Privacy and Online Social Networking Websites

Richard Goettke

Joseph Christiana

Computer Science 199r: Special Topics in Computer Science Computation and Society:
Privacy and Technology

Professors: Prof. Michael D. Smith, Dr. Jim Waldo, Dr. Alon Rosen, Allan Friedman

May 14, 2007

I. Introduction

Social networking sites, while not an entirely novel phenomenon, have become increasingly more popular in recent years. Networking sites such as myspace.com and Facebook.com have become a significant part of adolescent American culture. Facebook.com alone is accessed by over 23 millions users[1]. There is a tension between the lucrative business side of social networking sites, where huge monetary gains can be made through online advertising, and the companies' resolve to ensure a basic level of privacy for its users. From this tension users receive privacy setting recommendations from social networking sites whose default settings are rarely altered or even questioned. The privacy problems that ensue stem from the fact that individuals are unaware of the amount of personally identifiable information they have provided to an indeterminate number of people. The purpose of this paper is to explore the threats to privacy that arise when users lack a sense of privacy awareness and concern when accessing social networking sites. We explore past literature and previous empirical studies of privacy implications for online social networking. We will also draw conclusions from our own study to determine how much information a typical user of a social networking site makes widely available both knowingly and unknowingly while also classifying social networking sites based on the privacy protection they offer. Then, we will illustrate the concern for privacy that users should have and the implications and privacy threats that may arise if they fail to do so.

II. Past Literature

Past studies have attempted to determine the reasons why social network users are unconcerned and unaware of the privacy concerns associated with their online practices, but the reasons prove to be numerous and varied. Ralph Gross and Alessandro Acquisti, in their report *Information Revelation and Privacy in Online Social Networks*, consider the privacy implication that arise from social networking sites upon their transition from "niche phenomenon to mass adoption.[2]" To do this, they observed the online behavior of over 4,000 students attending Carnegie Mellon University. While the reasons for joining such networking sites range from business interests to purely pleasure, the reasons behind the alarming amount of information people allow others to acquire are more ambiguous. The real privacy concerns arise when users allow people they do not know and normally would not trust to have access to the personally identifiable information they have made available. Certainly such an exchange of information would not ensue in a real life scenario, but occurrences such as these occur in high frequency on social networking sites. Gross and Acquisti explain that it may, in fact, stem from a *lack* of privacy concerns. That is, people allow a precarious amount of information about themselves to be available on these social networking sites because they are unaware of the large number of people who are allowed to view this information and the implications associated with these viewings.

---

[1] Facebook. "Facebook Overview." http://harvard.facebook.com/press.php Cited 11 May 2007.
[2] Gross, Ralph and Acquisti, Alessandro. Information Revelation and Privacy in Online Social Networks. p.71

As a result of this lack of privacy concern, Gross and Acquisti explain, that "a minimal percentage of users change the highly permeable privacy preferences" that are set as a default for these social networking sites. Subsequently, users profiles become "intimate portraits" of themselves and their lives[3]. "Privacy expectations may not be met by privacy reality" and this is where users run into trouble and privacy implications arise[4]. While the "perceived benefit of selectively revealing data to strangers may appear larger than the perceived costs of possible privacy invasions,[5]" Gross and Acquisti explain that such practices allow "third parties to create digital dossiers of their behavior.[6]" In addition, when providing real and accurate information, users contribute to the ease with which stalkers can target and victimize individuals as well as a prime contributor to the number of identity theft occurrences in the United States.[7] However, users are not the only ones to blame and many researchers are much quicker to point the finger of blame towards the websites themselves.

