Users’ (Mis)Conceptions of Social Applications

Andrew Besmer
University of North Carolina at Charlotte
9201 University City Blvd
Charlotte NC, 28223
arbesmer@uncc.edu

Heather Richter Lipford
University of North Carolina at Charlotte
9201 University City Blvd
Charlotte NC, 28223
heather.lipford@uncc.edu

Abstract

Many social network sites, such as Facebook and MySpace, feature social applications, applications and services written by third party developers that provide additional functionality linked to a user’s profile. Current platforms allow these applications to consume much of a user’s profile information, as well as the profile information of the user’s friends. Researchers are proposing mechanisms to reduce the risks of this data sharing, yet these efforts need to be informed with an understanding of application use and impressions. This paper examines users’ motivations, intentions, and concerns with using applications, as well as their perceptions of data sharing. Our results indicate that the social interaction driving application use is also leading to a lack of awareness of data sharing, its risks, and its implications.

Keywords: Social Networking Applications, Web 2.0, Human Computer Interaction, Security, Privacy, Identity Management

Index Terms: H5.m [Information interfaces and presentation]: (e.g., HCI)––Miscellaneous.

1 INTRODUCTION

Online social network sites have hundreds of millions of users sharing a variety of personal information. In order to expand functionality, many of the leading social network sites have created a platform to allow third party developers to create applications that utilize and enhance users’ profiles. These applications have been widely successful, with very high adoption rates. Applications add value to the users of social network sites by allowing them to add additional content to their profiles, participate in games, share photos, and much more.

In order to provide engaging experiences, these platforms provide the ability for applications to consume users’ profile data. This data commonly includes attributes like name, birthday, interests, and more. Applications are also commonly allowed to access this same information about friends of the user who have not yet directly accessed the application. The result is that a large set of data is made available to third parties that might not necessarily need it. To demonstrate the risk to users, the BBC News developed a malicious application that had the potential to harvest large amounts of user profile data in just three hours [1].

In order to provide engaging experiences, these platforms provide the ability for applications to consume users’ profile data. This data commonly includes attributes like name, birthday, interests, and more. Applications are also commonly allowed to access this same information about friends of the user who have not yet directly accessed the application. The result is that a large set of data is made available to third parties that might not necessarily need it. To demonstrate the risk to users, the BBC News developed a malicious application that had the potential to harvest large amounts of user profile data in just three hours [1].

To further complicate the matter, information on the user’s friends is given without the adequate knowledge or consent of the user. For example, on Facebook a dialogue such as Figure 1 is shown to users on the first access to the application. We do not believe this message adequately conveys the data sharing that occurs. The message is generic at best and likely ignored because the message dialog looks identical each time. Previous research has shown that over 98% of users rarely read EULA’s [8]. While this dialogue is much shorter, we think users are similarly going to become habituated to the dialogue box and ignore or not understand the information in it, in order to get to the primary task of accessing an application.

For example, consider Katie, a typical social network site user. Katie just signed on and sees that her friend Jason sent her a bumper sticker for her profile. Katie is interested in what the bumper sticker might be, so she clicks a button to see it. Since Katie has never used the bumper sticker application before she is prompted to review the agreement shown in Figure 1 and accept it. Katie quickly clicks the allow button in order to view what Jason has sent. Most of her profile data, as well as much of her friends’ profile data, is now available for the application to query and use.

Existing application platforms also provide little in the way of tools for limiting the profile data that is given to applications. For example, Facebook, one of the most popular social network sites, takes an all or nothing approach, where in order to access an application the user often must consent to sharing most of her profile data. This violates the well-known principle of least privilege [19].

Some users might expect that not using or visiting the application would protect themselves. Even this can violate expectations, as applications can request users’ information by utilizing a friend who did authorize the application. On several sites, users are able to set a default policy on what information is accessible to applications their friends have authorized. These policies are highly permissive by default to encourage social use, and users may also not understand the purpose of these settings or set them appropriately.

