Student Awareness of the Privacy Implications When Using Facebook

Tabreez Govani
tgovani@andrew.cmu.edu

Harriet Pashley
hlp@andrew.cmu.edu

1. Abstract

One of the first things that a new college freshman does upon entering Carnegie Mellon University (CMU) is create a profile for themselves on *Facebook*, a popular college social network. These profiles contain pictures, contact information such as cell phone numbers and residential location, sexual and political preferences, as well as a list of "friends." Profiles are defaulted to be viewable by all *Facebook* users at your college as well as to "friends" at other universities. While *Facebook* is arguably convenient, it does present many privacy concerns.

By conducting a pilot survey of Carnegie Mellon University *Facebook* users, we investigated student awareness of these issues and available privacy protection provided by *Facebook*. We have found that most students are aware of possible consequences of providing personally identifiable information to an entire university population, such as identity theft and stalking, but nevertheless feel comfortable providing it. Despite the overwhelming majority of survey participants knowing that they are able to limit who views their personal information, participants did not take the initiative to protect their information.

We will begin our paper by explaining the background of *Facebook* and the motivations for our research. Secondly we will examine the research that has been done previously on online social networks and the *Facebook*. Next we will explain the method we used to conduct our survey and the results that we obtained. We will conclude with our evaluation of the results and possible avenues for future research.

2. Background and Motivation

With the growing popularity of online social networks, more and more personal information is being displayed on websites. This is despite the fact that privacy groups advise Internet users not to "reveal personal details to strangers or 'just-met friends" (McCandlish 2002). Privacy groups cite social consequences of risky online behavior as harassment, stalking, and spamming ("Privacy in Cyberspace" 2005). While Internet users may feel safe behind their computers, they have "zero privacy" (Regan 2003).

Facebook has become a standard part of college life. With over 60% of Carnegie Mellon students having a profile (Gross 2005), it has become an important source of information about the student population. Because the information on *Facebook* is personally identifiable, there is a risk that the information given by the user could be abused by stalkers or identity thieves (Whelan 2005). A less severe consequence is that the information posted by a student will be read by individuals the information was not intended for, like university officials or other family members (Schweitzer 2005). Information provided by students could be mined and stored for future reference. While students may not see the information they provide as a threat to their future at present, if running for a political office or if they are put in the public eye for any reason the information can be published. Information could potentially be used by future employers or the government for judgment of character.

While research has been done about the types of information posted on *Facebook* profiles and the privacy settings that users use (or don't use) (Gross 2005), it has yet to be investigated if users do not protect their information out of ignorance or lack of caring. Our main purpose in this study is to see the aftereffects of a subject taking our survey. The survey is intended to make a *Facebook* user aware of the privacy options available to them and alert them to the possible harmful consequences of giving out cell phone numbers and personal pictures to strangers. After they took the survey we looked at their profile to see if the user changed the amount of information that they provided and/or who they made the information available to. If users did change their profile then awareness is what is stopping users from changing privacy settings and giving out personal information. On the other hand, if profiles remained unchanged then it indicates that users are not concerned with protecting the information that they give out about themselves.

3. Related Work

Facebook has become a popular personals site among college students. Among freshmen at UNC, usage of *Facebook* is reported to be alarmingly high as measured by profile update statistics (Stutzman, *Notes* 2005). In the study done by Gross and Acquisti, it was also concluded that a wealth of private information including identifying pictures, birthday, high school attended, interests, and hometown were provided by a majority of users. Unlike other personals sites, *Facebook* uses full names and about 89% of names are valid (Gross 2005). In fact, *Facebook* allows users to post the most amount of information compared with *Myspace* and *Friendster* (Stutzman, *Evaluation* 2005). Gross and Acquisti pose questions of whether users overly trust the site, how peer pressure impacts information that is divulged, and how default privacy settings impact users' privacy settings (Gross 2005).

One possible answer to the question of trust comes from an article in *The Boston Globe*. "The scope of *Facebook*'s impact may not be felt for years to come" may be the case according to a professor at the University of Illinois who states that he would bet that a political candidate will get questioned about information posted on *Facebook* (Schweitzer 2005). Interestingly, political affiliation is a field that can be indicated on *Facebook.* Political trends and individual political preferences can be data-mined from the site. Stutzman demonstrates this in a comparison of political affiliation at UNC (Stutzman, *Political* 2005). Action has already been taken based on students' posts including police intervention due to sexual posts, and family members being surprised about drug posts. Students post "simple jests" and "thoughts of the moment" (Schweitzer 2005). This suggests that perhaps users trust *Facebook* too much. Users on *Facebook* can also post a link to a website. The majority of users that post a website post a page that links to other "photo, blog, or profile hosting" sites (Stutzman, *Notes* 2005). The Schweitzer article details on how users' comfort in the site may be over-sighted, but it leaves open the question of where the trust is coming from.

An article by Jessica Sidman comments on a different side of the *Facebook*. The site is much like other personals sites in that it allows a user to post a profile, search for other people, and add them as friends. It differs because, according the *Facebook* spokesperson Chris Hughes, the groups and social structure on the site model structures that are already present in a physical sense (Sidman 2005). Because of its popularity, the site received an investment of $13 million by Accel Partners (Sidman 2005). Hughes goes on to say that the site regularly receives letters saying that the site has helped users to meet old friends or solidify new significant relationships.

