

# Enhancing Privacy on Social Networks By Segregating Different Social Spheres

**Anthony Onwuasoanya**  
anthony73091@yahoo.com

**Maxim Skornyakov**  
devivos@mail.ru

**Jonathan Post**  
crispyjon@comcast.net

## Abstract

Even though users of Facebook, a popular social networking site, can segregate their friends into different “groups” and restrict information from members of certain groups, this feature is widely underused. We hypothesized that if users were forced to group their friends and had to actively choose to show information to each group, less potentially volatile information would be distributed to Facebook friends whom the user knows less well. In a usability study of 20 rising high school seniors, we forced users to group a random subset of their friends and set privacy preferences independently for each group. We found that 14 users out of the 20 only chose to only create one group, meaning that Facebook's default privacy settings accurately reflect their privacy wishes. However, 6 users of the 20 created different groups and restricted information only from certain groups. As this information is currently visible to those Facebook friends, we recommend that future social networks should emphasize features to craft different privacy settings for different groups of friends in order to help users protect their privacy online.

## 1. Introduction

In today's world, the way in which people communicate with others is much different than it was years ago. Social networking websites are becoming an integral part of teenage life. Teenagers use such websites to display their personalities to the enormous online community,

meet new people, or to simply chat with friends. Social networking websites are web-based services that allow individuals to create personalized profiles and communicate with others on the network in the variety of ways [1]

Facebook, the second largest social network on the internet, was created in 2004 [2]. Since then, it has become extremely popular with high school and college students. On Facebook, users create personalized profiles that display their real names, date of birth, education, and other personal information. Because this information is displayed publicly, privacy can be a major issue. [3, 4]

Our team would like to see from whom users restrict what sort of personal information if they are forced to group their friends. These results would be beneficial to suggesting user security improvements for social networking websites.

## 2. Related Work

Although the study of privacy on social networking sites is a relatively nascent field, there have been quite a few related works performed.

A study on Facebook privacy was performed by Jones and Soltren, two researchers from MIT. Their study involved an examination of users' privacy decisions on Facebook. To collect data, Jones and Soltren used surveys to analyze various aspects of students' Facebook usage and their concerns about privacy online. Three main flaws found within Facebook are that users disclose too much information, Facebook does not provide measures to protect

user privacy, and information about users is easy to obtain by others capable of using it for malicious acts. Like our study, the researchers used surveys to collect data and carefully analyzed users' Facebook usage and privacy settings. They also created specific recommendations for future improvements on social networking websites. [6]

Another study on the usage of Facebook's privacy settings and disclosed information was done by Gross and Acquisti, from Carnegie Mellon University. Their study analyzed the online behavior of more than 4,000 Carnegie Mellon University students on Facebook. They collected data on the types and amount of information disclosed by the users, as well as the users' understanding of how privacy settings work. Their results showed that very few students actually changed the default privacy settings and were therefore disclosing large amounts of personal information on the internet. [8]

A study performed on Facebook' interface usability was produced by Lipford, Besmer, and Watson from the University of North Carolina at Charlotte. Lipford, Besmer, and Watson examined the problems within Facebook's privacy interface. The main problem they found was a lack of an "audience view" of a user's profile after settings were modified. The lack of such a feature contributed to users displaying too much personal information to the world, because they couldn't see how others viewed their profiles. They then introduced a prototype application that solved this issue. In the end, the researchers concluded that their prototype "significantly improved the understanding of privacy settings." (5) This study was similar to ours in that it involved research on interface usability, but different since the researchers attempted to quickly solve issues by developing a prototype interface rather than studying at the broader issues and making recommendations for the future.

Aside from studies done specifically on Facebook privacy, there have been other studies performed on social networking websites and

their roles in society. Many of these works were written by danah boyd, an American social networking researcher. In her paper titled, "Social Networking Sites: Public, Private, or What?" she wrote about the importance of social networks in today's world. The paper also stressed adults' acceptance of social networks and the idea that young people's online social lives should be guided but not controlled.