According to Harvey Jones and José Solton, "Facebook is undermined by three principal factors: users disclose too much, Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook.[8]" Not only are privacy protection default settings inadequate, social networking sites often discourage users from altering default settings. Myspace.com warns its users that altering default settings may make it more difficult for them to network with their friends. Thus, "the use of real names to (re)present an account profile to the rest of the online community may be *encouraged*." This is because social networking sites "aspire to connect participants' profiles to their public identities.[9]" Part of the research conducted by Gross and Acquisti involved determining if Facebook.com users provided real and accurate information. They found that 89% of users use their real name and, after considering a multitude of variables, they concluded that users are "by large, quite oblivious, unconcerned, or just pragmatic about their personal privacy.[10]"

If users were concerned about their privacy, and aware of the alteration that could be made to the default privacy settings, many social networking websites would be able to provide a substantially higher level of privacy protection. When considering the capabilities of Facebook.com to offer user protection, Jones and Solton explain that "From a systems perspective, there are a number of changes that can be made, both to give the user a reasonable perception of the level of privacy protection available, and to protect against disclosure to intruders.[11]" However, since the main goal of social networking sites is to maintain a connection between users' profiles and their real world identities for the purpose of networking, the responsibility of privacy protection often falls solely on the individual. As a result, "lasting change in online privacy will only come from a gradual development of common sense regarding what is appropriate to post

[3] Gross and Acquisti, Citation is for the previous two sentences both taken from p. 71
[4] Gross and Acquisti, p. 74
[5] Gross and Acquisti, p. 73
[6] Gross and Acquisti, p. 79
[7] Gross and Acquisti, p. 28
[8] Jones, Harvey and Soltren, José Hiram. Facebook: Threats to Privacy. December 15, 2005. p.1
[9] Gross and Acquisti, Citation is for the previous two direct quotes both taken from p. 72
[10] Gross and Acquisti, p. 76-78
[11] Jones and Soltren, p. 4

in social networking forums.[12]" While the general consensus, from both experts and users, is that it is not the duty of social networking sites to ensure users' privacy, social networking websites differ greatly in the amount of protection they initially provide and in the extent to which they will further provide protection.

According to Harvey Jones and José Soltren, "The environment that Facebook creates should be one that fosters good decision-making" so that "privacy should be the default, encryption should be the norm, and Facebook should take strides to inform users of their rights and responsibilities.[13]" In fact, compared to other social networking sites, Facebook.com does a good job of providing its users with an effective level of default privacy protection. Users are provided with the default setting that no persons outside of their network can have access to their profile. For example, a student at UCLA cannot access the Facebook profile of a student at Harvard College. Moreover, privacy settings can be further restricted on Facebook.com with comparative ease. Upon realizing the varying degree of privacy protection that can be maintained by social networking sites we developed a five tiered categorization of social networking sites.

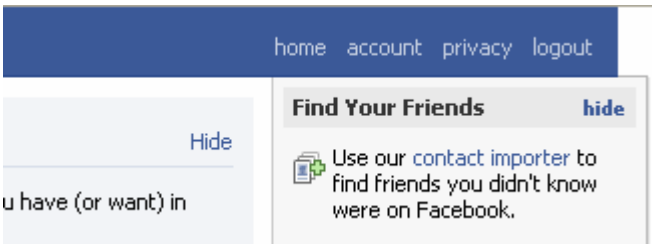
III. Privacy Protection Scale

The four websites we deemed appropriate for the purposes of this study were Facebook.com, MySpace.com, Classmates.com and Frienster.com. When classifying the websites we took into consideration 1) the visibility of the privacy settings link, 2) the ease to which privacy settings can be changed, 3) the default privacy settings, and 4) the search / browse capabilities a user is allowed.

Our scale is broken up into five tiers. **TIER ONE (1)** websites are those on which users' information is completely transparent to third parties. While **TIER TWO (2)** websites offer more privacy protection than tier one, privacy protection is still insufficient with the presence of user awareness. **TIER THREE (3)** websites offer users a significant amount of privacy protection but only under the condition that users are aware of privacy concerns and make the possible alterations to the default privacy settings. **TIER FOUR (4)** websites provide significant privacy protection even in the absence of such user awareness. And finally, **TIER FIVE (5)** websites completely ensure the privacy protection of all users.