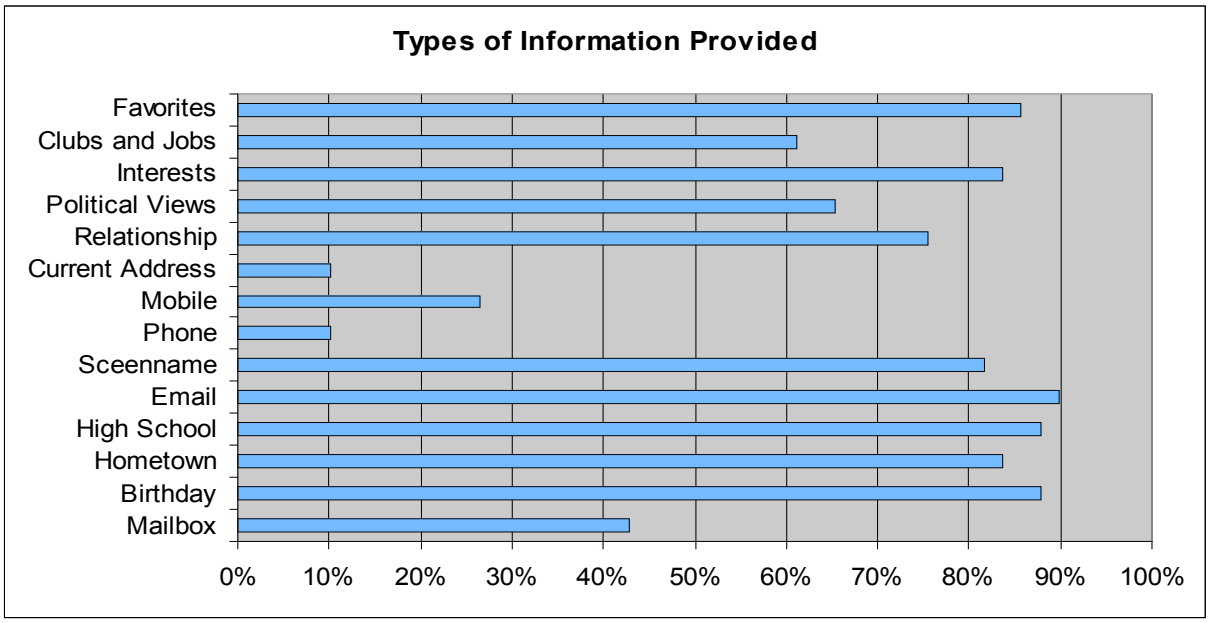
Sidman's article ends with a question about whether "online interaction helps or hinders personal interaction" and whether the addiction to *Facebook* is taking away from other elements of college and life (Sidman 2005).

Many users befriend other users "even if they are precarious acquaintances or absolute strangers" (Majmudar 2005) on the *Facebook,* but not in a non-cyber environment. Since a number of strangers whom a user categorizes as friends have access to that user's profile, there may be privacy concerns. Hughes fields questions of privacy concerns by commenting that all of the information "has been available inside university systems already" (Majmudar 2005). However, it was noted in a comparison done at UNC by Stutzman that *Facebook* prompts users to enter much more personal and social information than is asked for by the university directory (Stutzman, *Evaluation* 2005). The article by Majmudar brings up the point that users have extensive privacy options. It asks whether *Facebook* should be considered a privacy concern if it gives users options (Majmudar 2005). In answer to this question, an article by Bridget Whelan shares students' comments saying that the site has an element of "'creepiness'" (Whelan 2005) and causes fear of stalking among some students (Whelan 2005). The article notes that *Facebook* has popularized stalker like behavior and has become a popular word on college campuses. The difficulty in resisting "the overwhelming urge to anonymously check up on old high-school acquaintances" (Whelan 2005) keeps users addicted to the site and open to looking up people and sharing their information with other users. The article doesn't conclude whether the site is merely a fun resource or a privacy invasion, but it gives students' view points on both sides of the "Internet craze" (Whelan 2005).

Reasons for *Facebook*'s popularity as a campus networking tool over other campus networking tools include the depth of information that is encouraged by the site to be shared, viewable social networks, course tracking, and the ability to post messages for all users to see (Agraz 2004). There are also features that integrate into other services like linking an AIM away message to a user's profile and viewing a school newspaper article in which a user was featured (Agraz 2004). Features like these aren't available for all users, but many users that have them don't realize that supplemental information is attached to their profile (Acquisti 2005). Where to draw the line between a useful feature and an invasive feature is what researches grapple over.

4. Method

A pilot study was conducted of 50 Carnegie Mellon University undergraduate *Facebook* users of varying concentrations of study and ages (see Appendix B). Our aim was to select participants evenly distributed among the various colleges at Carnegie Mellon to ensure different levels of technological ability. Survey participants were recruited in common areas of the university to try and maintain a balanced student population. To begin, we saved a copy of the participant's *Facebook* profile before they took our survey, both from the view of a Carnegie Mellon *Facebook* user (local user) and from the view of a *Facebook* user from another university (global user). This was done to look at the different privacy settings that the participant had chosen; their profile is viewable to all *Facebook* users, only users from their own university, and to only their "friends". As the participants were not "friends" with the researchers, this could be easily tested. The survey asked about the types of information that participants are willing to reveal to other *Facebook* users and their motivations for doing so. It also asked about their



rr

Figure 1. This chart shows the percentage of survey participants that chose to provide different categories of information.

reasons for joining *Facebook* and whom they ask to be their "friends" and what criteria they have for accepting requests from other users to be their "friends." Demographic data was also collected to analyze trends once all of the data had been collected.

After the taking the survey, we looked at their *Facebook* profiles two and five days later and saved it to our files both from a local and global user perspective. We then stripped all identifying information from the 6 saved profiles and only made note of whether or not the information was provided. This was done to protect the personal information of the participants.

5. Results

5.1 Data That Users Share on *Facebook*

Users on *Facebook* can share a multitude of different types of data with others users. These types of data include contact information, personal information like gender, birth date, hometown, and school concentration, information regarding interests in movies, music, clubs, books, relationship status and partner, and political affiliation. Users can in fact choose to fill in any of this information and update their information at any time.

We found that a majority of users do provide most of this information. Our results in Figure 1 mostly corroborate the results found by Gross and Acquisti (Acquisti 2005). We found that more than 60% of CMU profiles contained a profile image, birth date, home town, AIM screenname, high school, relationship status, interests, and various types of their favorite things (books, movies, musicians, etc). It has been found that the validity of the fields provided is overwhelmingly accurate (Acquisti 2005).