### **3. Background**

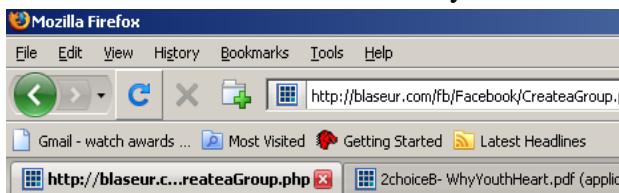
By default, all of a user's friends can see his/her full profile. This can be problematic, because people often add others as friends even though those people are not close or trusted friends outside of Facebook. [9] Also, users tend to post particularly private or possibly embarrassing information on their profiles. This information includes detailed conversations between friends, contact information, and rumors. Some unfortunate byproducts of the difficulty of privacy on social networks include: harmful persons gaining access to incriminating, or personal information; learning the location of Facebook users, and 'Facebook Stalking' – following someone through Facebook. Also, certain images can be displayed that would be suitable for viewing by friends, but not by colleagues, teachers or family members.

Due to these issues, Facebook has recently added a friend grouping feature, which allows a user to create groups of friends and restrict certain information from them. Although this feature is useful, there are many problems with its implementation. Instead of being publicly announced, the feature was quietly added. It is also not mandatory, and the privacy settings are scattered and confusing.

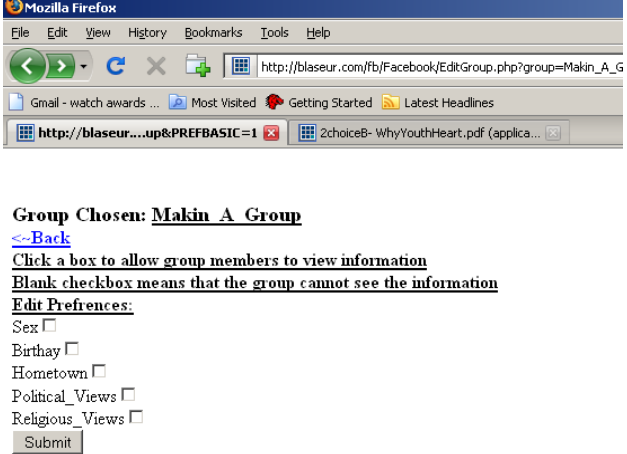
### **4. Methodology**

To evaluate how users would restrict information from certain groups of friends if they were forced to group and segregate their friends, we conducted a usability study of the friend

grouping feature. In order to study how users use Facebook's privacy settings, our team needed to monitor user privacy and group creation. We did not want subjects to have to alter their own accounts, so we designed and developed a Facebook application that mirrored Facebook's privacy and grouping interface. Our application included these five components: 1) "Show Friends", 2) "Create a Group", 3) "Add Members to Groups", 4) "Edit Group Settings", and 5) "View Group Privacy". We made two major changes from Facebook's default interface. First, we decided to include opt-in privacy settings rather than opt-out (all settings were initially restricted to created groups by default). This decision allowed people to actively choose what their Facebook friends should and should not see. Second, we made our application text based instead of visual to have the most simple interface possible and thus focus on the idea of the interface rather than the implementation. We wrote our application in PHP, a widely used web development programming language. Once the program was completed, we uploaded it to the web using Facebook's official application programming interface. Users' groups and privacy selections were added to a MySQL database, and we saved the data for analysis.



**Figure 1.** The "Create a Group" section of our test application.



**Figure 2.** The "Edit Group Settings" section of our application. Here, users can choose to allow specific aspects of their profiles to a selected group.

Our study included three main sections: a pre-survey, the actual testing of our application, and a post-survey. The pre-survey asked the volunteers about their normal Facebook usage and their familiarity with Facebook's friend grouping feature. The post-survey asked the volunteers about their comfort levels with different types of people viewing their profiles (e.g. friends, classmates, and school administrators). We performed the study on 20 volunteers. Each of the volunteers was between the ages of 16-18, was an upcoming high school senior, and had his or her own Facebook account. Thirteen males and seven females participated on our study. First, we gathered volunteers by passing out advertisement fliers. Once the actual study began, the volunteers were given a consent form and a pre-survey. They then tested our application by grouping their friends and selecting privacy settings, simulating a mandatory process. Next, the volunteers completed the post-survey. The data from each user was uploaded to a database, and the results were collected. Once we organized the data, we analyzed the friend groups that our volunteers created, as well as what settings they allowed each group to view. Then, we constructed graphs and looked for trends within each user's privacy settings. These trends helped us create recommendations for an improved privacy interface on Facebook.