It is not hard to believe that privacy problems are occurring given users’ lack of control over their information and their difficulty in understanding the implications of application use. These motivations paved the way for researchers to begin examining alternative access control tools that may help to reduce the risk in utilizing these applications. Proposed solutions have ranged from models where no information about a user is given [7] to sharing generalizations of the personal attributes [20], to providing fine grained privacy settings [2]. While these solutions may address some of the problems, there has been no study of users’ motivations and perceptions to inform these efforts. What is still lacking is not an image has been modified with a fake application name.
articulation of what problems are occurring but an understanding of why. Understanding users’ behavior and conceptions around social applications can help determine why users are struggling and aid in the design of effective and usable tools.

Monitoring and controlling the release of information to applications is a privacy issue where users determine the boundaries of their information disclosures [17]. People manage these boundaries by determining which types of information to share with different groups of people. Thus, even digitally, people do not wish to share everything, with everyone [15]. We find that in this domain, Nissenbaum’s contextual integrity framework is illustrative of the privacy issues [14]. Contextual integrity describes how information sharing is situated within the social context, and privacy problems will occur when the information flows go against social norms and expectations. We believe that users do not understand the information flows of the application platform, and as such, cannot make privacy-appropriate decisions. This makes boundary maintenance difficult as users do not fully understand the scope of the information, actors involved or how the boundaries could be violated.

It is currently unclear where the balance lies between privacy and social value for these social applications. It is clear however, that little is known about why users use applications and how they perceive them operating. This understanding is crucial in order to suggest socially acceptable and understandable methods for using applications while maintaining adequate and desired privacy. This paper examines how users are currently finding, adding, and removing applications as well as what data they perceive is shared as a result of this use. Our results indicate that the social nature of these applications colors user perceptions, leading users to be very unaware of what data applications can access. We then discuss potential implications of these results and the impact on the creation of new privacy tools for social network site platforms.

2 BACKGROUND

Our study focused on Facebook, as it is currently the most widely used and oldest application platform. Facebook currently reports having 400 million active users with 50% of those users signing on any given day [6]. Facebook was the first major social network site to offer an application platform to its users. When creating the API they also created a SQL-like querying language, aptly named FQL, that allows applications to access the vast majority of a user’s profile information, including a user’s name, birthday, education, work history, current location, photos, and more.

The platform has been very successful; Facebook reports that there are over 1 million developers who have created over 500,000 applications [6]. In addition to a large producing developer base there is also a very high adoption rate. Every month 70% of Facebook’s users use at least one application [6]. Indeed many of the features Facebook provides such as the marketplace, photo sharing, and events were written as Facebook applications by Facebook themselves. Soon after Facebook’s platform was introduced, Google created OpenSocial, an open platform that serves as a common application platform across a number of other social network sites such as MySpace, LinkedIn, Orkut, and more [9].

Research on social network sites has shown that users tend to share a large amount of personal information including contact information, associations, photographs, and more [12, 23] which has motivated their friends to participate as well [11]. One study at Carnegie Mellon University found that over 70% of students disclosed their picture, birthday, hometown, and high school information in their profiles [10]. Other research has also examined how various profile information on these sites is used for managing identity, communication, and strengthening relationships [3, 4]. Furthermore, because of the ever increasing amount of personal information, users are putting themselves at risk of identity theft, spear phishing, and stalking [21]. For example, in a 2008 study, Rabkin showed that many challenge questions used to reset or remember passwords can automatically be answered by using Facebook profile data [18].

Additional work has focused specifically on the application platforms we are discussing. Currently these applications are being given access to most of the information on a user’s profile. In addition, applications are able to request similar information on user’s friends. Yet a study by Felt et al. of the top 150 Facebook applications showed that most only needed access to the users’ name, list of friends, and networks they belonged to [7]. This suggests that as many as 91% of applications that are currently available have access to data they do not need, violating the principle of least privilege [7, 19]. This led Felt et al to propose a framework, privacy by proxy, that severely restricts the information available, yet may also restrict value in social applications. Others have suggested generalization of personal attributes in order to help users maintain privacy yet still be able to benefit from sharing information [20].

Research regarding the social application platform has primarily been concerned with the design of access control models. Yet while work is trying to improve privacy, none have examined why applications are used and what users actually think of them. This understanding is critical both to expand and enhance social applications as well as mitigate the risks currently associated with using them. We aim to show how users interact with applications and examine users’ comprehension of data sharing through the platform in order to inform the design of privacy management tools for application platforms.