From Figure 1 we can also see that the only types of information that users consistently do not provide are their mailbox, current address, and mobile and home phone numbers. These

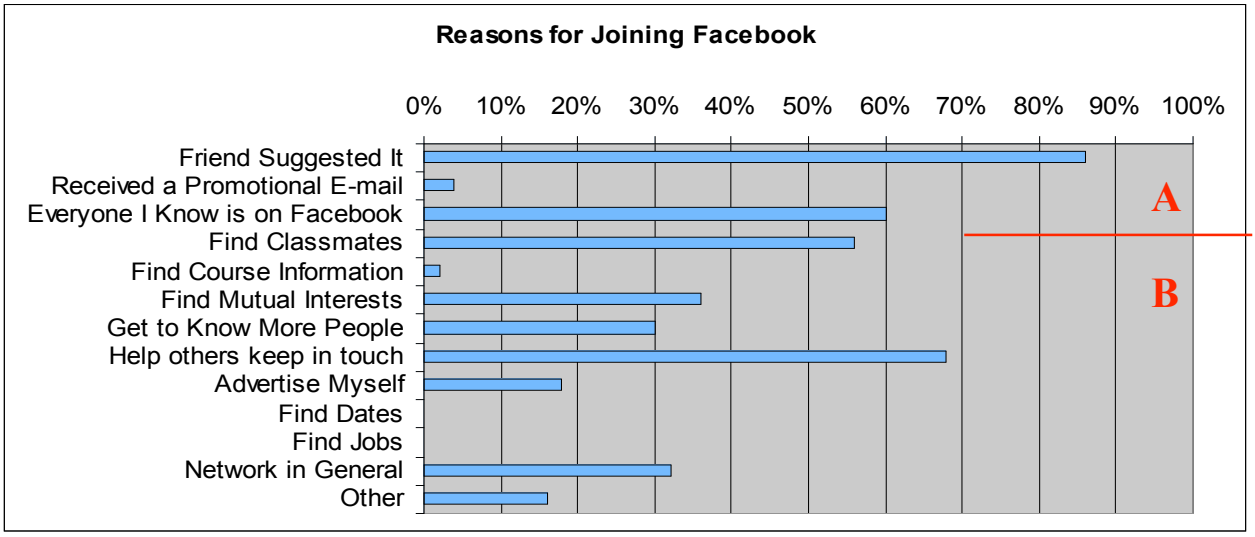


Figure 2. The red line separates the different reasons from joining *Facebook* into Category A and Category B as indicated by the different red labels.

pieces of information are probably considered to be more private and are direct way of contacting a user. They are the primary pieces of data that would be needed for identity theft or stalking. While the percentage of given cell phone numbers and home phone numbers are of the same magnitude, current addresses have a vast difference. The results from Gross and Acquisti show much higher percentages of *Facebook* users providing address contact information. They found that 50.8% of users gave their current address (Gross 2005), where as our data shows that only 10.2% provided their current address.

We believe that the similarity of phone numbers is caused by the convenience of this information. Users want their friends to be able to reach them. Users may have decided that home addresses are not needed for convenience and could be considered more personal. In general, it has been shown that Internet users are willing to reveal personal preferences online such as favorite books and movies; however they are hesitant to share their personal contact information online (Cranor et al. 1999). Our results for *Facebook* demonstrate this fact. Information relating to contact information is provided less than 45%, but all other types of information that we looked at are provided more often than 60% of the time.

5.2 Why Students Use *Facebook*

Actual *Facebook* statistics report that over five million accounts have been created and over 70% of those accounts are accessed every day (Cohler 2005). The reasons why users join *Facebook* that we explore in our survey fall into two broad categories. Category A from Figure 2 involves joining *Facebook* due to friend recommendations and peer pressure. Category B from Figure 2 relates to the usefulness of *Facebook* in meeting new people, keeping in touch, getting help in courses, finding old friends, and making new friends. Our results indicate that most students joined *Facebook* for reasons belonging to both categories. The distinction of these categories is important because the reasons in Category B suggest that those surveyed were well aware of how *Facebook* could be used and some of the advantages of using it. These users probably view *Facebook* like a social network and enhanced directory tool to aid in various

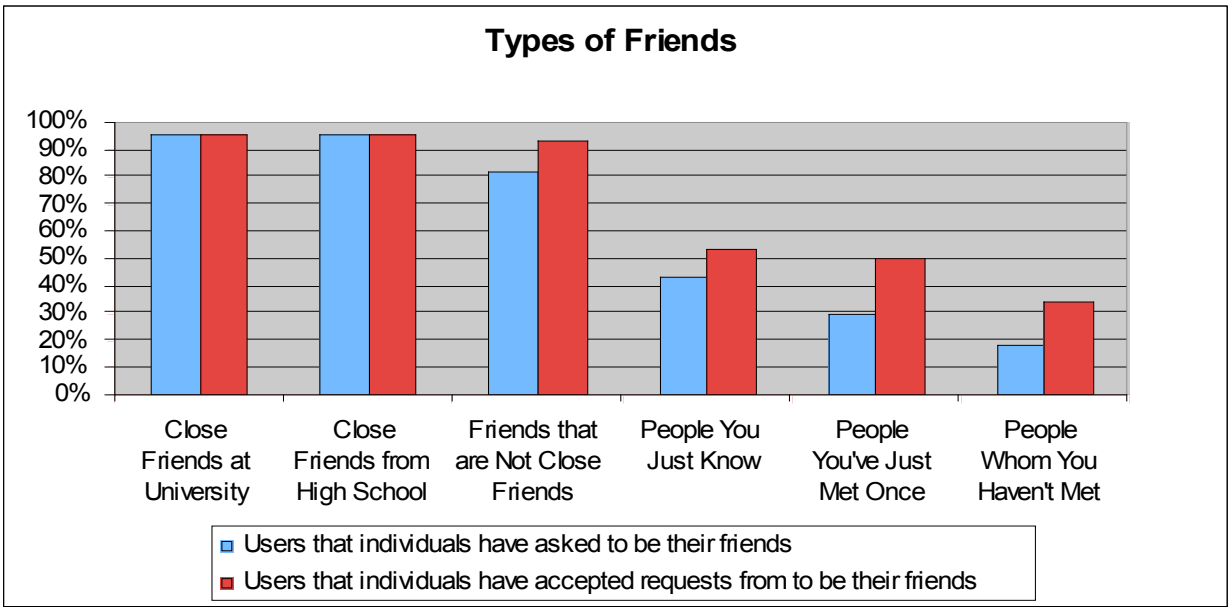


Figure 3. Graph showing the percentage of different types of *Facebook* users that surveyed participants initiated a "friend" request to and accepted a "friend" request from.

social connecting. From the reasons listed in Category A, we may be able to conclude that other influences exist besides the usefulness of the tool that encouraged users to join.

