MQP CEW-0901

Privacy in Online Social Networks

A Major Qualifying Project Report

Submitted to the Faculty of

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfillment of the requirements for the

Degree of Bachelor of Science in Computer Science

By

Tyler Flaherty

Professor Craig E. Wills, Advisor

Professor Daniel J. Dougherty, Advisor

Date: April 30, 2009

Table of Contents

Abstract

With over half a billion users, online social networks (OSNs) are becoming part of everyday life. However, the large amount of information shared on these networks has become a privacy concern. The privacy settings for OSNs can be difficult to understand, especially for novice users. This project investigates the privacy settings for a popular OSN, Facebook. Part of the project involves development of Privacy Helper, an application that can be run from inside Facebook and that helps users understand the intricacies of their privacy settings. Statistics gathered from use of this application are then analyzed to investigate the relationship between a user's desired settings and current settings.

1. Introduction

This project aims to deal with privacy settings in online social networks, specifically Facebook. As online social networks become more popular, and more personal information is being stored on the Internet, protecting this information becomes more important. The application presented here, Privacy Helper, can be run from inside Facebook and provides its users with a more understandable representation of the privacy settings available. It presents common scenarios where the application user's information is shared with different types of Facebook users, and asks if the user is comfortable with those users seeing the information. It offers suggestions for privacy settings based on these answers. In addition, the application collects the users' answers to help characterize the relationship between a user's desired settings and the user's current settings.

1.1 Goals

There are two main goals for this project. First, I wanted to create a tool that could be used to both inform users of online social networks about their privacy settings. Second, I want measure the users' understanding of these settings.

1.2 Motivation

Online privacy is becoming more and more important every day, and with the rise of online social networks, more personal information is on the Internet than ever before. These online social networks provide privacy controls, but these controls may be difficult to understand for novice users. Also, it is not in the best interest of the companies to restrict access to the information about their network's users. From a business perspective, these companies want the information available to users so that more time is spent on the website, and more advertisements are presented to those users.

This issue is also important to college students who will soon be looking for employment. There have been numerous articles detailing the use of companies using online social networks as background checks [1,2,3]. Many users are led to believe that the information in their profile is private, and they know everyone who has access to it. However, this is not the case. For example, the default privacy settings in Facebook allow full access to the user's profile for all other users in the same network. In the case of college networks, all it takes is a single employee in a corporation who attended the same college as a perspective applicant to conduct a background check.

1.3 Roadmap

This report explores the privacy settings of Facebook, how they interact with each other, and the default settings presented to new users. Chapter 2 explores prior research in online social networks, the existing privacy related Facebook applications, and Facebook's default privacy settings. Chapter 3 formalizes these settings. Chapters 4 and 5 go on to introduce Privacy Helper, a Facebook application designed to inform users about their privacy settings. Results from the information gathered by Privacy Helper are analyzed in Chapter 6, and Chapter 7 concludes with a summary and a description of future work.

2. Background

2.1 Online Social Networks

Online Social Networks are computer networks that connect people or organizations. There is a wide range of online social networks offering a variety of services. There are networks for sharing media, such as Flickr[4] and DeviantART[5], networks for connecting college students, and networks open to anybody, such as MySpace[6] and Facebook[7]. There are networks for just about every common interest.

The most important aspect of any online social network is the relationships that users create inside the network. These relationships often allow users access to additional information about the user the relationship is created with. For example, in Facebook there are two relationships: the “friend” relationship and the “network” relationship. The “friend” relationship is stronger, as it requires confirmation from both users before the relationship is created. The “network” relationship is created between all users in the same Facebook network. These networks exist for various groups of users, such as users attending the same school, users working for the same company, or users from the same regional area. While some networks require confirmation prior to joining, others, such as regional networks, do not.

2.2 Prior Research

The paper “Characterizing Privacy in Online Social Networks” [8] discusses privacy controls for various OSNs and examines the extent to which a user will change the default privacy settings. It finds a correlation between network size and the number of users who changed the default settings. The authors find that the smaller the network is, the less likely the users are to change the default settings.

The paper “Antisocial Networks: Turning a Social Network into a Botnet” [9] talks about the possibility of creating malicious software within Facebook. Using only the Facebook provided API, the authors show it is possible to write an application that, through image-loading HTML tags and JavaScript instructions, can carry out Denial-of-Service attacks. The more users the application gets, the more powerful it becomes. They show that with the most popular applications on Facebook, it is possible to deliver an unsolicited 23 Mbit/sec to the victim.

The paper “Verification and Change-Impact Analysis of Access-Control Policies” [10] explores access control policies on a broader level that just online social networks. It presents Margrave, a software suite for analyzing role-based access-control policies.

There are also privacy related Facebook applications that already exist. One Facebook application is simply called "Know Your Privacy" [11]. On their application page they say, “Know Your Privacy is designed to show you how your data is at risk by allowing untrusted third-party applications to see your data." It shows the user all the information it can possibly gather. It shows user info, groups, events, "fan of", marketplace listings, photos, and friends. It also gives some generic advice at the end.