3 STUDY METHODOLOGY

We conducted a semi-structured interview as well as a survey, to examine key points in an application’s life-cycle: its discovery by users, addition and use, as well as possible subsequent removal. We also examined users’ conceptions of what information is shared, and with whom, and what they would be comfortable sharing with applications.

In the summer of 2008, we recruited 15 students from the city of Charlotte and from our University using paid advertising on Facebook and flyers to participate in an hour long semi-structured interview. Inclusion criteria for the study included the participant being 18 years of age or older, having an active Facebook account, and having used at least one application other than photos, marketplace, or events within the last three months. Interested participants were offered a small financial incentive in exchange for their participation. We recruited 11 additional participants to take just the survey we had developed regarding data sharing with applications.

To conduct the interview, we sat down with participants in front of their Facebook profiles and framed questions around each of the applications the participant had authorized. We asked questions about how the participants found the application, why they decided to authorize it, and if they had removed any applications, examining any factors that were important in making their decisions.

We asked participants if they had ever invited others to use the application, and why. In addition, we asked what they like most/least about the application, and any concerns they might have with it. We also asked participants to explain how applications fit into their usage of the social network site as well as what they consider a good application and a bad application. Since participants were asked to self report, they did not always remember details for every application. When this occurred, we simply moved on to the next application on their profiles.

After discussing all the applications, we administered a survey to participants to gather information about their demographics such as age, sex, race, and education. We used Westin’s privacy segmentation index [13] as part of the survey to identify participants as privacy fundamentalists, pragmatists, or unconcerned. In addition, we used a series of questions with Likert scales to gauge participants'
understanding of which profile attributes were shared with applications. We tested their understanding for applications their friends had authorized as well as applications they had authorized. We included items that are not on Facebook profiles like social security number and files to prevent participants from assuming the correct answer was everything and ensure that participants were truly answering the questions and not simply checking a column. This survey was administered after the bulk of the interview was completed to prevent a bias towards a privacy-centered interview. We then finished with additional interview questions regarding their conception of data sharing in applications. We later invited an additional 11 participants to complete the survey.

4 Interview Results

We interviewed 15 participants with ages ranging from 18-25. Most participants were male (9) and undergraduates in college (13). This is a limitation of this study and future studies examining those who are outside of college would be necessary in order to determine if these findings hold for all groups of people.

Our participants had an average of 13 applications each (min = 3, max = 26), for a total of 195 applications or cases. Participants were unable to recall any details in 36 cases (cases = 18%, participants = 10). We did not include these applications in the analysis. While this is by no means the majority of applications we were still surprised by the number of applications that users could not remember any details of. We suspect at least some of these included cases where our participants might have been uncomfortable discussing the details of an application, such as an application used specifically for dating.

We now present results of our interview, followed by the survey results. We first discuss users’ motivations around finding, adding, and removing applications. We also discuss users’ concerns with applications as well as perceptions of data that is shared with applications. Finally, we discuss what information participants expressed they would be comfortable in sharing.

4.1 Application Life Span

4.1.1 Finding Applications

There are several ways in which applications can spread, including a directory, friends inviting other friends, activity of others displayed in the user’s news feed, and a box displaying the application on the user’s profile. For applications the participant remembered they could not remember the source 17% of the time. Most participants found an application by being invited by a friend (cases = 39%, participants = 14). These invites were broken down into two different categories: those that were based on interaction, and those that were not. Invitations based on interaction inform the user that a friend has shared information or performed some action for them. In order to view the information, or return the interaction, the user must access the application. For example, a bumper sticker application allows users to send interesting bumper stickers to friends to be displayed on their profiles. The act of sending the bumper sticker notifies the other user and serves as an invite for those who have not yet authorized the application. As one participant stated:

P10: “I wanted to see what I had gotten and then I wanted to send them something back.”

That user can then send bumper stickers to other users, further propagating the application.

Other invitations are explicit messages, sent after a user is asked to choose a set of friends to invite. Participants reported being forced into inviting in order to use the application or get a result from it (cases = 6%, participants = 7). Participants generally referred to this as spam, and many of them mentioned that they do not like invitations as a result (participants = 9). Participants mentioned a specific reason or objective for sending, despite seeing them as spam:

P15: “I invite the friends to add the application to earn extra points for something and for each person you invite you get a certain amount of the thing. When you join you earn that extra certain amount too.”