Category A responses provide some interesting questions. The choice to reveal personal information may be attributed to peer-pressure or curiosity. Because a certain student's peers and friends are users and are sharing certain types of information, that student may feel obligated to become a user. If they do not feel obligated, the student might instead have more trust of other users because of how much information others share, and therefore act carelessly when sharing information.

On the other hand, Category B also has high responses. Users of *Facebook* also joined because they hoped to make it more convenient for others to get in touch with them, find classmates, and find friends with mutual interests. High response in this category suggests that users see *Facebook* as a tool. Their decision to join was based on information about what the site can actually be used for. If users made an informed decision to join *Facebook*, then maybe they see the benefit of the information that they are sharing and they believe it outweighs the cost of a loss in privacy.

Since users provided high responses for reasons to join *Facebook* in both categories, then either analysis could be correct or it could be a combination of the above analyses. Users may be informed about what the benefits and risks are to an extent, but they could still be influenced to join and use *Facebook* based on peer pressure and because everyone else is doing it. Users may be misinformed on not only all the benefits of *Facebook*, but also some of the risks of divulging large amounts of personal information. We discuss our results as far as the use and knowledge of privacy settings in the next section of this paper.

The reasons why people joined the *Facebook* community are important in examining the reasons people share certain types of information and expose themselves to certain privacy risks.

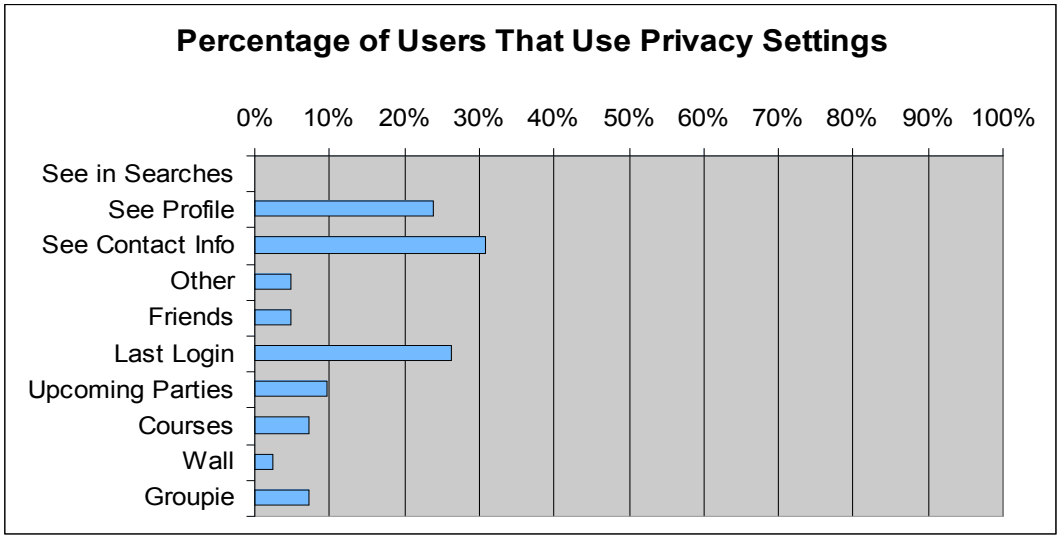


Figure 4. This graph shows the different percentages of users that chose to restrict categories of information by using the privacy options provided to them by *Facebook*'s privacy settings.

5.3 *Facebook* Privacy Settings May Be Under-Utilized.

Facebook provides users a way to restrict and specify the types of users that can view different parts of their profile. They can control who can search for them, who can view their profile, who can see their contact information, and who can see various other profile details. The types of users they can choose from to view parts of their profile are users attending the same school, just friends, and friends of friends at the same school. Friends can always view everything. For profile searches, users can allow everyone, or some subset of people to search for them. They also have the option of blocking specific people.

Because friends can always view an entire user's profile, it is important to find out how people choose their friends on *Facebook*. Those surveyed were given choices of a variety of levels indicating how much interaction they have had with users whom they befriend and accept as friends. Close friends from university and high school have been asked and befriended by 96% percent of users surveyed. Friends that are not close friends have been added as friends for over 80% of participants. 54% of participants selected that they have accepted friends on *Facebook* whom they wouldn't consider friends, 44% selected that they have asked users who aren't friends to be *Facebook* friends. Figure 3 summarizes our results. In general, participants were more lenient when accepting friends than asking other users to be their friends. We expect that friends on *Facebook* are chosen and accepted much more readily than outside of *Facebook*. Although they are referred to as friends, the trust level of *Facebook* friends may be different than the trust level of friends outside of *Facebook*. We believe that a large percentage of users may not make this distinction. The possibility exists that users do not make the best decisions for their situation as to what information to allow their friends on *Facebook* to see.