A. Facebook.com

We have classified Facebook.com as a tier 4 website. In the top right hand corner of the Facebook.com welcome screen (seen below), users can easily access links to either log out, access the home page, or alter their privacy settings. Thus, users are typically aware that privacy settings can be altered because the privacy settings link is highly visible. Once inside the privacy settings page, a user is given simple options



[12] Jones and Soltren, p. 34
[13] Jones and Soltren, p. 34

in drop down menus that guide the user into choosing the desired privacy settings.

One of the best privacy features of Facebook is that it does not allow global searches. A user must be part of a specific network (ex. college, high school, city, organization, etc.) in order to browse / search the individuals that are a part of that network. Easy access to the privacy link, the straightforward ability to change one's privacy settings, and the limited ability to globally search are all positive aspects that help guard users' information from users in other networks. Therefore, we are classifying Facebook.com as a tier 4 website offering significant privacy protection even in the absence of user awareness.

B. Myspace.com

We have classified Myspace.com as a tier 3 website. While Myspace.com offers similar privacy setting restrictions as Facebook.com, the web site has a more ambiguous privacy settings link that is less obvious for users to access. As seen in the pictures to the left, there is no word 'privacy' anywhere on the homepage (top picture). The link 'account settings' sends the user to another page with the link "privacy settings." (bottom picture). Myspace.com does allow users to change their settings, but it is not user friendly.

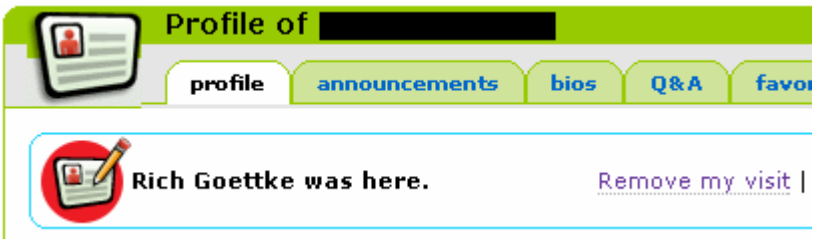
Privacy Settings:	- Change Settings -
IM Privacy Settings:	- Change Settings -
Mobile Settings: New!	Change Settings -
Groups Settings:	- Change Settings -
Calendar Settings:	- Change Settings -
Blocked Users:	- View List -

As explained earlier, Myspace.com warns its users that altering default settings may make it more difficult for users to network with their friends. The best manifestation of this and the most troubling is that the default privacy setting for *Who can view my profile?* is set to public! Combining the confusion in changing default settings, Myspace's warning that changing settings will have a negative effect on social networking, and the website's default setting of a user's profile to public, are the main reasons why we deemed it appropriate to classify Myspace.com as a website that offers a significant amount of privacy protection only when users are aware of the alterations that can be made to their privacy settings.

C. Classmates.com

We have classified Classmates.com as a tier 4 website. Classmates.com is different from both Facebook and Myspace because to experience the entire website, a user must sign up for a subscription costing between $2.50 and $5.00 per month depending on the length of subscription. Thus, our experience was as a 'free member.' This monetary expense is positive in protecting privacy because only those people who want to reconnect with classmates will be willing to pay. The fee can be seen as a privacy premium contributing to this website's classification as a tier 4 website. Another positive

for Classmates.com is the amount of personal information accessible to other users. Once a user creates a username and password, the website guides the user through a template for filling out the user's profile, giving the user the choice of what and what not to include.