Some participants stated that they would never invite or add an application that required them to invite because of too many unwanted invitations from others. In one case a participant expressed frustration with invitations:

P7: “I never do that because its annoying. Everyone does it to me and I’m like ignore ignore ignore ignore so I don’t want to do that to other people.”

However, this participant later went on to tell us about applications where he had sent things like bumper stickers or gifts to others. While this can also act as an invitation, the perception is less negative and seen as sharing rather than inviting.

Another common way participants found applications was browsing the profiles of their friends (cases = 29%, participants = 12). Participants did not indicate that they were browsing the profiles for the purpose of finding applications. Instead, they indicated that in the course of viewing the profiles of their friends they found an application which was of interest to them. Participants mentioned several other ways they found applications: newsfeed, advertisements, and off-line communication.

Interestingly, browsing for an application in the application directory was the least cited method of finding applications for our participants (cases = 1%, participants = 2). Thus, the most commonly cited ways which participants found applications were social in nature.

4.1.2 Adding Applications

Participants cited a variety of reasons for adding applications, such as to play games or add interesting information to their profiles. A desire for additional interaction with others was the most common reason for adding an application (cases = 25%, participants = 14). This interaction varied from viewing a picture made by a friend to playing an online chess game with friends. In several cases this interaction was a one time event in which a user sent a picture, opened a virtual gift, or viewed another user’s interaction with an application. In many cases, participants mentioned that interaction was based on the need to meet new people or strengthen ties with existing social circles (cases = 11%, participants = 12).

P14: “I added that because I knew I was gonna be in college and I put my courses on there so I could network with people that had my same classes.”

Thus, many applications are facilitating an interaction between two people, enhancing the social experience on the site. Participants reported liking the social interaction created by applications (participants = 15). They frequently discussed how they would compete, play, collaborate, or have contact with others through their applications.

Although social interaction seems to drive much of application use, interest (cases = 22%, participants = 14) and entertainment (cases = 21%, participants = 10) were also mentioned, frequently overlapping interaction with one another.

P9: “Cause I thought it would be cool to compare my best friends with it and my friends that were with it... kind of like a six degrees of separation thing almost.”
Applications revolving around interests commonly include categories like: sports, horoscopes, TV shows, music, movies, and more. Entertainment generally referred to participants who mentioned adding the application to reduce boredom or fill time. Interaction, entertainment, and users’ interests accounted for the majority of the application authorizations.

4.1.3 Application Removal

Many participants reported regularly going in to remove applications (participants = 6) every couple of months. Their reasons for removing applications during this time included inactivity, cleaning up their profile, and an application that looked cluttered.

P14: “Whenever there is some applications that I feel are cluttering up my facebook profile I just delete them basically. Just for aesthetic reasons.”

Participants occasionally removed an individual application immediately after authorizing it. These applications were removed for not meeting the user’s expectations, taking up too much space or also having a cluttered look.

P12: “I just installed it, looked at it, realized I didn’t like it and deleted it.”

Several participants mentioned receiving unwanted messages due to an application, which prompted removal. Participants also reported blocking applications, usually to stop recurring invitations from other users. However, this is not the main purpose of the blocking feature. The block feature is supposed to be used to prevent any information about the user from being consumed by an application. There is a separate button for blocking all invitations from an application. Participants did not appear to understand the true purpose of the blocking feature, although its use did have added benefits in that it prevented any further data sharing with the application.

4.2 Application Perceptions

4.2.1 General Concerns

We asked participants what concerns they had with each application they had authorized or removed, or concerns they might have in general. The concerns reported included profile space, others’ perception, privacy, time investment, and inappropriate content. Privacy is specifically discussed later, for now we will discuss the other issues.

Participants reported profile space as the number one concern of having an application (cases = 19%, participants = 10). They frequently questioned how much space would be required in order to have an application as well as if that space would later be recoverable.

P10: “Well I wanted to make sure it didn’t take up too much room like the fun wall and it looked alright so I kept it and I liked it.”

Once deciding that they would authorize or keep an application, they would become concerned about where to put the application on the profile. Some participants even strategized by speculating on where best to place the application in order to complement their profile. This is less likely a concern today because, since this interview, applications on Facebook are not given a box on the user’s profile automatically, and application boxes are now displayed on a separate tab on the profile. 