Users surveyed were also asked questions that examined their awareness of privacy settings on the *Facebook*. Specifically, we wanted to measure whether users know that they can change their privacy settings, what settings users have changed and why, whether users have read the privacy policy, and whether or not they know some of the ways that *Facebook* can use their data as stated in their privacy policy. Users rarely change their privacy settings from the default

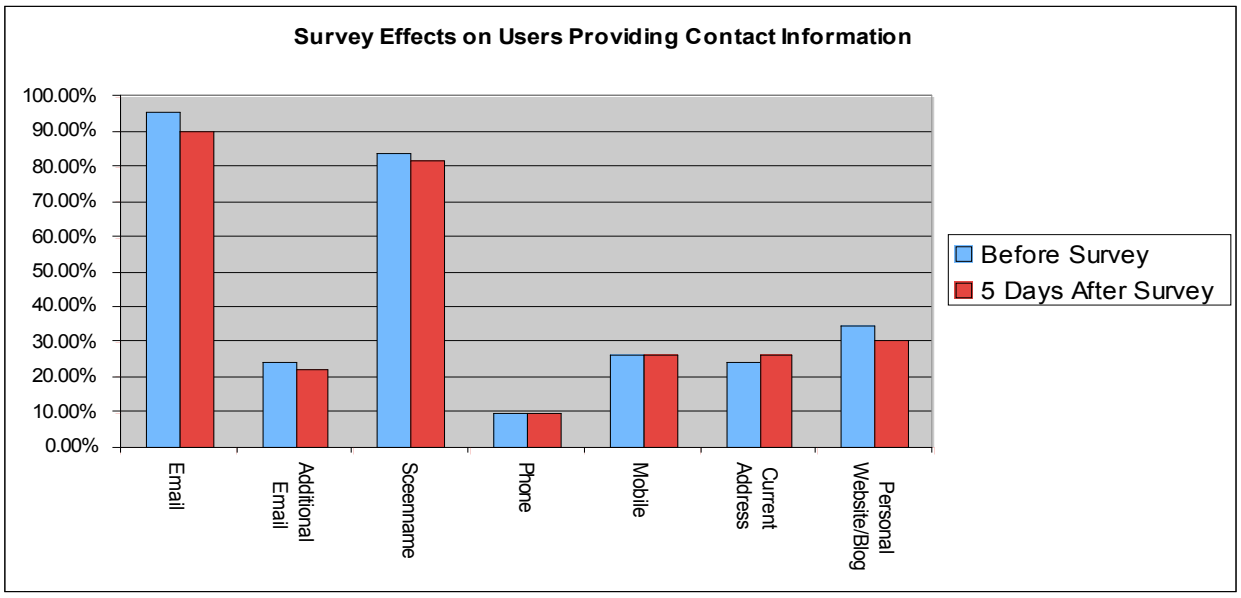


Figure 5. This chart shows the changes in the percentage of surveyed participants that gave each of the seven possible fields of contact information before and five days after taking the survey.

(Cohler 2005). Our results corroborate this fact. We found that 80% of users surveyed have not read the privacy policy. 40% of users reported that they are aware of *Facebook*'s policy on sharing data with third parties. These results correlate to what we found about the number of users who altered their privacy settings as far as the number of users who have used privacy settings.

Our results regarding how many users are aware that they can change their privacy settings compared to how many users actually have changed their privacy settings demonstrate that users are knowledgeable about their options within *Facebook*, but have chosen not to use them. 84% of participants reported that they are aware that they can change their privacy settings. Of those 84%, less than 48% have made use of the privacy settings. Figure 4 details the specific types of information that users restricted. Maybe users don't see any issue with restricting who can see the information they post and are fine with the restrictions that are provided by default. Another conclusion could be that users aren't aware of the risks of not protecting their personal information that they share. They are not fully educated about how easy it may be for a stalker to follow them or employer or parent to get a hold of what they and others post on their profile. Maybe they haven't considered how information on their profile can be used against them. This idea is suggested by articles that report consequences of information being openly available on *Facebook* (Schweitzer 2005).

5.4 Awareness Did Not Increase Privacy

One goal of administering surveys that ask users if they are aware of privacy settings and that *Facebook* can share their personal information is to make users more aware of their options. We checked each surveyed user's profile after they had initially filled out the survey. As participants listed identity theft and stalking as their primary privacy concerns, we looked at the changes in the amount of contact information provided in *Facebook* profiles after taking the survey. We found that there were minimal changes in the amount of information that survey participants

provided after taking the survey, as Figure 5 indicates. The percent decrease of users who provided their website address had the largest drop with a drop just under 12%. Additional e-mails being provided dropped by 8.33%, primary e-mails dropped 6.4%, and AIM screenname disclosure dropped by 2.44%. The amount of phone numbers and cell phone numbers remained constant. The disclosures of current addresses increased by 8.33%. Although there were some changes to the amount of information disclosed, the strong majority of users made no changes to their profile as far as reducing the amount of information in their profile. The 25-50% changes that we expected were not prevalent in our data.

This suggests that users are comfortable with how much information they share and that they may have already made an informed decision. In fact, research has been conducted that concludes "even though individuals express concerns and awareness about Internet privacy, they are still willing to engage in risky online activities" (Campbell et al. 2001). These online risky behaviors could include providing contact information such as residence and cell phone information to the entire Carnegie Mellon University *Facebook* user population. And although we only observed minimal changes surrounding our survey, our results show that most users haven't already changed their privacy settings and provide a majority of the possible data categories. Users in general haven't taken advantage of the privacy settings that *Facebook* has to offer and our survey had only a small effect in changing this.

6. Discussion

Facebook provides its users with a chance to share information and model their social networks online. Along with the benefits of making it easier to keep in touch and find out about others more easily, there are risks and concerns with sharing information with large amounts of people.

From the results that we obtained we found that overall, the majority of students were aware of the ability to restrict the amount of information they provided to different *Facebook* users. While 40% of users did restrict some of their information, there are still large numbers of users that are sharing very personal information like cell phone numbers and home addresses. The overall effect of our survey seemed to be minimal. From the surveys we conclude that *Facebook* users generally feel comfortable sharing their personal information in a campus environment. Participants said that they "had nothing to hide" and "they don't really care if other people see their information." These attitudes and behaviors will be difficult to change by merely asking students to take a survey, no matter how informational it is. We believe that it will take an unfortunate incident such as a victim of identity theft or stalking to shock *Facebook* users into being more selective about the information that they make available to other users. To substantiate our claim, a survey could be conducted on the amount of privacy settings and restriction of information of *Facebook* users based upon their knowledge of an incident of stalking or identity theft. If users have experienced identity theft or stalking, or know somebody who has, they may be less likely to share their personal information.