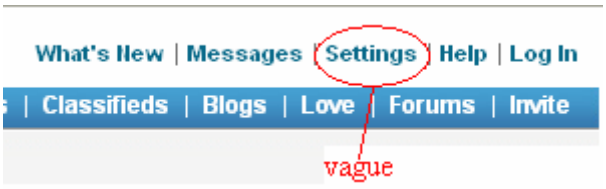


A negative to Classmates.com is that viewing/changing default privacy settings can be confusing. The user must first click on the link 'account settings,' then click on the link 'privacy settings' in order to access the necessary webpage to change the default privacy settings. In addition, Classmates.com has a setting that allows a user to know when another user has visited their profile. At first this seems to help privacy; however, all a visiting user has to do is click the link 'Remove my visit' to keep their visit anonymous/secret (see picture above).

Because users must subscribe to Classmates.com to fully experience the website and at the onset users are forced to determine how much personally identifiable information they are willing to provide, we categorize Classmates.com as a website offering significant privacy protection even in the absence of user awareness.

D. Friensterc.com

We have classified Friendster.com as a tier 3 website. Users can only alter the default privacy settings of this online social networking by clicking the obscure 'settings' link in the top right hand corner of the website's home page (see picture to the left). Once inside and only after a user scrolls down can s/he change the default privacy settings. Moreover, only 10 percent of user profiles on friendster.com accessed during our study had altered the privacy settings to prevent us from contacting these users, thus supporting our conclusion that access of privacy settings is relatively unclear. Further, the default privacy settings are not very restricting, allowing third parties to message users and view their information in the absence of privacy awareness. It is also unclear as to which default settings should be altered in order to fully prevent this invasion of privacy to occur. For these reasons Friendster.com has been classified as a tier 3 website, one that offers a significant amount of privacy protection only when users are aware of the alterations that can be made to their privacy settings.



IV. Friend Request Survey

After establishing the color-coded scale for each of the four social networking sites, we devised a plan to create an experiment to obtain results on whether or not users from these four social networking sites are concerned with privacy. Individuals between

22 and 25 were randomly selected and were contacted in two ways: **1)** by a friend request **2)** by a message detailing our survey's purpose. Three questions were asked in the message:

> **1)** Do you normally accept "friend requests" from persons you do not know (i.e. would you have accepted my friend request without this message.)?
>
> **2)** Second, do you base your decisions to accept a "friend request" with your privacy in mind?
>
> **3)** Could you rank this website on a scale of 1-5 as to how much you feel your privacy is protected. (1 being poorly protected and 5 being completely ensured).

Following the conclusions of Ralph Gross and Alessandro Acquisti in Information Revelation and Privacy in Online Social Networks, we expected that most users would not be concerned with protecting their privacy. Furthermore, this would be manifested through our survey in that 1) the friend requests sent out would be accepted more than they would be denied, 2) users would answer "no" to the question of whether or not privacy influences their friend acceptance decision, and 3) users would rate websites as average or above average in protecting user privacy.

V. Results of Initial Survey

A. Facebook.com

50 messages and friend requests were sent out to a random group of users. 5 of 50 blindly accepted the friend request, while 8 of 50 participated in the survey with the following results. (Note: no one responding to the survey accepted our friend request) All 8 said they do not accept random friend requests, 5 of 8 said they base their "friending" decision on privacy, and 3 users gave the website a rank of 3; 4 users gave it a rank of 4; and 1 user gave it a rank of 5

B. Myspace.com

Out of 45 friend request and message attempts on MySpace.com only 5 were undeliverable due to privacy setting alterations. Out of the 40 sent friend requests and messages there were only two responses to the survey. A male and female responded to the survey, classifying MySpace.com as tier 3 and 1 respectively. However, both users explained that they view privacy protection as their own responsibility, not holding Myspace liable for any privacy invasions. Both say they will accept random friend requests on rare occasions, but their decisions are in no way based on privacy concerns. Aside from these two, four other people accepted our friendship request.

C. Classmates.com

20 messages and friend requests were sent out; however, no friend requests were accepted and no messages were answered because users are unable to answer messages for free unless they sign up for a Classmates.com Gold Membership (the subscription mentioned earlier). Therefore, because of this requirement Classmates.com was not used

in the survey analysis; however, we still adhere to our classification in the earlier part of this document categorizing Classmates.com as a tier 4 website.