Participants were also largely concerned with others’ perceptions of them (cases = 13%, participants = 10). This concern was based on the applications they had authorized or their activities within them. It was magnified at times based on stereotypes about groups of people. For example, a participant who referred to himself as Mexican, had serious concerns about an application involving criminal activity. He mentioned that the activities he would engage in on an application involving ‘mob activity’ did not reflect his activities in the real world.

P2: “[People might say] alright well if he would do that on there… would he do that in real life.”

Other participants were concerned about the conversations others were having about them inside of applications. Examples of this are the ‘hot or not’ application, the compare friends application, or an application involving the buying and selling of friends. In cases like these, participants would authorize the application not to use it, but to monitor the perception others could have about them (cases = 2%, participants = 3).

P9: “I wanted to see what everyone else had to say. I mean who doesn’t want know what other people think about them.”

These participants added the application they were concerned about, then removed it from the profile and newsfeed, just to monitor others’ activities about them occurring inside the application.

The time involved in using an application was another consideration for our participants (cases = 10%, participants = 6). Participants referred to the amount of time required to use the application almost exclusively as a waste of time. Many participants did not want to be bothered with an application that would take up too much of their time, instead preferring applications where they could decide how much time was appropriate. Some cited their own habits about procrastination and how these applications would help them perpetuate this.

Some participants were concerned with the inappropriate content that might be generated due to applications (cases = 4%, participants = 3). This included both viewing the inappropriate content and/or having it posted to their profile.

P7: “[A bad application has] dirty stuff. Umm they all do kind of. Bumper stickers has really nasty stuff…”

One of our participants surprised us though by mentioning her use of an application in which she would poop on other friends’ profiles, which she found humorous. Her biggest complaint: many others were unwilling to authorize it.

4.2.2 Potential Problems With Use

We asked participants what problems they had heard of or could see occurring as a result of using applications. We expected a large number of privacy-oriented responses, yet we were surprised with few of them.

The leading response was that participants were unsure or had never heard of any problems (participants = 7). Being unsure was followed with concerns about identity theft (participants = 3). One participant simply casually mentioned it as part of a response with no further explanation as to why it might be applicable. The other mentioned that she might be redirected off the Facebook site where someone could attempt to steal her password. Another said that people are posting too much public information that could be consumed by others and result in a compromised identity.

Other miscellaneous problems included copyright violations, where the participants specifically mentioned someone profiting from remaking well-known games such as Scrabble. In addition, a concern that people would be able to make themselves appear to be a younger child rather than an adult. Malfunctioning applications, malicious applications, and concerns of SPAM where also mentioned once each.
4.2.3 Privacy

Participants said they desired being able to know what new information is exposed as a result of using an application. Many applications are quizzes, for example, to determine what type of beer or cartoon character people are most like. Participants using such a survey application can give others more information about themselves than they would be comfortable with sharing. It is very important to note this is not a concern about profile data being given to the application or its developers, but rather about additional information flows within their social spheres generated as a result of an applications use.

P8: “[Surveys contain] what attributes you are looking for potential boyfriend, girlfriend, you know I really don’t want everybody to read that.”

Only one of our participants was concerned with an application built with the purpose of maliciously collecting information about himself. This participant thought the way such an attack would be executed would include someone sending him pictures of a woman and starting a conversation in which he would divulge his personal information. He was not in any way referring to the automated collection of his profile data as a result of having authorized the application.

In general, participants’ concerns stemmed from the social interactions that they participated in online, and managing identity and impressions appropriately through applications. They were largely unaware of privacy dangers due to data sharing with applications.

4.2.4 Who Gets Data

We administered a survey (described in the next section) in which we asked participants to select which attributes they would be willing to show applications and indicate their understanding of what was already shared. When we asked participants why they indicated that they were willing to share each of these items they usually responded by saying that these items generally did not say too much about who they were. The information was not considered very personal. We also asked participants several questions including whom they envisioned they were giving this information to when they gave it to applications. It was clear from the responses that users were not very sure.

Participants said that they would be giving personal information to friends, businesses, and developers. The most cited group participants said would be receiving information is their friends (participants = 5).

P5: “Well I mean based on my privacy settings I think my profile is limited view, so only my friends.”