7. Future Work

We hope to circulate this survey to more users in the future to get a broader answer on the various questions we pose. Additionally, we can include demographic analysis to see if

demographics or technical ability correlate to awareness of privacy. Getting a larger body of participants is essential for evaluating these finer points.

Facebook has added a new service on their site dedicated to the social networks of high school students. The privacy implications of this could be quite astonishing. High school aged users may be less aware of privacy risks and less able to assess the consequences of sharing their personal data. Information from the high school site could be used in evaluating students applying to universities by admissions staff. A much larger population of students in high school are minors and therefore may be more vulnerable to issues relating to rules for minors. Examples of these issues are alcohol consumption and stalking issues. There are many questions regarding the ability of high school students to judge how sharing their personal information may impact them negatively in the future.

Another feature has recently been launched on *Facebook* that may be of interest. The photo album feature allows users to post photos of them and other users. Additionally, the users that appear in a picture can be specified and the picture can be linked off of each identified user's profile. A user can remove the tag of them on the picture by going to an individual picture and removing the tag. All pieces of information on *Facebook* where the user has a choice had been opt-in previous to this feature. There may be some interesting questions about how opt-out affects social networks. The shift to opt-out could also be a trend reflected in users' willingness to share personal information.

Examining these issues further will allow us to draw stronger conclusions and more specific conclusions to different users and different types of information. Answering more questions will give us more insight into the trends of how users view privacy and how privacy may be treated and viewed in the future.

8. References

Agraz, Diana. "Making Friends Through Social Networks: A New Trend in Virtual Communication." *Stanford.edu.* 15 March 2004. 11 October 2005 <http://www.stanford.edu/ ~aneesh/NewFiles/Dian%20Agraz.pdf>.

Campbell, J., Sherman, R.C., Kraan, E., & Birchmeier, Z.. "Internet Privacy Awareness and Concerns among College Students." *Paper presented to APS, Toronto*. June 2001. 7 Dec 2005 <http://www.users.muohio.edu/shermarc/ aps01.htm>.

Cranor, L., Reagle, J., Ackerman, M. "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy." *AT&T Labs – Research Technical Report TR 99.4.3.* 14 April 1999. 5 December 2005 <http://www.research.att.com/ resources/trs/TRs/99/99.4/99.4.3/report.htm#general>.

Gross, Ralph and Alessandro Acquisti. "Information Revelation and Privacy in Online Social Networks." *WPES '05* 7 November 2005.

Gross, Ralph and Alessandro Acquisti. "Information Revelation and Privacy in Online Social Networks." *Heinz Seminars*. 3 October 2005.

Majmudar, Nishad. "Facebook users say friendship has its limits – or ought to." *Democraticandchronicle.com*. 28 August 2005. 27 September 2005 < http://www.democratandchronicle.com/apps/ pbcs.dll/article?AID=/ 20050828/BUSINESS/508280335/1001>.

McCandlish, Stanton. "EFF's Top 12 Ways to Protect Your Online Privacy." *Electronic Frontier Foundation*. 10 April 2001. 8 December 2005 <http://www.eff.org/Privacy/ eff_privacy_top_12.html>.

"Privacy in Cyberspace: Rules of the Road for the Information Superhighway." *Privacy Rights Clearinghouse.* September 2005. 8 December 2005 <http://www.privacyrights.org/fs/fs18-cyb.htm>.

Regan, K. "Online Privacy Is Dead – What Now?" *E-Commerce Times.* 2 January 2003. 8 Dec 2005 <http://www.ecommercetimes.com/story/ 20346.html>.

Schweitzer, Sarah. "When students open up – a little too much." *Boston.com*. 26 September 2005. 27 September 2005 < http://www.boston.com/news/local/new_hampshire/articles/2005/09/26/ when_students_open_up____a_little_too_much>.

Sidman, Jessica. "In Your Facebook." *Csindy.com*. 17 August 2005. 27 August 2005 <http://www.csindy.com/csindy/2005-08-11/cover.html>.

Stutzman, Fred. "An Evaluation of Identity-Sharing Behavior in Social Network Communities." *Ibiblio.org.* 2005. 11 October 2005 <http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf>.

Stutzman, Fred. "The Freshmen Facebook Zeitgeist." *Ibiblio.org.* 2 October 2005. 11 October 2005 < http://www.ibiblio.org/ibiblog/?p=154>.

Stutzman, Fred. "Political Orientation of the UNC campus." *Ibiblio.org.* 7 October 2005. 11 October 2005 < http://www.ibiblio.org/ibiblog/ ?p=141>.

Whelan, Bridget. "Facebook, a fun resource or invasion of privacy." *Athensnews.com*. 08 September 2005. 27 September 2005 <http://athensnews.com/issue/article.php3?story_id=21491>.

APPENDIX A
Survey given to participants

Survey

Check1_____ Check2_____

Please answer all the following questions as truthfully as you can. Thank you!

Participant Identification Number: _____

1. Place a checkmark next to all of the types of information below that your *Facebook* profile accurately contains.

   __ Birthday
   __ Cell phone number
   __ Home phone number
   __ Personal address
   __ Schedule of classes
   __ AIM screen name
   __ Political views
   __ Sexual orientation
   __ Partner's name
   __ Picture of yourself

2. Briefly give a few reasons why you share the data that you do.

3. If you don't provide all the types of information from question (1) in your profile, briefly give a reason why you don't provide that information.

4. Check all of the following reasons for joining *Facebook* that apply to you.

__ a friend suggested it
__ I received a promotional e-mail and it sounded like a good idea
__ everyone I know is on *Facebook*
__ learn about and find classmates
__ find information about courses, lectures, etc.
__ find people who share my interests
__ get to know more people
__ make it more convenient for people to get in touch with me
__ show information about myself/advertise myself
__ find dates
__ find jobs
__ to network in general
__ other reason (specify)_____

5. Check all of the following types of "friends" that you have asked to be your friend on *Facebook*.

__ close friends from university
__ close friends from high school
__ friends that may not be close friends
__ people you know but may not be friends with
__ people you've met just once
__ people whom you haven't met

6. Check all of the following types of "friends" that you have accepted from "friend" requests on *Facebook*.

__ close friends from university
__ close friends from high school
__ friends that may not be close friends
__ people you know but may not be friends with
__ people you've met just once
__ people whom you haven't met

7. Are you aware that you can change your privacy settings on *Facebook*?

__ YES __ NO

If no, please skip to question 10.