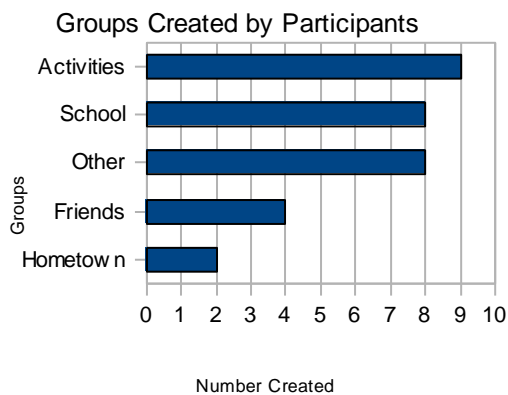
## 6. Results

### a) Previous Familiarity with the Friend Grouping Feature

In our study, we found that 35% of users were familiar with Facebook's current grouping feature and 25% actually used it. 5% found it easy to use. In terms of privacy settings, we found that the same 35% of users who were familiar with Facebook's grouping feature were also aware of the ability to control privacy settings for each group. Four out of the five users who actually used the grouping feature used the privacy controls.

### b) Types of Groups Created

Most of the volunteers created similar groups, including school, friends, hometown, activities, and others (e.g. relatives and unknown people). According to our results, nine people created activities groups, eight people created a school group, eight people created groups that fell into the "other" category, four people created a friends group, and two people created a relatives group.(see Figure 3).



**Figure 3.** Common friend groups and the number of each created out of 20 participants.

### c) Multiple Groups

Next, we looked exclusively at users who created multiple groups. 6 people (30% of our test participants) created multiple groups. The first

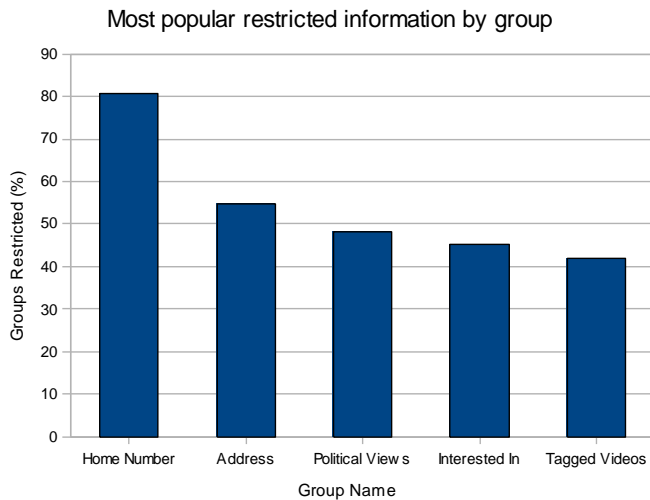
participant created one *school* group and one *other* group. The second participant created a *friends* group, a *school* group, and two *other* group. The third person created a *friends* group and two *other* groups. The fourth person created an *activities* group, an *other* group, and a *school* group. The fifth person created a *hometown* group, a *school* group, and an *activities* group. Finally, the sixth person created a *school* group and an *activities* group (see Figure 4).