Others felt the same way believing that only friends and possibly friends of friends would be given access to their data through the applications.

Some believed that Facebook would be using this information for advertising on Facebook. They believed that some companies would then be given this information in order to solicit them for products or services (participants = 3). Most seemed to view this in a strictly professional light, even citing that this information would not be used for identity theft. This point of view is itself paradoxical. Indeed, if Facebook is giving the information to applications why would it need to re-consume the data to provide ads? We believe this demonstrates users’ lack of a mental model for data sharing and data flows on these platforms.

Three participants believed that the information would be given to the developers of the application (participants = 3). Even then however, two of those participants mentioned that this information would be used to keep the application running and was “mostly computer generated stuff”. Thus, the many participants who indicated in the survey that data was being shared, did not have an accurate conception of who data is being shared with.

5 Survey Results

In addition to the 15 participants we recruited for the interview/survey, we invited another 11 participants from another study to complete just the survey. One participant did not fill out all the questions completely so their data was discarded. The remaining participants were predominantly female (15) and ages 18-25 (23). Using Westin’s 2003 classification criterion [13] we separated our participants into groups of fundamentalists (7), pragmatists (17), and unconcerned (1), although we found no differences in response based on this classification.

The survey asked participants to use a series of 7-point Likert scales to answer whether they thought each profile attribute was shared with applications they had authorized. After answering this series, we then asked if they thought applications’ friends had authorized could see the same data using the same 7-point Likert scale. The Likert scale indicated that a value of 1 meant that the attribute was definitely not shared, a value of 4 meant they did not know, and a value of 7 meant they definitely knew it was.

For the purposes of reporting in Table 1 we grouped responses of 1-3 into one category of no, for responses of 4 we left the category as did not know, and for 5-7 we categorized as yes. The table
has been sorted by no responses, ascending for applications that the participant has installed on the profile. For applications the user has installed the answer should be yes 100% of time, provided the information is filled in on their profile. None of our participants responded correctly for all data. Data sharing for friends’ applications depends upon the user’s application privacy settings. We viewed the settings for the 15 interview participants and 13 had default open policies, indicating that their data would be shared with any friends’ applications. Thus, the correct answer is not 100%, but should still have a high percentage of yes responses provided the information is filled in on their profile.

We can see from Table 1 that participants generally agree that their name and picture are being shared with applications they have authorized. After these two attributes we see a large increase in the number of participants who specified that they do not know. There are two exceptions to this, current location and photo albums. In both cases, participants are often wrong, with many who did not feel or did not know the data fields are being shared with applications.

Table 2: Differences in Perception for Disclosure to Applications

<table>
<thead>
<tr>
<th>Applications</th>
<th>I Installed</th>
<th>Friends Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>6.12</td>
<td>1.433</td>
</tr>
<tr>
<td>Birthday</td>
<td>5.08</td>
<td>2.722</td>
</tr>
<tr>
<td>Work History</td>
<td>3.96</td>
<td>2.491</td>
</tr>
<tr>
<td>Events</td>
<td>5.08</td>
<td>2.159</td>
</tr>
<tr>
<td>Education History</td>
<td>5.08</td>
<td>2.308</td>
</tr>
<tr>
<td>Relationship Status</td>
<td>4.72</td>
<td>2.441</td>
</tr>
<tr>
<td>Significant Other</td>
<td>3.72</td>
<td>2.475</td>
</tr>
</tbody>
</table>

Table 2 reports the average score for each attribute. In this table, we see that in most cases participants felt less sure that data is shared with friends’ applications than their own. For example, more participants perceived that their hometown, status, about me, education history, and information about their significant other was given to applications they had authorized than applications their friends were using. It should be noted that the default policy protects information about who the user’s significant other is from friends’ applications (in summer 2008). However all other attributes in Table 2 are not protected by the default policy, which was employed by 13 of our 15 interview participants.

We also asked participants to specify which attributes they would be willing to share with applications. The results are shown in Table 3. We can see that participants were almost universally willing to share their name and profile picture. This reflects current practices in Facebook applications. Many also were willing to share their education history. Since most of our participants were of the college age and using their university email in order to sign up for Facebook was a requirement, this may have impacted their willingness to share educational history.

