reduced in day-to-day interactions with friends. Users often did not think through the consequences of their regular activities until reminded of the public audience of their information, such as after unwanted messages from strangers [8]. Thus, we propose to improve privacy management in Facebook and other sites by structuring privacy settings around the notion of the audience to help users better conceptualize the impact of information sharing and protection. By improving users' understanding of privacy and information sharing, we hope to encourage greater utilization of privacy settings and to reduce the inadvertent sharing of personal information.

3. Current Facebook Interface

Facebook has extensive privacy settings, controlling access to nearly all profile information. The settings are accessed through a privacy link displayed on the top right of a user's profile. This link brings up a privacy overview page with six information categories. Each of these links, some of which link to additional sub pages, opens a page of menus and checkboxes to set privacy levels or control information flow. Alternatively, a few settings are visible while entering or editing profile information, namely for the birthday and contact information. Users can generally choose to show information to no one, friends, or some or all of their networks (university, region, or workplace).
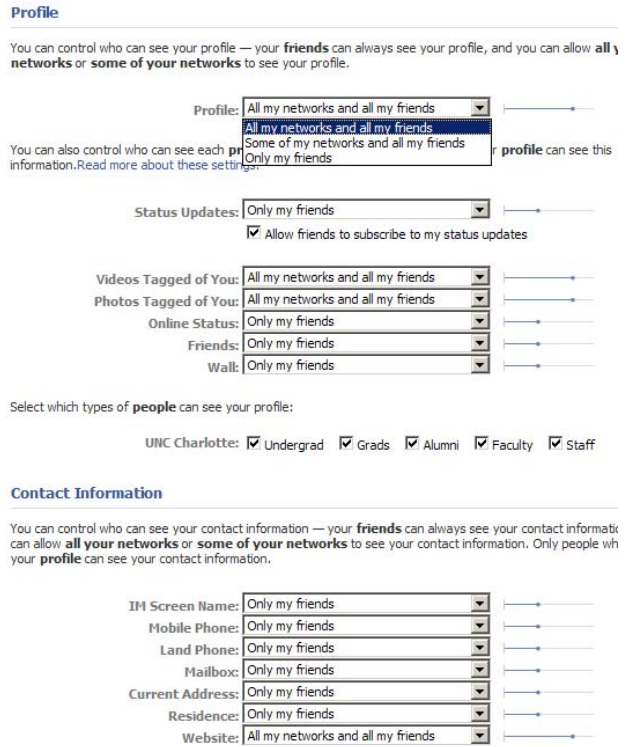

Figure 1. Facebook profile privacy settings.

Our study primarily focuses on privacy settings involving profile data (as opposed to settings regarding Applications or the NewsFeed.) A piece of the profile privacy settings page is shown in Figure 1. Most fields or categories of information can be set to "All my networks and all my friends," Some of my networks and all my friends," or "Only my friends." Users can also restrict their entire profile with a global setting. This is often the only setting users touch, restricting all of their profile to just friends with one menu item without having to even look at the rest of the settings pages. The interface also provides a visual summary of the setting with a dot on a line, indicating how much or how little access applies to that item or category. There are currently no mechanisms for determining how a setting modifies the viewed profile page, except for viewing the profile from someone else's account.

One usability issue with the current interface is consistency. While some individual settings appear straightforward, configuring settings for an entire profile is confusing and settings can have strange affects on one another. For example, when editing the birthday, users are able to obfuscate part or all of the date, see Figure 2. Yet this setting differs from all of the other privacy settings by not allowing configuration for the different

audiences. And, unlike other privacy settings, there is no corresponding setting on the profile privacy pages. We have found even more baffling issues. For example, the global profile privacy setting seems to somehow interact with and override the setting for showing the friends list on a Search profile! Finally, settings and their effects change over time as Facebook modifies their application, making it even more difficult to understand and remember how to use the privacy settings.
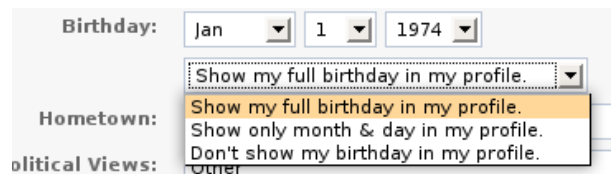

Figure 2. Facebook birthday privacy setting.