Subject	Groups
1	"School", "notschool"
2	"Friends", "GovSchool", "McNair", "Relatives"
3	"Friends", "PeopleIDontKnow", "ScaryPeople"
4	"GovSchool", "Other", "Shawnee"
5	"Chicago", "GovSchool", "Neptune"
6	"School", "GovSchool"

**Figure 4.** Distribution of multiple groups among study participants.

### d) Most Often Restricted Privacy Settings

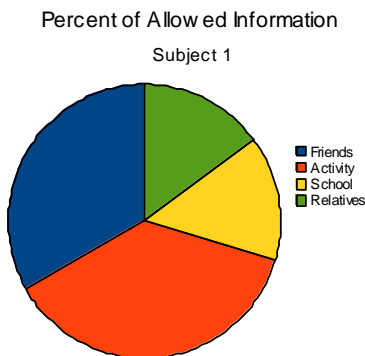
We discovered that a few areas of their Facebook profiles were restricted most often by users, indicating that these are the most volatile pieces of information in a Facebook profile. Such settings included: home number (restricted from 80.6% of all groups), address (restricted from 54.83% of all groups), political views (restricted from 48.3% of all groups), interested in – *a user's sexual orientation* (restricted from 45.2% of all groups), and tagged videos (restricted from 41.9% of all groups created by study participants). (see Figure 5)



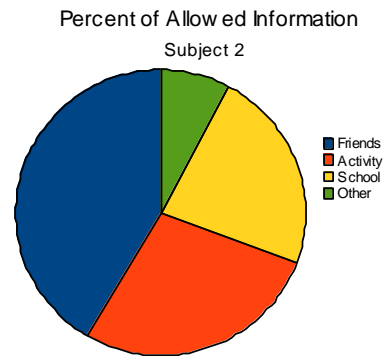
**Figure 5.** Most often restricted privacy settings.

### e) Privacy Settings in Multiple Groups

For this section, we used data from two test participants who split their friends into multiple groups. These groups included friends, classmates, and relatives. In subject 1 we found that the user restricted his phone number to everyone except relatives, his address and zip code from his “School” group, and his relationship status, tagged photos, and videos from relatives (see Figure 5). Subject 2 restricted his birthday from everyone except from his group titled “other”, his political and religious views from everyone except close friends and classmates, cell phone number from everyone except close friends, and tagged photos and videos from everyone except close friends (see Figure 6).



**Figure 6.** Percent of personal information subject 1 allowed to each group.



**Figure 7.** Percent of personal information subject 2 allowed to each group.

## 7. Discussion

We found that the most commonly created groups were “friends”, “school”, “hometown”, and “activities”. These consistently created groups existed mostly because of demographics of our participants (rising high school seniors aged 16-18). Participants grouped their ‘friends’ into groups that showed how they wanted that group to view and interact with them. Family was often not shown tagged videos or photos, because friends could upload pictures that may shatter a family’s view of its child. Instead, friends were commonly allowed to see tagged photos and videos. Strangers and others were given even less information, because the user had not built a trusting relationship with those people. The ability for a user to be able to restrict specific personal information (rather than preset configurations) is a promising idea based on trends showing that the volunteers were commonly restricting specific aspects of their contact information (e.g. address and zip code) and tagged photos and videos from everyone but those who they knew closely. The knowledge of Facebook’s grouping and privacy interface was very limited among study participants. 35 % of study participants knew about the grouping and privacy features, but only 25% actually used the feature (most likely due to a lack of advertisements on Facebook). These results also

show that in order for better user security; Facebook should probably make the features compulsory.

## 8. Future Work

For more accurate results, an increased number of subjects can be included in our surveys. Including people from more diverse age groups would also be a good idea. These additions could possibly allow for more trends in user privacy and group settings. Aside from changes in our surveys, our application could include graphical features (such as a “drag and drop” interface) for increased ease of use and simplicity. Finally, our ideas and results can be submitted to social networking and computer companies. In the future, our team would like

Facebook's privacy interface problems should also be changed in future work. We hypothesize that these changes would further spur adoption. Problems include the following:

- In order to create a group of friends on Facebook, a user must click on a link titled “Make a New List”. This link is located under Facebook's “friends” tab and is situated on the right side of the page. The link is small and blends in with the surrounding settings. This makes it hard for a user to spot, especially if the user is not aware of the feature and therefore is not looking for it. (see Figure 7)
- Once a group is created, the user is not prompted to set privacy settings for the group. This poses a problem, because the average user may not know that those privacy settings for different groups can be modified.
- To set privacy settings for a group, a user must click on a small tab at the top of the page simply called “privacy”. This can confuse a user, because the privacy tab is also used for setting privacy settings other than those for his/her groups. (see Figure

8)

- By default the available privacy settings are set to allow every person in the user's network as well as the user's friends to see every bit of information displayed on the user's profile. To change this, the user must navigate through a series of clumsy drop-down menus. (see Figure 8)
- Users are able to restrict photo albums and “tagged” photos (photos where a user is identified by a friend), but are not able to restrict their main profile pictures (main profile pictures are visible by everyone, not just friends).