There are still some troubling findings. First, participants do not have the correct mental model of information flow for applications. As such, it is highly likely that they are not referring to sharing these attributes with developers, but rather with other users. Still, there are many attributes that participants are unwilling to share. So even though they do not understand how far the information is being spread, they still do not want complete disclosure. This clearly does not match their behavior or the platform’s design. Second, a few fields users are willing to share are particularly sensitive for security, namely their birthday and hometown. Again, users may believe they are only sharing these with friends, or may not realize the risks in disclosing these data fields.

6 DISCUSSION

Our results identified several important perceptions of social application usage that we now summarize:

- The use and perceptions of social applications are primarily driven by social interaction.

Participants of our study used applications for several purposes, reflecting the general goals of social network site use [3, 4, 11]. Some applications were used for identity management, to share additional information, affiliations, or interests. Others simply relieved temporary boredom and filled time. Yet interaction with others was still key for most successful applications. Users mentioned many different ways they are interacting with other users, including challenging them, communicating with them, playing games, and strengthening their ties by sending virtual gifts back and forth. Participants’ most favored and most used applications were those that generated repeated interactions with others. Thus, applications on social network sites are truly social in nature and interaction through the social network is driving the spread and use of applications.

The concerns that users do have about privacy are also based around interaction with others, similar to the general privacy concerns with overall social network site usage [22]. Thus users were concerned with monitoring and controlling the flow of information to the social network to further manage their identity.

- Users do not realize they are sharing so much information with applications, and do not wish to do so.

Our interviews and surveys made clear that users do not realize they are sharing so much personal information. This lack of awareness is driven by the expectations that are created by the application platform. For example, particular parts of the user’s profile such as name, picture and friends are commonly used within applications to customize them towards the user as well as provide the application with a way of communicating and interacting with the users’
friends. Users can actually see that information flow within the application itself. As a result, most expected that this information can be accessed and were comfortable with that. Yet all potential data accesses were not visible and thus not understood.

The survey and interviews indicated that users do not wish to share all their data. They only consent to sharing because it is impossible to interact with others using applications without doing so. Users did assume additional information is shared and are indeed informed of the data sharing every time they access a new application (Figure 1). This warning does not seem to be influencing their mental models. We believe this highly relates to previous findings within the phishing domain, where users are more focused on their primary task than that of privacy or security [5]. As such, the screen warning of data sharing is simply skipped as something the user must do in order to accomplish their primary goal. Thus, relying on dialogue boxes and warnings is likely not sufficient to inform users of the data sharing.

Unfortunately for users who do read the warnings and notices and attempt to understand their content, they may still arrive at an incorrect model. For example, if they were to remove an application on Facebook they will see Figure 2. This warning clearly states that by removing the application it will no longer have access to their profile data. This is simply not true since if a friend has the application authorized it may still query the users’ data. While this is a very site specific observation, it underscores the need for a consistent interface that helps to build an accurate mental model. This leads to the next perception problem:

- Users do not realize that they are sharing so much information to the applications of their friends.

Users are completely unaware of the privacy dangers that the media and security community have identified, that of third party developers having access to so much information:

- Users do not realize that they are sharing information with third party developers outside of Facebook.

These misconceptions have important implications. Users shape their behavior by their perception of the social context [14]. Without a clear understanding of how information is shared, users can not weigh the risks and rewards of application usage and behave as desired. Users’ underlying trust and motivation gained from their friends’ application use, combined with their lack of understanding about the data flows, leads users into a very dangerous situation. There is a potential for a malicious application to quickly spread and harvest a large amount of valuable user data. Facebook tries to stop such harvesting by limiting the number of requests an application can make. However, this limit appears to be based on user “affinity”. All an application must do in order to spread quickly is create an entertaining experience with frequent interaction with others. This creates a type of herding which leads others to add the application as well. Ironically, this behavior increases the number of calls the application is allowed to make as it spreads.

Our findings help explain user behavior and motivate the need to take a different approach to the design of privacy mechanisms on a social network site application platform. Our results indicate that platform changes or new tools are needed that reflect our results:

1. Social applications and privacy mechanisms for them need to reflect the social needs and motivations driving application usage.

2. Application platforms need to provide users with more control over the flows of information between users and their friends and developers.