There is another application called “Privacy Guard” [12] that takes a different approach. It goes through all the information available to it and tries to answer commonly used "secret questions" about the user. The user tells the application if it is correct on any of it answers, and in the end the application gives a "privacy rank" to the user's profile. For example, it might say, "The Security Level of your profile is 33% better than the average FB user. Your Profile's privacy rank is 97%."

Finally, there is an application called “Privacy Protector” [12]. Essentially, the user creates a second profile within the application. If another user wants to see this information, he has to add the application, and the application only reveals the information if user grants him access.

These applications are helpful to users, but not enough. They are all focused on the information contained in users' profiles. None of these applications attempt to inform the user about the effects different privacy settings have.

2.3 Privacy Settings

Facebook's privacy settings are broken up into four main categories, Profile, Search, News Feed and Wall, and Applications. In the "Profile" section, there are options for the visibility level of various parts of the user's profile. The user can set these to no one, friends of the user, friends of friends, or people in the network and friends. There is also a "customize" option for each section that allows the user to show the profile to only certain friends, or only block certain people. The sections of the profile that have settings are the following:

Profile – This is the page itself. A user can allow access to the page, but still block most of what is on it
Basic Information - Gender, Birthday, Hometown, Political and Religious Views, and Relationship Status.
Personal Information - Interests, Activities, Favorites (music, movies, etc.) and your About Me section.
Status Updates
Photos tagged of you
Videos tagged of you
Friends
Wall Posts
Educational Information
Work Information

Next is the "Search" section which determines when a user shows up in search results, and how much information is shown. The first option is search visibility, which can be set to everyone, friends of friends, friends only, or only certain networks. The next option is the Search Result Content, which the user can use to select which of the following is shown: profile picture, friends list, a link to add the user as a friend, a link to send the user a message, and pages the user is a fan of. Finally, there is an option for Public Search Listing, which controls whether a very limited profile of the user shows up in search engines such as Google or Yahoo, and can either be turned on or off.

The News Feed and Wall section controls which user actions are broadcast to all the user's friends. Stories are published when the user edits profile information, joins a new network, or updates his Status. There are checkboxes to also include the following: remove profile info, write on a friend's wall, comment on a note, comment on a photo, comment on a video, comment on a posted item, post on a discussion board, add a friend, remove a relationship status, or leave a network. There are also options to show the stories in chat conversations, and if timestamps should be shown. Also, there is an option called "Appearance in Social Adds" which can be set to "no one" or "only friends".

The last section is for applications. Applications always have access to the user's name, network, and list of friends. The user can chose to allow or block all the other parts of his profile. There is an option to not share any information with applications, but it is grayed out unless the user has no applications added. There are also options for allowing friends to view memberships to other websites, and for allowing Beacon to post stories about the sites the user has been to. Beacon is the controversial "feature" that follows the user everywhere on the Internet, and reports the user's actions back to Facebook [15].

It was also important to note the default values for all of these settings. After creating an additional account, I went directly to the privacy settings and noted what was there. In the profile section, the settings for basic information and personal information was set to "my networks and friends" which means that anyone the user is friends with or anyone in a network with the user can see all the information. Contact information was slightly different. All the options were set to "friends only" except for website, which was set to "my networks and friends."

In the search settings, search visibility is set to "everyone." This is an important setting because it means that the user will be in the search results if the words being searched for are anywhere in the user's profile. For example, if a user listed "Who Framed Roger Rabbit?" as a favorite movie, that user would show up in the results for a search on "Roger" for anyone on Facebook. For the search result content, profile picture, friends list, add as friend, send a message, and pages the user is a fan of were all checked to be displayed.

In the News Feed and Wall section, all of the possible actions are set to be shown in the news feeds of the user's friends. This means that whenever the user removes information, writes on a friend's wall, comments on a photo or video, adds a friend, removes a relationship, or leaves a network, all of the user's friends will see a little notice informing them of the change. Also in this section is the setting for the user's appearance in social ads and is set to "friends only." This means that the information in the user's profile affects the types of advertisements that appear to the user's friends.

In the last section, Applications, is the option to limit what types of information friends of the user can see through applications. By default, all parts of the profile are allowed except for relationship information and religious views. This section also has an option to turn Beacon on or off, and is on by default.

The four main privacy categories are important because they are all independent of each other. For example, suppose a user changed the settings in the Profile section so that only friends of the user could see the information. This change does not affect what data is visible through searching. With the default search settings, the user would show up in the results for a search on any words contained in the user's profile by any other user on Facebook. It is this type of situation that my program will deal with.

2.4 Default Settings

The following list describes the default settings for a newly created Facebook profile. In general, these settings allow anyone to search for the user, but only friends and members of the same network can see the profile.