## 9. Conclusions and Recommendations

Privacy on social networking sites is not perfect, though, and after analyzing our usability results we have come up with a number of recommendations for improving it. The following friend grouping and privacy interface improvements are not only recommended for Facebook, but for other current and future social networking websites as well:

- **Preset user groups**  
Since most of our volunteers created similar groups (e.g. friends, school, relatives, and activities), we believe that social networking websites should include commonly entered user groups to start out with. This would allow for quicker, easier customization. The preset group titles would not be required and would be able to be removed from the list.
- **Increased customization**  
A major recommendation for current and future social networking sites is more in-depth privacy customization. Currently,

Facebook users can only select limited privacy settings that change an entire collection of settings rather than individual settings (e.g. restricting “personal information” currently restricts the entire set of information instead of individual settings). In our study we observed trends in selected individual settings for common audiences.

- **“Opt-in” rather than “opt-out”**

Currently, Facebook uses the opt-out method for its privacy settings, meaning that all of the available group privacy settings are able to be viewed by anyone in a user's network. In our application, all of a user's settings are restricted by default, forcing the user to carefully (yet quickly) navigate through the menus and individually select which setting he/she would like a group to see. We feel that this method is more effective in user security. If this feature were to be added to pre-existing sites, every user should be notified of the change. Current users should have to re-apply their privacy settings for the sake of their security online.

### **Mandatory grouping and privacy features**

A main aspect that contributes to users

being unaware about grouping and privacy settings (aside from clear directions) is the fact that such settings are not mandatory. Making them mandatory would definitely increase user security on social networking sites, as *everyone* would need to take the time to carefully set their privacy settings before jumping into the networks. If a user has a legacy profile- a no-longer-used profile, that has not been deleted, the user should be emailed, and if the user does not log in within 30 days, the profile should be deleted for safety and storage reasons.

Each of these settings can simply be added to future social networking websites without problems. As for current social networking websites, users would need be notified about these changes in advance by email. They should be informed of the positive reasons for such upcoming features. These changes would probably cause much controversy online, but users would be much safer in the future and privacy concerns would be dramatically reduced.

### **Acknowledgements**

Thanks to:

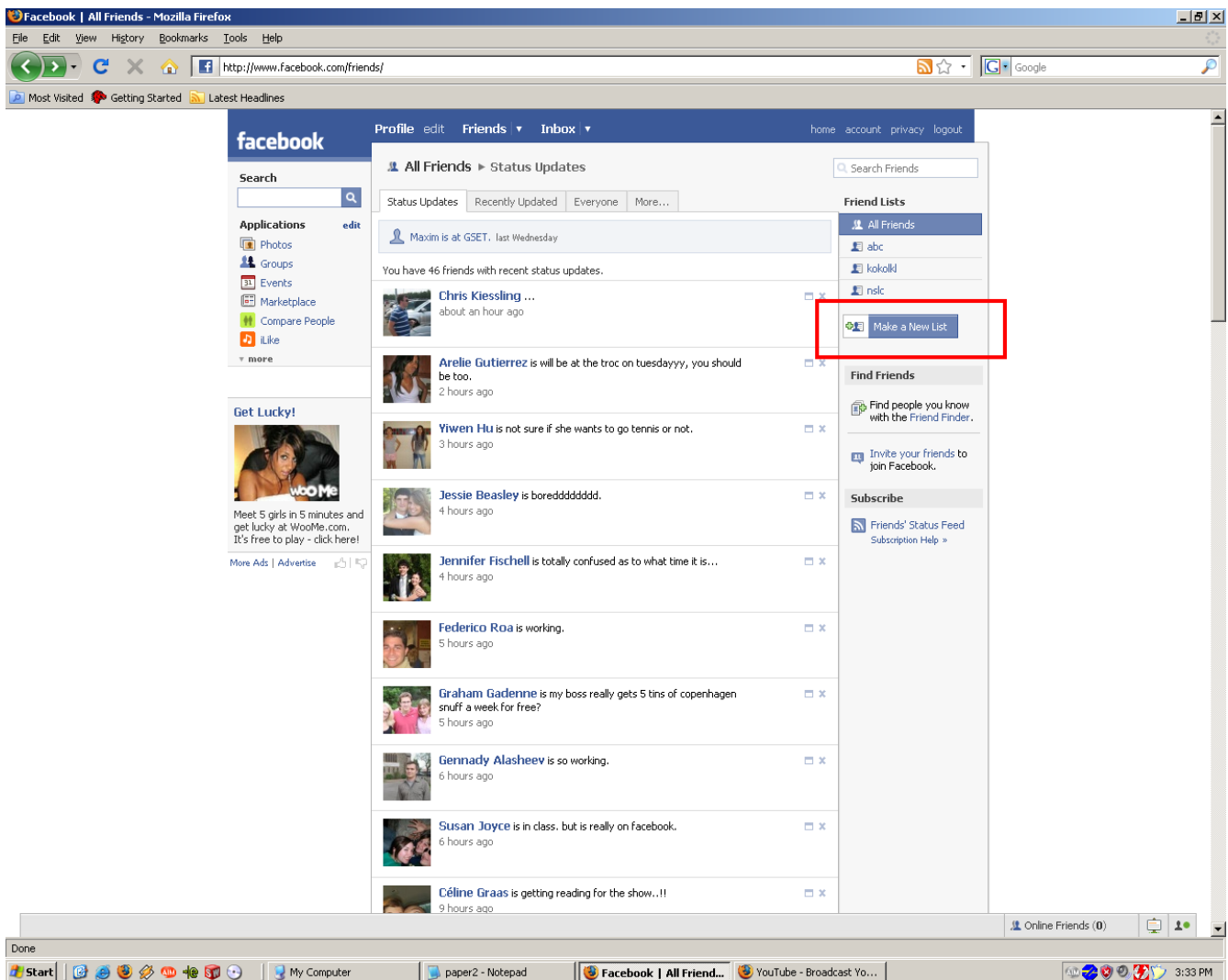
Governor’s School- Dean Brown, Blase Ur,  
The Governor’s School Board of Overseers  
Our RTA advisor Kristin

Sponsors: Prudential, Morgan Stanley, Rutgers  
University, The John and Margaret Post  
Foundation, John and Laura Overdeck,  
Colin Sidoti, and anyone else who made this project possible!

## Citations

1. boyd, d. m., & Ellison, N. B. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), article 11.(2007)
2. Yadav, S. "Facebook – The Complete Biography." August 25, 2006. Mashable.com  
<http://mashable.com/2006/08/25/facebook-profile/>
3. Kelly, S. "Identity at 'Risk' on Facebook." May 1, 2008. bbc.co.uk.  
[http://news.bbc.co.uk/2/hi/programmes/click\\_online/7375772.stm](http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm)
4. Rampell, C. "What Facebook knows That You Don't." February 23, 2008. washingtonpost.com  
<http://www.washingtonpost.com/wp-dyn/content/article/2008/02/22/AR2008022202630.html>
5. Lipford, H., Besmer, A., Watson, J. "Understanding Privacy Settings on Facebook with an Audience View."(2008)
6. Jones, H., Soltren, J. "Facebook- Threats to Privacy." ( 2005)
7. Acquisti, G., Gross, R. "Information Revelation and Privacy in Online Social Networks."ACM Workshop on Privacy in the Electronic Society (WPES) (2005)
8. boyd, danah. (2007) "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." MacArthur Foundation Series on Digital Learning – Youth, Identity, and DigitalMedia Volume (ed. David Buckingham). Cambridge, MA: MIT Press.