D. Frienster.com

20 messages were sent out to users. 2 of 20 had restricted their privacy preferences so that messages were undeliverable. Despite our ability to contact 90 percent of the users we identified we received no responses from Friendster.com users. It is our conclusion that users of this social networking site either a) visit the website less frequently or b) are less interested in responding to individuals whom they do not know on a personal basis.

VI. Analysis and Decision to Restructure the Survey

It should be noted that there are two obvious problems with the results and subsequent analysis above. 1) There are too few results due to the small sample size, and 2) there is a large portion of users that did not respond at all. Because any conclusions from this are skewed, we think it is better to reevaluate what we should have done or what would have been most effective, rather than analyzing and forming bad conclusions on bad data. However, we were able to obtain some worthwhile data. The most interesting part of this experiment was the discrepancies found between how a user responded to our survey and his/her privacy settings.

VII. New Experiment Layout

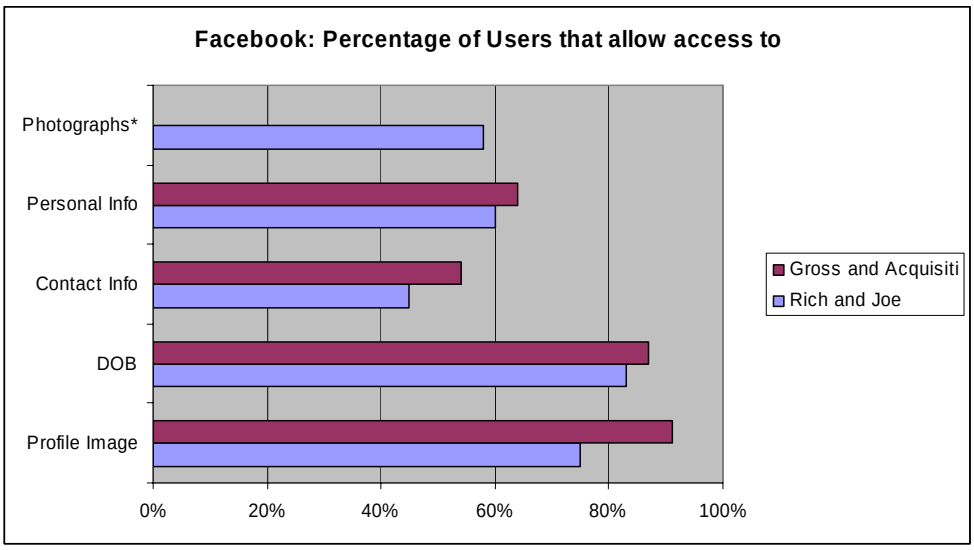
As stated before, the survey of three questions and friend requests we designed was flawed because it relied heavily on user participation. A better approach would have been to run a similar experiment to the one performed by Ralph Gross and Alessandro Acquisti. As previously discussed, they sampled over 4000 Carnegie Mellon University students and looked at the amount of personally identifiable information they disclosed. In our restructured experiment, we would randomly browse through the desired social networking websites, cataloging how much personally identifiable information users displayed. We decided that because of time constraints, and the capabilities of two individuals without a research team, we were unable to perform this on all four social networking websites; however, as a preliminary test we collected data on 300 profiles using Facebook.com. We viewed and cataloged whether a user allowed his/her 1) profile image, 2) date of birth, 3) contact information, 4) personal information, and 5) photographs. Although this is a simplified version, we hypothesize that our results will be similar to those found by Gross and Acquisti despite the problem of a small sample size.

VIII. Cataloging of Facebook

A. Facebook

Looking at 300 profiles of random males and females 22-25 in the Cincinnati, OH network (of which I, Rich, belong) I found the following results, and compared them to the results found by Gross and Acquisti.