Profile Settings

Basic

Profile, Basic Info, Personal Info, Status Updates, Photos Tagged of You, Friends, Wall Posts, Education Info, Work Info

All set to "my networks and friends"

Contact Information

Screen Name, Mobile Phone, Other Phone, Current Address, Website, Residence, Email

Everything is set to "only friends" except for website, which is set to "networks and friends"

Search Settings

Search Visibility (who can find you through search)

Set to "everyone"

Search Result Content

Profile Picture, friends list, link to add as a friend, a link to send a message, pages I am a fan of

All selected

News Feed and Wall

Actions Within Facebook visible to friends

Remove Profile Info, write on a friend’s wall, comment on a note, comment on a photo, comment on a video, comment on a posted item, post on a discussion board, add a friend, remove relationship, leave a network

All turned on by default

Appearance in Social Ads

“Facebook occasionally pairs advertisements with relevant social actions from a user's friends to create Social Ads. Social Ads make advertisements more interesting and more tailored to you and your friends. These respect all privacy rules. You may opt out of appearing in your friends' Social Ads below.”

Set to “friends only”

Applications

What Other Users Can See via the Facebook Platform

“You can use the controls on this page to limit what types of information your friends can see about you through applications. Please note that this is only for applications you do not use yourself”

Everything turned on except relationship information and religious views

Beacon Websites

Allow Beacon websites to post stories to my profile

Turned on by default

2.5 Summary

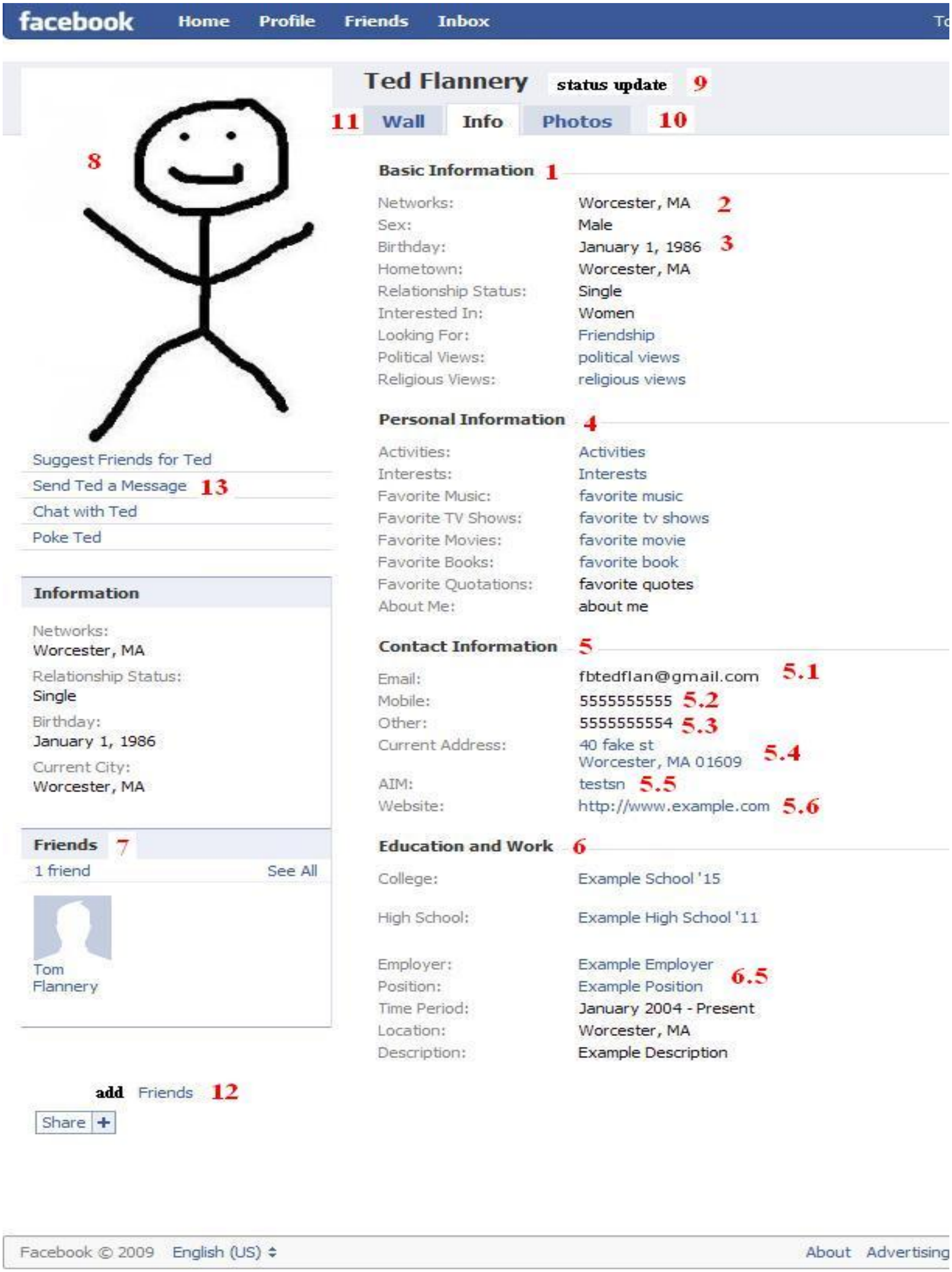
As this chapter has shown, the Facebook privacy controls are fairly complex. As prior research has shown [8], users often provide personal information without knowing exactly who has access to that data. Additionally, many users do not change their privacy settings from the defaults, which in the case of Facebook, are quite permissive. There are currently no tools for informing users of the impact of their settings.