8. If you have changed your privacy settings, do you remember what settings you have changed?

__ I restricted who can see me in searches
__ I restricted who can see my profile
__ I restricted who can see my contact info
__ Other: _____

For those people that can view my profile, they **cannot** see:
__ My friends
__ My last login
__ My upcoming parties
__ My courses
__ My wall
__ That I'm a groupie of groups which I know a lot of the members

9. Please explain why you changed or why you did not change your personal privacy settings.

10. Have you read the *Facebook* privacy policy?

__ YES __ NO

11. Are you aware that *Facebook* can share your information with people or organizations outside of *Facebook* for marketing purposes as per their privacy policy?

__ YES __ NO

12. If you believe that there may be a privacy risk with sharing too much information on *Facebook*, give at least one consequence of a user of *Facebook* sharing too much information.

13. How often do you login to *Facebook*?
__ Many times a day
__ Once a day
__ Many times a week
__ Once a week
__ Less than once a week

14. How often do you update your profile on *Facebook*?
__ Multiple times a week
__ Once a week
__ Multiple times a month
__ Once a month
__ More rarely than once a month

15. What is your age?
__ 18
__ 19
__ 20
__ 21
__ 22

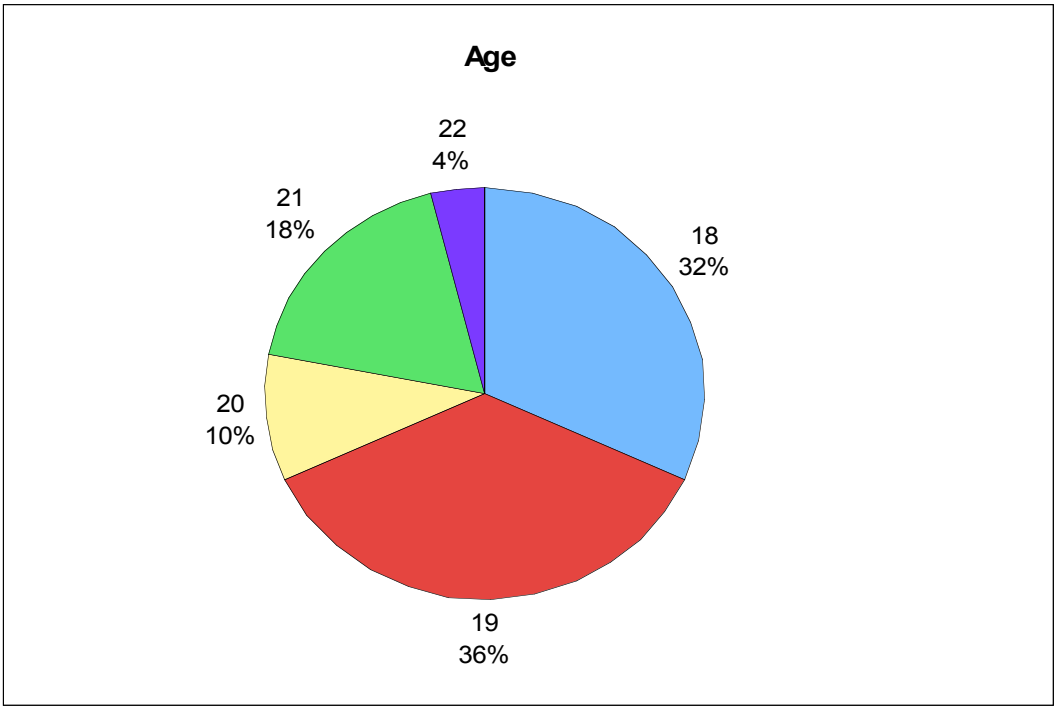
16. What is your college?
__ H&SS
__ MCS
__ CIT
__ SCS
__ CFA
__ Tepper
__ Other_____

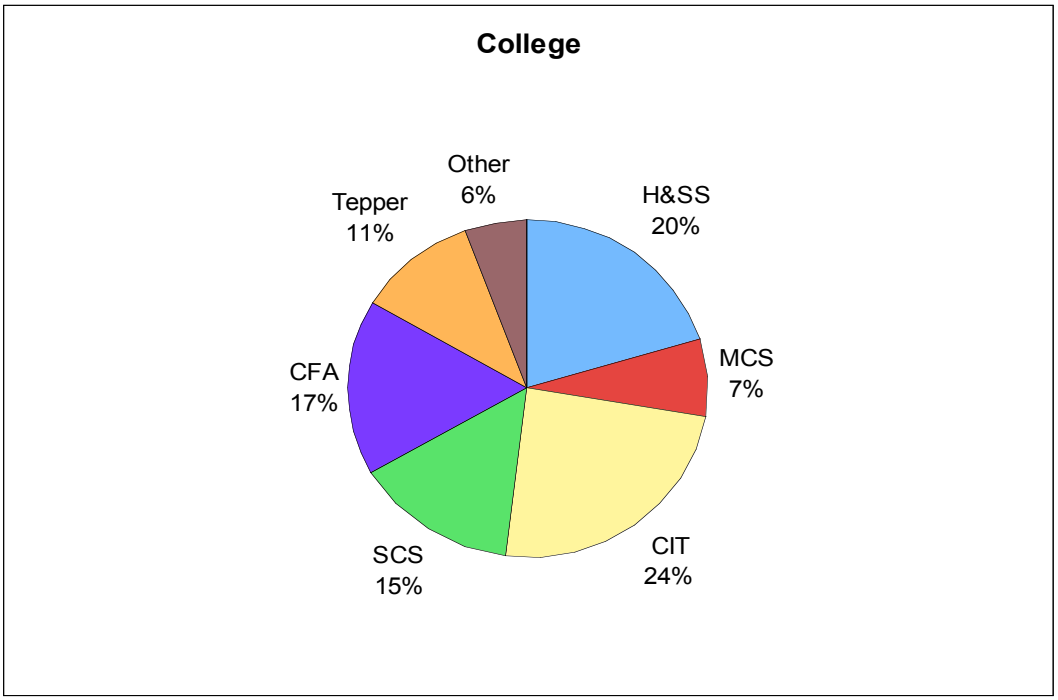
17. What is your gender?
__ Male
__ Female