Facebook: Percentage of Users that allow access to:



	Profile Image	DOB	Contact Info	Personal Info	Photographs*
Rich and Joe	75%	83%	45%	60%	58%
Gross & Acquisiti	91%	87%	54%	64%	0%*

There are a few important notes about the graph. *Photographs was a variable not cataloged by Gross and Acquisti; however, we thought that the choice to allow others to view photographs is an excellent indicator of whether a user is privacy conscious or not. Also Gross and Acquisti did not specifically catalog Personal Info and Contact Info; rather, they were more specific by cataloging such things as AIM screenname, Address, etc. Therefore, the percentage in the graph for Personal Info for Gross and Acquisti is an average of the percentages they found for these variables. Their graph is attached in Appendix A for further clarification.

Even though our sample was significantly smaller than that of Gross and Acquisti's (300 vs. 4000), the findings are very similar. A significant majority of users are willing to allow access to their personally identifiable information. It is noteworthy that 58%, the percentage of users allowed access to photographs of themselves, is very close to the 60% that allow personal information.

IX. Analysis

Our small experiment as well as Gross and Acquisti's, shows that users, between the ages of 22 and 25, do not see any problems with allowing other users they do not know to access personally identifiable information such as AIM screennames, email

addresses, and photographs. Because the information is on the World Wide Web, these young adult users feel protected more so than they would sharing their information in person. However, as we have seen in class this feeling of comfort is merely a false sense of security created by the individual user.

Another explanation for the amount of personally identifiable information floating in cyberspace is that the reasonable expectation of privacy has broadened for younger generations and they blindly accept that in this information age of increased technology that is the price we pay. No longer do they expect activities or information online to be secret. But this conclusion does not stand up when individuals are asked about how much they value privacy.

For example, in one response to our first survey, a Facebook user answered that she does not accept random friend requests and she does have privacy in mind when making this decision. Consequently, on Facebook if you receive a friend request or message you have to separately decide how much of your profile the requester or messenger can see. Before sending the message we could not access the profile, but after the friend request and her responding to our initial message we were able to see her entire profile, meaning she had not thoroughly gone through her privacy settings. Lastly, at the end of the return message to us the user wrote "It is not Facebook's job to protect idiocy." This blatant discrepancy between opinion and action is startling and lends more support to the conclusion that many users want to protect themselves but are not fully informed or educated about how to change privacy settings on these social networking websites.

X. Conclusion

While we have recognized several flaws in our first experiment, due to both time and labor constraints, there are key takeaways from which we can draw certain privacy implications. Our classification of the four social networking websites and our second experiment involving a quick cataloging of Facebook.com proved to be the most telling aspects of our report.

Through our investigation of the privacy settings offered by each website, we found that users are generally unaware and/or unconcerned with protecting their privacy on social networking sites. With an emphasis placed on maintaining visibility, websites, in this case Myspace.com and Friendster.com, scored a 3 because they provide an insufficient amount of default privacy protection to unaware users and, in some cases, users who are aware of privacy concerns. Facebook.com was given a rating of 4 because the website limits global far-reaching searches and its platform is user friendly. Likewise, Classmates.com was given a 4 because it requires a subscription, or what we call a privacy premium, in order to join and experience the website fully.

In addition, some of the users we contacted believe that it is not the websites' responsibility to provide such protection. Instead, the responsibility should rest solely on the individual users. Given this, it would be wise for users to increase their knowledge of privacy implications associated with participating in social networking. It seems user awareness will play a large part in ameliorating these privacy concerns in the future.

As Jones and Soltren say, "Although the Internet has made it possible to publish personal information online for a decade, social networking sites are unique in that they standardize, centralize, and encourage the publication of personal data to an

unprecedented extent."[14] As millions of new users sign up for Facebook, Myspace, and a multitude of other social networking websites this year and in the future, the amount of personally identifiable information will only increase drastically. The largest challenge both now and in the future in terms of users protecting themselves and their information will be to find out and understand how to effectively access and change the privacy settings offered by these popular social networking websites.