3. Privacy Policy Rules

In an attempt to fully understand the intricacies of the Facebook privacy controls, I have written policy rules for the various settings. Below is a list of the most important privacy settings (the ones that directly affect visibility of information).

- A. Profile
  - B. Basic Info
  - C. Personal Info
  - D. Status Updates
  - E. Photos
  - F. Friends List
  - G. Wall Posts
  - H. Education Info
  - I. Work Info
- Contact Information
  - J. IM Screen Name
  - J. Mobile Phone
  - K. Other Phone
  - L. Current Address
  - M. Website
  - N. Email Address
- Search
  - O. Search Visibility
  - Search Result Content
    - P. Profile Picture
    - Q. Friend List
    - R. Add Friend
    - S. Message
- T. Birthday

Below is a screenshot of an example Facebook profile. The different pieces of information are labeled with numbers.



Ted Flannery status update 9

Basic Information 1

Networks:	Worcester, MA 2
Sex:	Male
Birthday:	January 1, 1986 3
Hometown:	Worcester, MA
Relationship Status:	Single
Interested In:	Women
Looking For:	Friendship
Political Views:	political views
Religious Views:	religious views

Personal Information 4

Activities:	Activities
Interests:	Interests
Favorite Music:	favorite music
Favorite TV Shows:	favorite tv shows
Favorite Movies:	favorite movie
Favorite Books:	favorite book
Favorite Quotations:	favorite quotes
About Me:	about me

Contact Information 5

Email:	fbtedflan@gmail.com 5.1
Mobile:	5555555555 5.2
Other:	5555555554 5.3
Current Address:	40 fake st Worcester, MA 01609 5.4
AIM:	testsn 5.5
Website:	http://www.example.com 5.6

Education and Work 6

College:	Example School '15
High School:	Example High School '11
Employer:	Example Employer 6.5
Position:	Example Position
Time Period:	January 2004 - Present
Location:	Worcester, MA
Description:	Example Description

Information

Networks:
Worcester, MA

Relationship Status:
Single

Birthday:
January 1, 1986

Current City:
Worcester, MA

Friends 7

1 friend See All

Tom Flannery

Facebook © 2009 English (US) ⬍ About Advertising

From here, I have listed all the numbers from the Facebook profile, followed by the letters that designate the settings that affect them.

1. A, B
2. (always visible)
3. A, T
4. A, C
5. A
    - 5.1 A, N
    - 5.2 A, J
    - 5.3 A, K
    - 5.4 A, L
    - 5.5 A, J
    - 5.6 A, M
6. A, H

6.5 A, I

7. A, F, Q
8. A, O, P
9. A, D, O
10. A, E
11. A, G
12. O, R
13. O, S

3.1 Datalog Rules

Datalog is a logic based database query language [17, 18]. It is useful for creating policy rules because of the facts and rules that one can create with the language. Both facts and rules are represented as Horn clauses. They are in the form of

L0 :- L1, … , Ln

where L_0 is only true if L1 through L_n are true. Facts contain only the left hand side (they are always true), while rules require both a right and left hand side.

Using the lettered settings from the previous section, I created Datalog rules. The rule:

$Access_y(profile_x)$:- sameNetwork(x,y), A(networks and friends) can be read as “User y has access to the profile of user x if x and y are in the same network and setting A has been set to networks and friends.” I haven’t listed all of the possible rules, only the interesting ones. The rest of them are simply “if the user has access to the profile and the piece of information is set to be shown.”

$\text{Access}_y(\text{profile}_x)$:- friends(x,y)
$\text{Access}_y(\text{profile}_x)$:- sameNetwork(x,y), A(networks and friends)

$\text{Access}_y(\text{profile picture}_x)$:- friends(x,y)
$\text{Access}_y(\text{profile picture}_x)$:- sameNetwork(x,y), A(networks and friends)
$\text{Access}_y(\text{profile picture}_x)$:- O(everyone), P(checked)
$\text{Access}_y(\text{profile picture}_x)$:- sameNetwork(x,y), O(networks and friends), P(checked)

$\text{Access}_y(\text{networks}_x)$:- O(everyone)
$\text{Access}_y(\text{networks}_x)$:- O(networks and friends), sameNetwork(x,y)
$\text{Access}_y(\text{networks}_x)$:- $\text{Access}_y(\text{profile}_x)$