Facebook also provides privacy settings for 3rd party applications, adding to the complexity. Applications are given access to profile data through a Facebook API (Application Programming Interface). As applications are added to the profile, Facebook provides users some ability to control the extent of access to personal data. Recently, advertisers were given the ability to create custom applications that could also gain similar access to users' profile information, if permitted by the user. Our initial focus is helping users control privacy to other human audiences. However, access to other applications is an important issue to address in future interfaces.

4. Audience View Interface

We propose to structure the privacy settings interface as the information that a particular audience – search, network, friend, or self – can see. This will help the user associate privacy settings with how their information is presented to different people instead of with lists of privacy menus. We envision this interface to be a series of tabbed pages, where each page presents a separate audience view of a profile, along with controls for showing or hiding information to that group. Thus, the interface naturally provides visual feedback as to the effect of modifying privacy settings, along with an accurate mental model of what information is shared with whom.

This proposed interface is an obvious idea. Orkut, another popular online social networking site, offers an audience view to the user as feedback on profile and

privacy settings. However, while Orkut does provide this valuable visual feedback, its settings are somewhat limited and less complex than Facebook, and there is currently no mechanism to alter any settings within the audience view. Facebook also provides a rudimentary preview in settings for 'Limited Friends' and for people who are messaged. However, this view is generic across all users and merely shows what subsections would be included in the profile without any specific information in them. We believe that by providing an interactive and expanded version of audience views, we can improve the user experience of setting privacy options.

We are currently iteratively prototyping our proposed interface. In our first iteration, we created and examined just the audience view without any mechanism for modifying settings, similar to Orkut's interface. This allows us to verify that this visual feedback is useful and provides guidance for continued design. The prototype, shown in Figures 3 and 4, adds a set of tabs for each audience on top of the existing Facebook interface. This was implemented with HTML by copying the static HTML from various Facebook profile pages, as viewed from other accounts, for each tab view.

To examine the effects of this design modification and to inform the next prototype iteration, we performed a user study to compare the existing Facebook interface with the prototype design. We focused on user understanding and confidence of judging existing applied privacy settings. We now describe this study, its results, and its implications for the design and evaluation of our next prototype.

5. Study

Our study compared the standard Facebook privacy settings interface with our prototype audience view interface. Participants interacted with one person's profile on the real Facebook site, logged in as that user. They also interacted with a different profile using the prototype interface. Note that since the prototype is essentially a mock-up, users could only interact by clicking on the tabs. No other Facebook links functioned. Users were told and shown the relevant pages of settings on the real Facebook interface so they would not get distracted by the other settings in Facebook.

The participants were first given a brief explanation and several minutes to familiarize themselves with each interface. We then did a within-subjects comparison study, where participants used either the Facebook privacy settings interface or our prototype for their tasks,

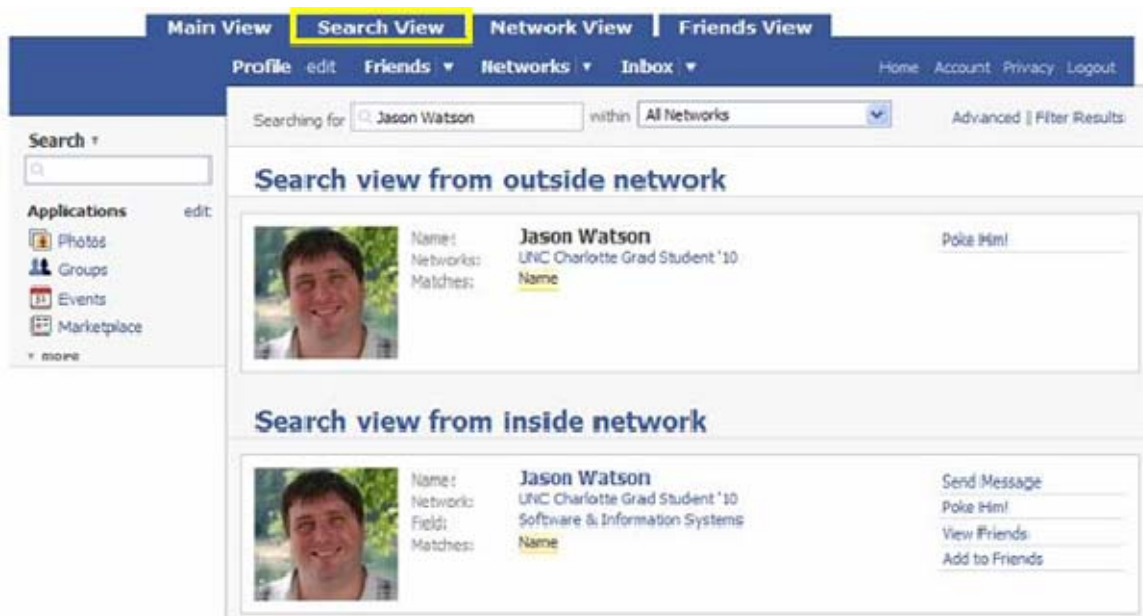**Figure 3. Prototype interface with tabbed view.**