[14] Jones and Soltren, p. 35

Bibliography

Facebook. “Facebook Overview.” http://harvard.facebook.com/press.php Cited 11 May 2007.

Gross, Ralph and Acquisti, Alessandro. Information Revelation and Privacy in Online Social Networks. pp. 71-79

Jones, Harvey and Soltren, Jose Hiram. Facebook: Threats to Privacy. December 15, 2005. pp 1, 4, 16, 34, 35

Other Related Sources

Govani, T. & Pashley, H. (2005). Student awareness of the privacy implications when using facebook. Accessed 7 May 2007. http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Pierre, Darren. A review of facebook.com. Association of Fraternity Advisors. *Essentials*, January 2006.

Stutzman, Fredric. An Evaluation of Identity-Sharing Behavior in Social Network Communities. *Ibiblio.org.* Accessed 5 May 2007 http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf

Appendix A

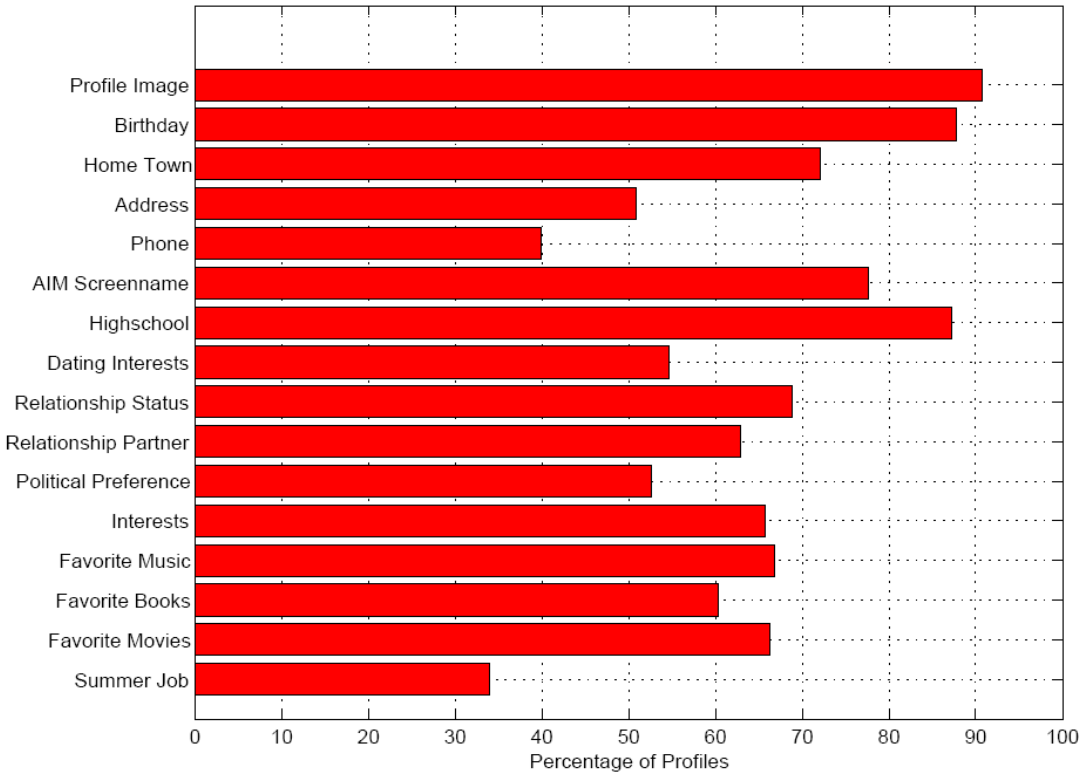


Figure 2: Percentages of CMU profiles revealing various types of personal information.

[15]

[15] Gross and Acquisiti p. 75 Graph showing their catalog of CMU students and the information provided on their profiles