$\text{Access}_y(\text{friend list}_x)$:- $\text{Access}_y(\text{profile}_x)$, friends(x,y), F(friends only)
$\text{Access}_y(\text{friend list}_x)$:- $\text{Access}_y(\text{profile}_x)$, sameNetwork(x,y), F(networks and friends)
$\text{Access}_y(\text{friend list}_x)$:- O(no one), friends(x,y), Q(checked)
$\text{Access}_y(\text{friend list}_x)$:- O(networks and friends), sameNetwork(x,y), Q(checked)
$\text{Access}_y(\text{friend list}_x)$:- O(everyone), Q(checked)
$\text{Access}_y(\text{birthday}_x)$:- $\text{Access}_y(\text{profile}_x)$, T(show)

Translating the Facebook privacy settings into formal logic-based rules allowed me to focus on a full coverage of the settings when formulating the questions to ask Facebook users in my application. Also, with formal rules in place, one can take a more systematic approach to analyzing the impact of changing various settings.

3.2 Summary

As this chapter has shown, Facebook’s privacy controls are fairly complex. There are overlapping settings that affect access to particular information. These settings need to be handled with care to insure that no information is revealed unintentionally.

4. Approach

The goal of this application was to lead Facebook users to their desired settings as easily as possible. The first step was to discover what level of privacy the user wanted. This was done by presenting likely scenarios in which the user's information would be shared, and recording the user's reactions. The second step was to set the user's privacy controls to this desired level. This proved to be more difficult than determining what settings the user wanted.

The first approach was to have the application change the privacy settings for the user. Using the API methods, the application would change the settings without requiring the user to look through the privacy controls. However, this was a naïve approach. The Facebook API does not have access to this information for security reasons. It could be disastrous if a malicious Facebook application could change a user's privacy settings at will.

The next idea was to use the application to determine the privacy settings and inform the user if the current privacy settings did not line up with the desired settings ascertained from the questions. When a Facebook application makes a request for information, it makes the request as the Facebook member currently using the application. The idea was to make requests for information about other users and see what was available and what was not. However, the problem was that access to the information via this method is only affected by the user's application settings. There would be no way to tell what a user's settings were for the profile, search, and news feed sections of the privacy settings.

The final decision was to link the users to the specific privacy settings page. The application would pose scenarios to the users that were linked to specific privacy settings. After answering the questions, the users would be presented with recommendations, based on their answers, and a link to each section of the privacy controls.

4.1 Summary

After exploring the limitations of the Facebook API, I realized there was no way to determine exactly what privacy settings a user had. Because of this, I had to leave it up to the users to change their own settings. With a link to each of the privacy setting sections that opens in a new browser window, the user is able to look back at the recommendations from the application while changing the privacy settings.

5. Implementation

In this chapter, I provide a brief discussion on the details of how Facebook applications work. I go on to explain how Privacy Helper was developed from a technical viewpoint. I then present the questions asked and the responses given.

5.1 How Applications Work in Facebook

Facebook provides a platform for its users to build applications that can be run inside the social network. There are over ten thousand applications, and they have a wide variety of uses. Some applications extend the functionality of Facebook, such as allowing more than just text on a user's wall or allowing more than sixty photos in an album. Other applications offer games like Scrabble or Texas Hold'em. For whatever users want to do on Facebook, there is probably an application for it.

The Facebook platform has six core components, the API, FBML (Facebook Markup Language), XFBML (an extension to FBML), FQL (Facebook Query Language), and FBJS (Facebook Javascript). These components allow developers to create applications in much the same way they would outside the Facebook platform, while still giving them access to the information on the social network.

The Facebook API uses a REST-like (Representational State Transfer) interface. Method calls to the Facebook server are made with HTTP GET or POST requests. Facebook provides client libraries for some languages (PHP being the most common), but there are also third party libraries for many other languages, such as ASP, C++, C#, Java, Perl, Python, Ruby on Rails, and others. The API methods provide the developer the ability to access any information that the user of the application would have access to. This includes all the information from the user's profile, as well as information from other Facebook users that if visible to the application user. The API also has methods for carrying out actions on the user's behalf. There are methods for creating events and notes, uploading photos and videos, sending notifications, publishing stories, and others.

When a Facebook user registers a new application, Facebook provides two unique strings, the API key and the Application Secret, which need to be provided before the application can call any of the API methods. They also supply the user with a canvas URL. This is the URL for Facebook users to access the application. The developer associates a callback URL on the developer's server that Facebook uses to fetch the HTML for the application.