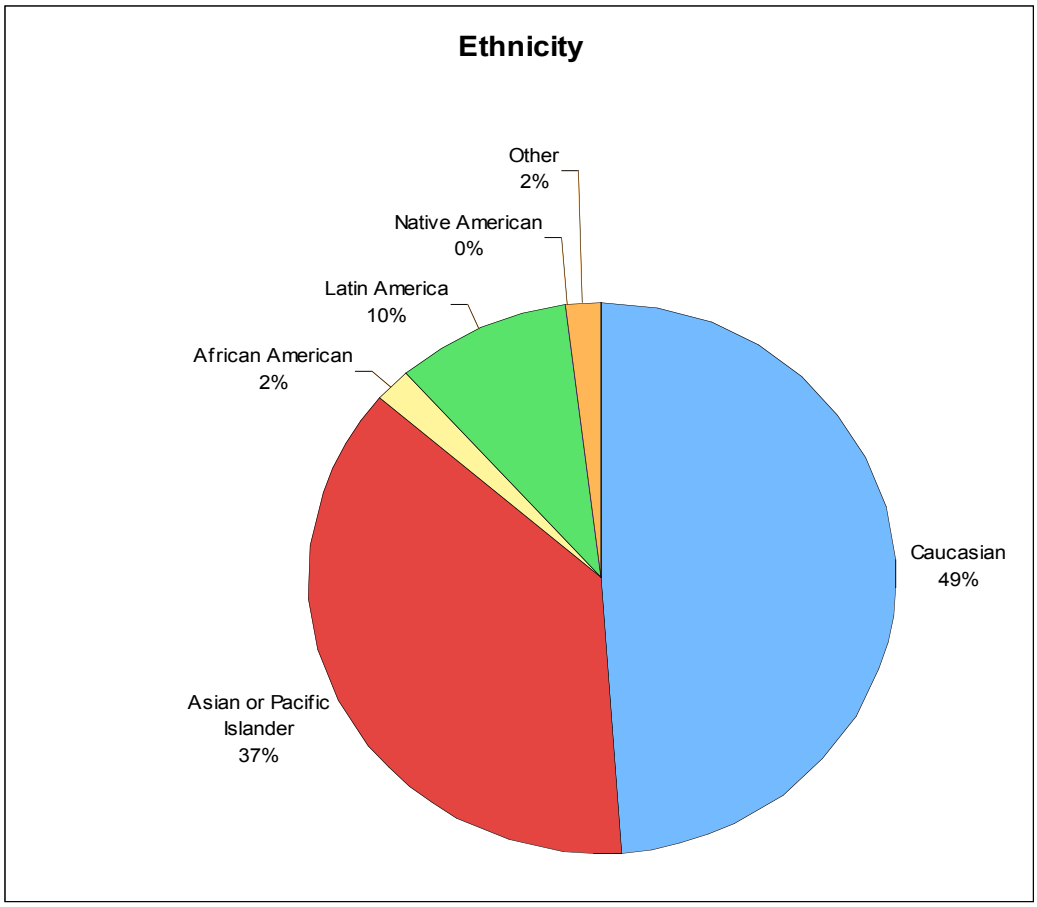
18. What is your ethnicity?
__ Caucasian
__ Asian or Pacific Islander
__ African American
__ Latin American
__ Native American
__ Other (please specify) _____

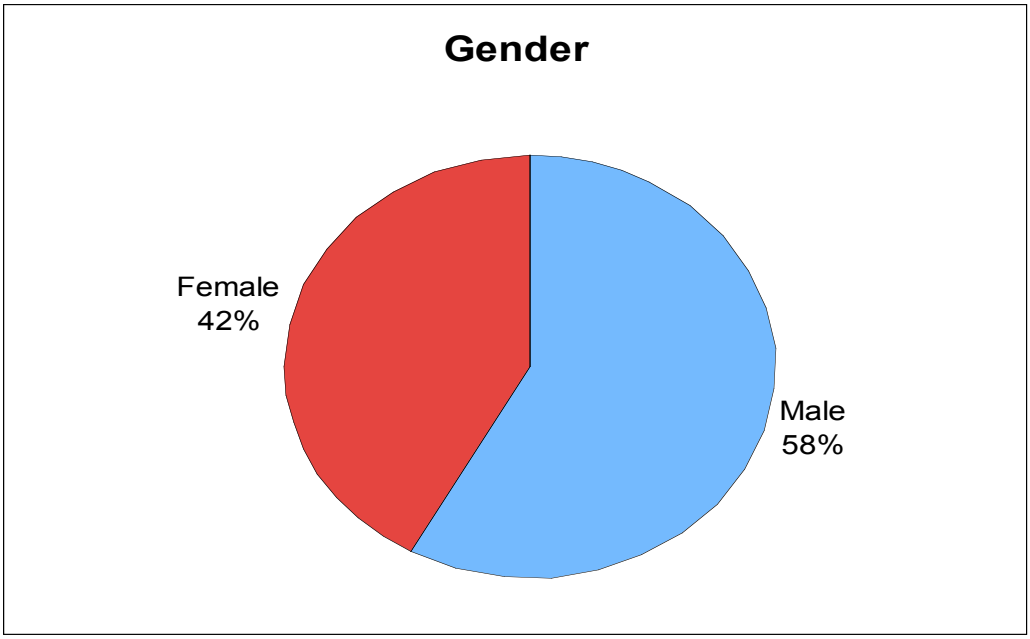
APPENDIX B

Charts of survey participants' demographics






Ethnicity
Other
2%
Native American
0%
Latin America
10%
African American
2%
Caucasian
49%
Asian or Pacific
Islander
37%


Gender
Female
42%
Male
58%