Figure 4. Prototype showing the Search view.

and then performed the same tasks on the other interface. The order of interface presentation was counterbalanced. Participants were given five different tasks asking them to determine the effects of the privacy settings – determining who had access to what information. Participants were also asked to indicate how comfortable they were with their responses for each task on a Likert scale from one to seven, seven being the most comfortable. As an example, one of the tasks given to participants was the following:

If a person outside this profile's network were to search, would they be able to get the following information from this profile:

- o Name
- o Profile Photo
- o Email Address
- o Birthday

On a scale of 1 to 7, how comfortable are you with your answer?

The interaction and audio/video were recorded with usability software. Overall time for all participants on all tasks was gathered, but we inadvertently gathered individual task timing data for only 6 participants.

5.1. Results

Sixteen people participated in the study, 7 females and 9 males. Sixty-three percent of participants had previously used Facebook, while 69% reported experience with another social networking site. Participants who had Facebook profiles reported being a member for an average of 2 years. Additionally, 63% reported modifying privacy settings on one or more social networking websites at least once.

Each task consisted of multiple parts or answers. In Table 1, we report the average percentage of correct answers for each task in both interfaces. We also averaged the comfort level for each task, with 7 representing the highest comfort level. Both accuracy and comfort level increased when using the prototype; this increase was significant in tasks 1, 2, and 3, and close to significant in task 4. Over all tasks, there was a 14.3% increase in comfort and 27.7% increase in accuracy.

Task Analysis				
	Facebook		Prototype	
	Accuracy %	Avg. Comfort	Accuracy %	Avg. Comfort
T1	**45.3**	**5.4**	**98.4**	**6.3**
T2	**37.5**	**4.7**	**100**	**6.7**
T3	**89.6**	5.8	**100**	6.7
T4	72.9	6.1	81.3	6.4
T5	85.4	4.8	89.6	6.2
Avg	**66.14**	**5.4**	**93.86**	**6.4**

Table 1. . Averaged performance for each task. Bold font indicates p<0.05 difference between the two interfaces.

Another way to visualize task performance is bivariate fit of accuracy percentage and reported comfort level for each participant in a task. In Figure 5, we show a plot for the Facebook interface for the first task. Note that several participants indicated a high comfort level yet had a low accuracy on the task. This demonstrates that the participants were comfortable in reporting incorrect answers, and therefore represents a potential false sense of security in understanding their privacy settings. For example, several participants exhibit this behavior in Figure 5.

Figure 5 also shows the variability and inconsistency of both the comfort and accuracy across participants in the Facebook interface. There were a considerable number of participants that reported a high comfort level and yet had many incorrect answers, both in this task and in the others. Figure 6, on the other hand, shows the performance for Task 1 in our prototype interface. Performance appears much more consistent across all participants, with no instances of high comfort and low accuracy. We continued to notice this trend, although to a slightly lesser degree, for the remaining tasks. As participants spent more time examining the Facebook interface, they would predictably be more accurate and more comfortable with the privacy settings.
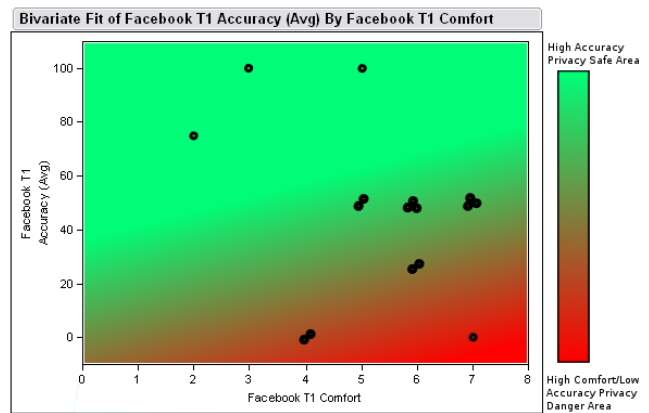