5.2 Application Development

The application was developed using the Java EE SDK and the third party Java Facebook library [14]. Facebook dropped official support for a Java API library in May of 2008. However, the library has been maintained and extended on Google Code by a handful of Facebook developers. The library is released under the MIT code license, and was last updated, at the time of this writing, in March of 2009. There is a main JSP page that displays the questions and the results to the user. In the background, there is a Java servlet that handles the majority of the processing done. This servlet connects to Facebook, sets up the questions, responses, and form HTML, and saves the user's answers. I use Java beans to store the user's answers during the session, and Facebook's data store to save the answers for the next time the application is used. The application is hosted on a remote Apache server.

5.3 Questions

The following is the list of questions used in Privacy Helper. The questions are related to certain privacy settings, in order to determine the user's desired settings. The subjects in the questions represent the different levels of relations in Facebook. A person from grade school and an unknown person represent people with no Facebook connection to the application user. The classmate represents a person in the same network as the user. The language used is as neutral as possible. For example, instead of the word “stranger”, the application says, “someone you don’t know.”

1. Someone you don’t know types your name into the search bar. Do you want this person to be able to find you?

2. Someone you knew in grade school is looking for you on Facebook. Do you want this person to be able to find you?

3. A classmate of yours is looking for everyone in class on Facebook. Do you want this person to be able to find you?

4. The person from grade school who was looking for you wants to see a list of your friends. Do you want to allow this?

5. The classmate that was looking for you wants to see a list of your friends. Do you want to allow this?

6. Do you want this classmate to have access to your profile page?

7. Do you want this classmate to have access to information like gender, birthday, hometown, political and religious views, and relationship status?

8. Do you want this classmate to have access to information like interests, activities, favorites and your “About Me” section?

9. Do you want this classmate to have access to your contact information, including email, screen name, phone number, and address?

10. Would you want the person from grade school to be able to see any parts of your profile?

11. Do you want all of your friends to see all parts of your profile?

12. You comment on a photo that a friend put up. Do you want this comment to be shown on the main Facebook page for all of your friends?

13. When a friend uses an application, do you want that application to have access to all parts of your profile?

5.4 Responses

The following list contains responses returned by the application. In brackets are the answers needed to show that response, using the numbers from the list in the previous section.

No brackets imply that the response is shown regardless of the user's answers. Multiple brackets imply that more than one set of answers can generate that response.

> A stranger and a friend from grade school both represent users that have no connection to you inside of Facebook. The person from class represents a user in the same network as you.
>
> [1-yes, 2-no, 3-yes][1-no, 2-yes, 3-yes] You cannot restrict only one of these two possibilities. You can allow anyone to find you though searching by setting "Search Visibility" to everyone, or you can restrict it to only people who are in the same network as you by setting it to "My Networks and Friends."
>
> [1-yes, 2-yes, 3-yes] You have indicated that you want everyone to be able to find you through searching. You will want to set your search visibility to "Everyone."
>
> [1-yes, 2-no, 3-yes][1-yes, 2-yes, 3-no][1-no, 2-yes, 3-no] You have indicated that you want people outside your network to be able to find you, but not someone in your network. You can allow only certain networks to be able to find you by selecting "Customize" for the search visibility setting, selecting "Some of my Networks..." in the Networks dropdown, and then checking only the networks you want to allow. However, it is impossible to block a specific network while allowing everyone else.
>
> [4-yes, 5-yes] You have indicated that you want everyone to be able to see a list of your friends. To do this make sure that "Search Visibility" is set to "everyone" and the box next to "My friend list" is checked. While you are there, look at the other options for "Search Result Content" and decide what you want or don't want to be available through searching.
>
> [4-no, 5-no] You have indicated that you don't want anyone to be able to see your list of friends. To do this, make sure that the box next to "My friend list" is unchecked. While you are there, look at the other options for "Search Result Content" and decide what you want or don't want to be available through searching.
>
> [4-yes, 5-no][4-no, 5-yes] You have indicated that you want only certain people to see your friends list. It is not possible to have different Search Result Content depending on who did the search. Your best bet is to change your Search Visibility setting to only allow people who you would want to share your friends list with to be able to search for you. Make sure that all the boxes next to information you don't want to show up in the search result are unchecked.
>
> The purpose of these questions is to determine what information, if any, you want to share with people who are in a network with you, but not friends with you.
>
> [6-yes, 7-yes, 8-yes, 9-yes] You have indicated that you want everyone in your networks to see the majority of your profile. You will, at least, want the dropdowns next to Profile, Basic Info, Personal Info, and the dropdowns under the "Contact Information" to read "My Networks and

Friends." However, if there is other information that you don't want to share with everyone, make sure that dropdown box reads "Friends only."

[6-no, 7-no, 8-no, 9-no] You have indicated that you don't want to share any of your information with people in your network. To do this, you will want all the dropdown boxes to read "Friends Only." Don't forget to click on the "Contact Information" tab and change those dropdowns as well.

[6-9 not all yes or no] You have indicated that you want to hide some parts of your profile from the entire network. To do this, you will want change the dropdowns next to any information that you don't want to share to "Friends Only." Don't forget to click the "Contact Information" tab and change those dropdowns as well.