3. Application platforms need to provide users with more accurate mental models of the sharing that occurs, both with their friends and with developers. Users need to understand all parties involved in the sharing of profile information.

External pressure has added to the haste in which changes must be made. In mid-2009 Canada’s Privacy Commissioner objected to several of Facebook’s practices including the third party use of user data described here [16]. Facebook agreed to address the disclosure of information to third party applications by giving users more control. This access control seems needed as simply restricting the platform from releasing all information is in direct contradiction with the needs and motives of both Facebook and its users. For example, horoscopes are popular, but could not operate without a user’s birthday. Still, it is not trivial to properly determine the least amount of information necessary in order to perform a task and balance privacy needs against the social benefits of individual applications.

Our results, however, indicate that currently proposed solutions do not adequately address the misconceptions we uncovered. For example, our recent study [2] examined behavior that occurred when the user was provided with fine grained access control for social applications. The proposed solution did attempt to address the 3 guidelines outlined above with an interface to improve the user’s mental model by presenting the concrete information to be shared, including information from a random friend, and allowing the user to limit disclosures to individual applications. The result of which led some users to take steps in order to protect their information. However, a significant number of users still did not, even in scenarios that were created to appear malicious.

Our results help explain this behavior. While this proposed access control interface improved the transparency of information flow, it still did not convey who the third party is and the risks of sharing information outside of Facebook. Thus, simply adding fine grained access control is not sufficient. The application platform needs to make all data flows transparent so that users can build accurate mental models to make informed privacy and sharing decisions. And as we have already observed on Facebook and in other security domains such as phishing, warning dialogue boxes and messages are likely to be ignored. Instead, users build their mental models through interacting with applications. We believe how to accurately convey such data sharing conceptions is an open and challenging problem that we hope to investigate in the future.

While we focused on Facebook for this study, other platforms likely have similar uses and suffer similar misconceptions. There are two caveats to this. First the population studied on Facebook was generally in the 18-25 range and this does not represent the entire Facebook demographic. Additionally, Facebook friends tend to represent real world friends whereas other social network sites commonly foster friendships between users who have never met. Future studies might examine not only whether these findings hold
The benefits of social applications. The users’ understanding of the risks of application use and ability to reduce the risks of data disclosures, as well as improving the users’ perceptions about privacy and information disclosure. Users are interacting, competing, communicating, and entertaining themselves. And their privacy concerns are centered around sharing data with other people on the social network, with almost no understanding of the data sharing that occurs with the application developers. The end result is that there are serious risks of applications maliciously harvesting profile information, and users are not truly understanding and consenting to these risks.

The solution to this problem may lie in better integrating privacy settings into the user interface during the primary interaction tasks, rather than only during the initial installation, conveying a more accurate mental model of data sharing throughout an application’s lifecycle. We hope that our results of the users’ motivations, concerns, and naive understanding of data sharing can lead to improved platform designs, with alternative privacy and data disclosure mechanisms which provide transparent information flow. We are continuing this work by examining new access control mechanisms to reduce the risks of data disclosures, as well as improving the users’ understanding of the risks of application use and ability to take desired actions while still enjoying the added interaction and benefits of social applications.

7 Conclusion

Applications on social network sites are now ubiquitous. Users are accessing these third-party services at an unprecedented rate, yet little research has examined what users think about accessing these applications and the overall platform. Our results indicate that similar to social network site use, social interaction is driving the spread and use of applications, and coloring users’ perceptions about privacy and information disclosure. Users are interacting, competing, communicating, and entertaining themselves. And their privacy concerns are centered around sharing data with other people on the social network, with almost no understanding of the data sharing that occurs with the application developers. The end result is that there are serious risks of applications maliciously harvesting profile information, and users are not truly understanding and consenting to these risks.

The solution to this problem may lie in better integrating privacy settings into the user interface during the primary interaction tasks, rather than only during the initial installation, conveying a more accurate mental model of data sharing throughout an application’s lifecycle. We hope that our results of the users’ motivations, concerns, and naive understanding of data sharing can lead to improved platform designs, with alternative privacy and data disclosure mechanisms which provide transparent information flow. We are continuing this work by examining new access control mechanisms to reduce the risks of data disclosures, as well as improving the users’ understanding of the risks of application use and ability to take desired actions while still enjoying the added interaction and benefits of social applications.

References