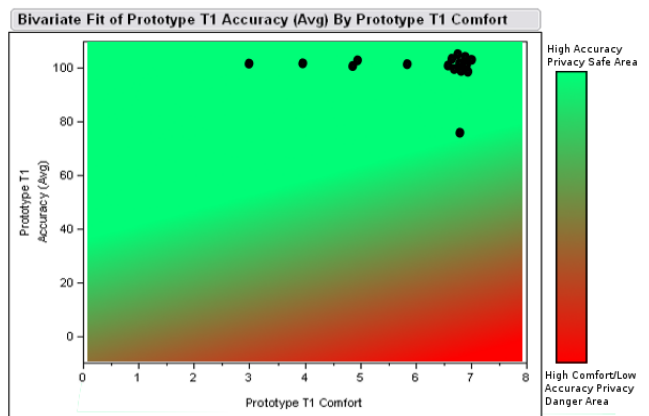**Figure 5. Individual performance on Task 1 in the Facebook interface.**

Figure 6. Individual performance on Task 1 in the prototype interface.

During the user study, we recorded the total time lapsed while completing the tasks. Participants took an average 7.7 minutes completing all the tasks with the Facebook interface, and 4.5 minutes with the prototype. This is a 42% improvement in time to complete the

tasks for the prototype interface. Surprisingly, even when the prototype was presented as the first interface, there was still a 39% improvement in time taken over the Facebook interface. Thus, while users did learn the Facebook interface over time, learning to use the prototype interface did not seem to help with using the existing Facebook interface.

Not only did participants perform more accurately in less time in our prototype, they also preferred the prototype interface to the existing Facebook interface with very positive comments such as:

"I like the new design. I didn't feel frustrated."

Thus, our early prototype appears to have potential to improve privacy management in Facebook by making privacy settings easier to understand in less time.

We evaluated users who were both unfamiliar and those who were already familiar with Facebook, and we did observe differences in behavior. Novices were generally confused about the different audiences; they did not understand the need to show different information to different groups of people. They also struggled to stay on the privacy settings and wanted to keep looking at other parts of the interface. This implies that new users may not immediately understand the need for privacy settings until they become more familiar with the online community, and that perhaps the settings should not be so separated from the rest of the interface.

The users familiar with Facebook were generally faster in performing their tasks, as they understood the audiences and knew where settings were located. However, they still struggled to find a particular setting in the existing Facebook interface, spending much time reading through a page of settings. They still made many errors, and sometimes focused on the wrong group of settings to answer a question. Their behavior was further complicated by the need to sometimes look at more than one setting on different pages in Facebook to complete a subtask. Thus, even with an improved understanding of the community and existing interface, users still struggled to find and understand the settings they desired. To summarize, while new Facebook users were generally slower, all users struggled to understand the existing Facebook privacy interface.

We did, however, notice one important usability issue for our prototype. The initial design hides data if it is protected, giving the user an aesthetically accurate view of what others see. The user however is left to search the entire profile page to find that nothing exists. This may provide a false sense of security since a user can overlook a field and assume it is protected. We observed our participants attempting to solve this problem by accessing the main view, which is less restrictive, to find where the information should be located, then returning to the view they were considering to verify that it was truly hidden. In order to address this problem, we could develop a way for users to visualize data even though it has been protected and hidden from an audience. By doing so, we should minimally affect the profile view so that the interface still remains mostly accurate in terms of aesthetics. We will attempt to solve this usability problem when we add actual modification controls to the interface to show or hide information in different views.