[10-yes] You have indicated that you want some people without any connection to you inside Facebook to see information in your profile. To do this, change any of the dropdowns for information that you want to share to "Everyone". Be very careful with this setting, as it opens the information up to over 200 million people.

[10-no] You have indicated that you don't want to share information with people who have no connection to you inside Facebook. To do this, make sure none of the dropdowns read "Everyone."

[11-no] You have indicated that you don't want to share all the information in your profile with all of your friends. To do this, select "Customize" in the dropdown next to the information you want to hide. Then, at the bottom, under "Except These People", enter the names of any friends that you want to hide this information from.

[11-yes] You have indicated that you want to share all of your information with all of your friends. This is the default for Facebook, so no changes must be made.

[12-no] You have indicated that you don't want your comments to show up in your friends' "Recent Activity" section. The example only mentioned photos, but there are also settings for posting on walls, commenting on other types of media, changing relationship status, removing profile info, and adding friends. Uncheck all the boxes next to activities that you don't want broadcasted to all your friends.

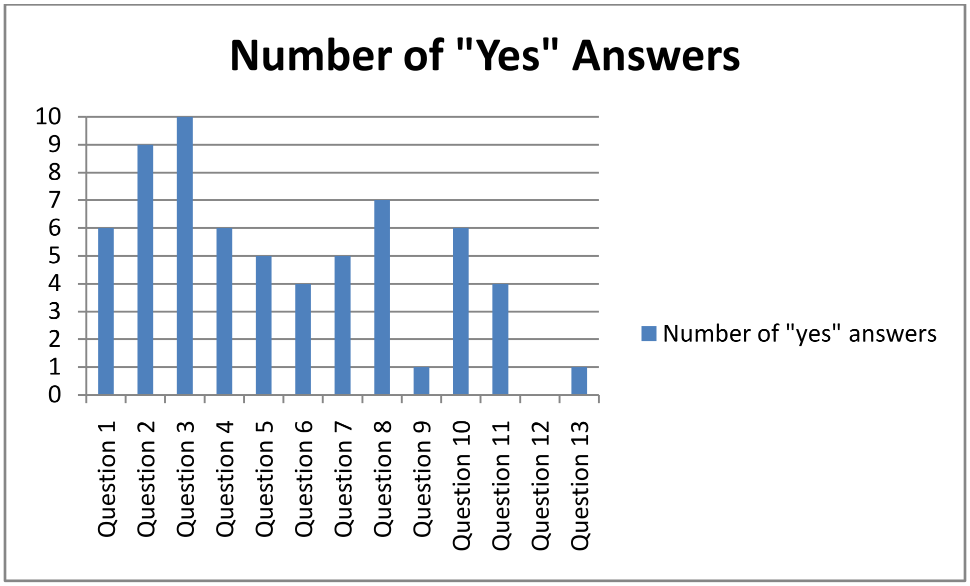
[12-yes] You have indicated that you don't mind your comments being shown in the "Recent Activity" section for your friends. Check any boxes next to activities that you want broadcasted to your friends and uncheck and boxes next to activities that you don't want broadcasted.

[13-no] You have indicated that you don't want applications used by your friends to be able to access all of your profile. These applications always have access to your name, networks, and list of friends, but you can hide all other information by unchecking the boxes.

[13-yes] You have indicated that you don't mind if applications used by your friends have access to your profile. You will want to check all the boxes, unless there is a specific piece of information that you don't want to share.

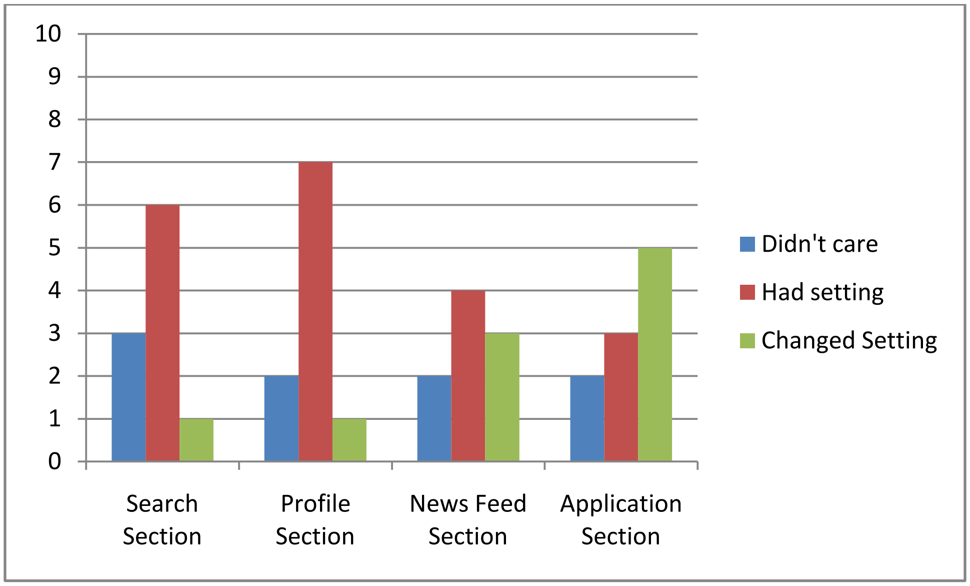
6. Results

Privacy Helper went live on April 15, 2009, and the preliminary results have been interesting. The following chart shows how many users, out of the ten so far, answered yes to each question.