## Appendix



**Figure 8.** “Make a New List” feature under the “Friends” tab is small and blends in with its surroundings.

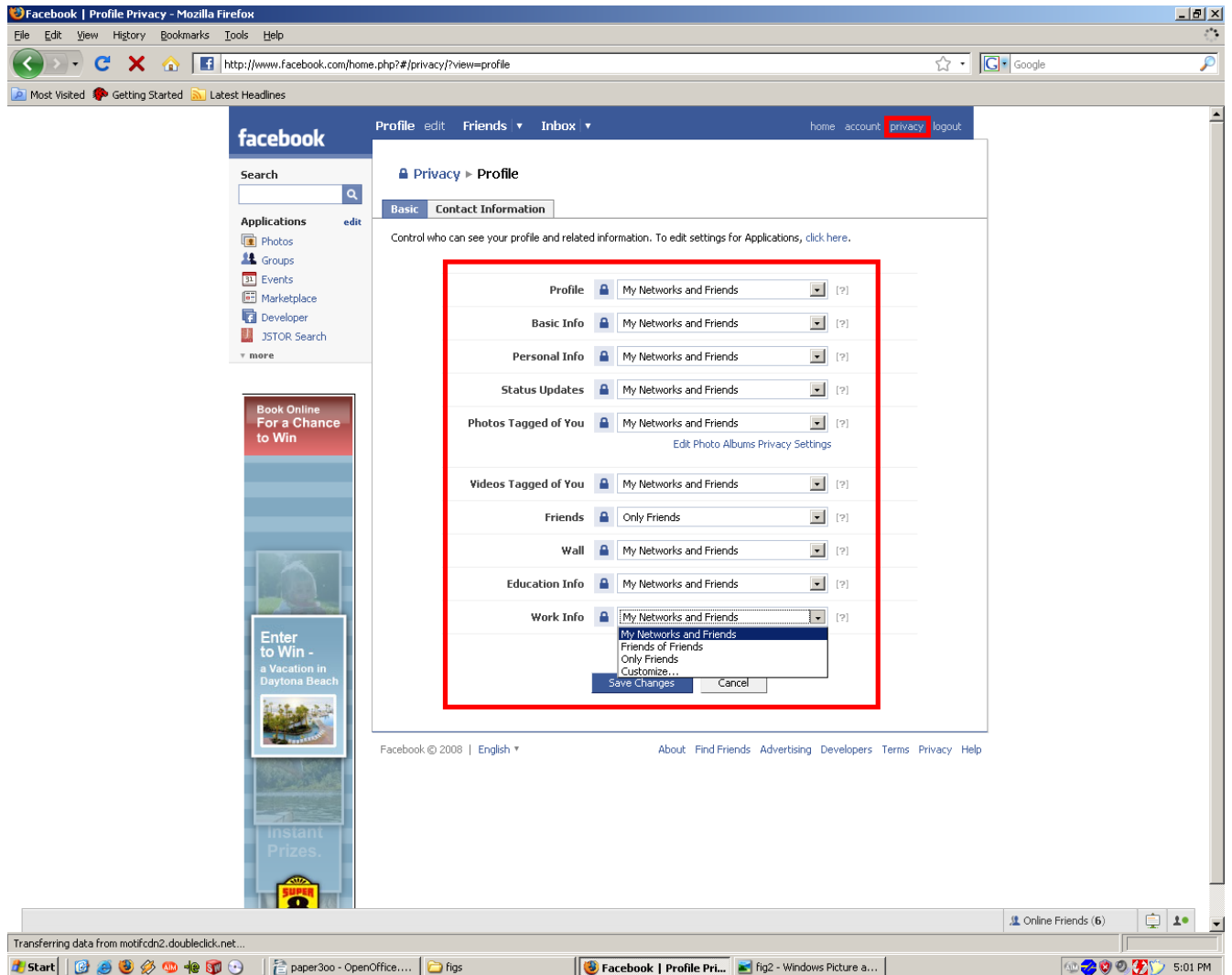


Figure 9. Small “privacy” tab and default profile privacy settings.