This initial evaluation has limitations. The existing Facebook interface does have more information than our prototype, so users could have been distracted by or confused by additional information. Thus, this is not as accurate a comparison as we could have performed. However, given the consistent results over even this small group of users, we feel it demonstrates usability does have an impact on privacy management in Facebook, and that our new design may be a step in the right direction.

6. Discussion

Our first prototype and evaluation demonstrates that Facebook users do have difficulty understanding the existing privacy settings, and that this can be improved. We believe our prototype interface allows users to have a better mental model than the existing interface. As one user said, "I prefer to see what is happening rather than just read the settings." Facebook's current interface requires the user to become acquainted with the site and be aware of the existing social structure to understand potential impact of the privacy settings. In our own personal experiences, we frequently used two computers with two profiles – modify one then view it from the other – to figure out what a particular privacy setting changed. Our prototype offers users the ability to see the model and the settings applied all at the same time.

The challenge and complexity of the current Facebook privacy interface implies that only those who are very motivated will exert the effort to adjust their settings. In our formative study, we saw this almost exclusively meant setting the entire profile to only be viewable by friends, as this could be done from a single menu without digging into the details of the rest of the privacy settings [8]. Thus, users were either entirely public, or

entirely private. This currently leaves many users with perhaps too much information available to the public. Yet, this could potentially negatively impact the community if too many users become completely private. By lowering the barrier for privacy management in online social networking sites, we hope users will be able to try more customized and nuanced settings in an understandable and usable way. A more usable interface may also allow for even more complex privacy controls, such as the ability to customize views for different groupings of friends or even for individuals.

In addition to making it easier to adjust privacy settings, an audience view also provides a more accurate mental model of information availability and the impact of adjusting privacy settings. This may in turn influence more users to want to protect their personal information as they reflect upon each audience view. However, improved mental models and easier configuration still do not help users understand the risks and implications of decisions to reveal personal information online. Thus, while usability is an important part of privacy management, we are also investigating ways to inform and educate users about the implications of information sharing to help them make more informed decisions.

There are several issues we will need to explore in future iterations of our prototypes. First, the current prototype took into account only one network view. There may be many networks, each with different views on different tabs. Additionally, Facebook or other sites could potentially expand their functionality to allow users to group friends and modify settings for each group, which also adds more potential audience views. We need to investigate how many tabs become too many, and how users would want to deal with a larger number of audiences.

Our design also requires the user to know who belongs to each audience in order to understand how a specific individual can view his or her profile. Several participants indicated they wanted to be able to search for another user and view their own profile from the perspective of that person. We call this the "Joe User" search feature, or as one participant put it, "this is how stalker psychos see you". If this is possible, users may even wish to customize views for individual users. This too will add more audiences and become potentially overwhelming, both conceptually and in the interface.

Finally, we have almost exclusively studied the design and usability of the Facebook interface. While this is a particularly interesting online social networking site, many others exist and offer different functionality and affordances. We need to expand our research to examine these other sites to be able to generalize our interfaces and results to a broad range of online social networking sites.

7. Conclusion and Future Work

Our early prototype and evaluation demonstrates that the usability of privacy settings could be impacting privacy management in online social networking. By providing a better mental model and improved visual feedback of the outcome of privacy settings, we aim to make utilizing these settings easier for both new and experienced users. We are currently implementing a more functional audience view interface that includes controls for modifying privacy settings. We plan to evaluate this interface with a more extensive user study to examine the use and impact of this new design. One aspect of this evaluation will include what settings are appropriate for this new interface, and what current settings may still require additional interfaces, such as the controls over the Newsfeed feature on Facebook.

Improving the interface, however, can only go so far. Our long term research agenda is to investigate novel ways to manage personal information online as well as methods to better educate users as to the impact of their online behaviors and activities.

Acknowledgements

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. 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.

3. 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.

4. Facebook Statistics.
http://www.facebook.com/press/ info.php?statistics. Accessed January 25, 2008.

5. Goffman, E. *The presentation of self in everyday life.* New York: Doubleday, 1959.

6. 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.

7. 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.

8. Strater, Katherine P. and Heather Richter Lipford. Strategies and Struggles with Privacy in an Online Social Networking Community. Unpublished manuscript.