It is useful to compare the trends here to the default privacy settings on Facebook. For example, question 3 asked if the user want people in the same network to find him through the search feature. All of the application users answered yes to this, and it matches the default settings. Also, only one user answered yes to question 9 which asked if the user wanted to share contact information with the classmate. Contact information is the only part of a user's profile that is shown to only friends by default. On the other hand, only 40% of the application users indicated they wanted users in the same network to see their profile. This does not line up with the default privacy setting allowing users in the same network full access. Another interesting point is that zero users indicated they wanted their comments broadcast to their friends, and half of them said they changed their settings after using the application. This implies that many users still do not know all the intricacies of Facebook privacy settings.

The responses for whether the user changed the privacy setting were also interesting.



While the majority of users had their desired settings for the search and profile sections, that dropped off quickly with the news feed and application sections. Clearly, many users do not know how information is shared through applications. It also shows that the majority of users are concerned about their online privacy. Over time, these results may become skewed as users who are curious about privacy settings discover this application. However, these preliminary results are fairly unbiased, as they came from users who were specifically asked to use the application, not users who were looking for a privacy application.

7. Conclusion

Although the numbers are small, the preliminary results have shown that not all users understand the implications of their privacy settings. Privacy Helper is proving to be a valuable tool for informing Facebook users. Over time, as Privacy Helper gets more users, the statistics can be used to show both the wide range of Facebook users, as well as the tendencies of the average user.

Future work should focus on the granularity of the privacy settings and the choices for default settings. Even the preliminary results have shown that some users want privacy settings not available in Facebook. Adding a change impact analysis to Privacy Helper, allowing users to see exactly what happens when they change a setting would also be useful. Additionally, the results have shown that there are occasions where the default privacy settings are not what the majority of Facebook users want. A study of the decisions behind the default settings, as well as a proposal for new default settings would be valuable.

8. Works Cited

1. Clark, Amy S. “Employers Look At Facebook, Too.” CBS Evening News. June 20, 2006. http://www.cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml

2. Searcey, Dionne. “Employers Watching Workers Online Spurs Privacy Debate.” The Wall Street Journal. April 23, 2009. http://online.wsj.com/article/SB124045009224646091.html

3. Balakrishna, Kanya. “Facebook Becomes Tool for Employers.” Yale Daily News. February 21, 2006. http://www.yaledailynews.com/articles/view/16696?badlink=1

4. Flickr. http://www.flickr.com/

5. DeviantART. http://www.deviantart.com/

6. MySpace. http://www.myspace.com/

7. Facebook. http://www.facebook.com/

8. Balachander Krishnamurthy and Craig E. Wills. **Characterizing privacy in online social networks**. In *Proceedings of the Workshop on Online Social Networks in conjunction with ACM SIGCOMM Conference*, pages 37-42, Seattle, WA USA, August 2008. ACM. http://www.cs.wpi.edu/~cew/papers/wosn08.pdf.

9. Elias Athanasopoulos, Andreas Makridakis, Spyros Antonatos, Demetres Antoniades, Sotiris Ioannidis, Kostas G. Anagnostakis, and Evangelos P. Markatos. **Antisocial Networks: Turning a Social Network into a Botnet**. In *Proceedings of the 11th Information Security Conference (ISC 2008)*. Taipei, Taiwan. http://www.ics.forth.gr/~elathan/publications/facebot.isc08.pdf

10. Kathi Fisler, Shriram Krishnamurthi, Leo Meyerovich, and Michael Tschantz. **Verification and Change Impact Analysis of Access-Control Policies**. In *International Conference on Software Engineering (ICSE*), May 2005. http://web.cs.wpi.edu/~kfisler/Pubs/icse05.pdf

11. Kinlan, Paul. “Know Your Privacy” http://apps.facebook.com/knowyourprivacy/

12. Zhao, Ben et al. “Privacy Protector” http://apps.facebook.com/privacyprotector/

13. Anonymous. “Privacy Guard” http://apps.facebook.com/privacyguard/

14. Anonymous. “facebook-java-api” http://code.google.com/p/facebook-java-api/

15. Perez, Juan Carlos. “Facebook’s Beacon Ad System Also Tracks Non-Facebook Users.” December 3, 2007. http://www.pcworld.com/businesscenter/article/140247/facebooks_beacon_ad_system_also_tracks_nonfacebook_users.html