Privacy Management for Facebook

Enkh-Amgalan Baatarjav, Ram Dantu, and Santi Phithakkitnukoon

Department of Computer Science and Engineering
University of North Texas, Denton, Texas, 76203, USA
{eb0050,rdantu,santi}@unt.edu

Abstract. As more people adopt the Internet as a medium of communication, the Internet has developed into a virtual world and this has resulted in many online social networks (SN). MySpace and Facebook, two leading online SN sites, have a combined user base of 170 million as of 2008. SN sites started to offer developers open platforms that provide users' profile information to the developers. Unfortunately, the applications can also be used to invade privacy and to harvest the users' profile information without their acknowledgement. To address this vulnerability, we propose a privacy-management system that protects the accessibility of users' profile. The system uses probabilistic approach based on information revelation of users. Our experimental result shows that the system can achieve high accuracy rate of 75%.

Keywords: Privacy, Privacy management, Social network, Facebook.

1 Introduction

Communication among friends, colleagues, and family members has been changing from strictly face-to-face interaction to increasingly include cyberspace or online social networking (SN) where individuals can receive/send messages, share photos, join groups, read gossips, and meet with strangers. The number of people with Internet access has fostered an environment where real-life social activities transform into online social activities [1]. As with real-life social networks, we can cluster this online social networking into sub-networks with common values. Among such values may be family bonds, common interests, regions, political preferences, activities, ideas, and religions. Anyone can join a particular subnetwork, which makes online SNs quite diverse.

Since they do not require face-to-face interaction, online SN sites make it easy to find and meet people. To ensure online interaction takes place, users tend to post personal information such as their actual names, birthdays, political preferences, religions, relationship status, interests, activities, favorite music, listings of movies, and other information they believe will attract others. This posting provides credibility (through identifying credentials) and suggests areas of compatibility between parties. In addition, the online SN allows users distribute their information through the network efficiently and quickly. For example, users having parties can send event invitations to their networks. Users may learn more

R. Sekar and A.K. Pujari (Eds.): ICISS 2008, LNCS 5352, pp. 273–286, 2008.

about friends on the social network site than they would in face-to-face meetings. Thus, sharing common interests and ideas with friends makes online SNs attractive cyber-places to hang out [2].

In this study, we will study architecture of Facebook platform and its privacy hole. Using the privacy hole of Facebook, we will show a way to harvest users' profile information. Finally, we will purpose a possible solution to protect privacy of Facebook users.

2 Background

Privacy is an inevitably issue for online SN. It has become much easier these days to find almost any person's personal information through highly sophisticated online technologies with search engines such as Google, Yahoo, and Ask. Social Networking Sites (SNS) provide the next big step toward invading users' privacy because users willingly post personal information either without considering the consequences or believing that their information is somehow protected. However, practically this is not always the case and privacy on social networking sites has received more attention from individuals in many fields of study, particularly, computer science, information science, and sociology. In 2007, Acquisti and Gross of Carnegie Mellon University [3] reported some privacy issue on Facebook. Their survey of 40 questions relating to Facebook privacy was taken by 506 respondents. Acquisti and Gross analyzed survey-takers behavior on Facebook based on before and after learning information revealed on Facebook. They also pointed out misconceptions of members' profile visibility in their network based on the survey.

Social networking has become increasingly popular among teenagers who can easily become victims of privacy invasion because of lack of awareness of privacy issues[4] [1] [5]. Consequently, members of this group reveal more information on their profile sites than older users. This lack of awereness can lead to unexpected consequences. To address this issue, Susan B. Barnes [6] proposes three approaches to solve this problem: social, technical, and legal. Social networking is one of the technologies that changes our everyday life-style. Danah Boyd's study [4] showed four properties: persistence, search-ability, exact copy-ability, and invisible audiences that SN sites had, but conventional face-to-face interaction did not. These properties had been changing the way people interact, especially for young people.

3 Facebook

Facebook is the Internet's fastest growing SNS. Facebook, founded by Mark Zuckerberg and launched on February 4, 2004, was initially restricted to Harvard University. However, because of its rapid success, Zuckerberg expanded it to users at Ivy League schools. Facebook was quickly spreading throughout institutions around the world. Any user with a valid university email address could join in. From September 2006 to September 2007, Facebook's Internet traffic ranking

jumped from 60th to 7th [7]. From September 2006, Facebook became accessible to any user 13 or older [8]. As of November 2007, Facebook had more than 55 million active users and 60 million users by the end of 2007. Facebook's average new user registration per day since January 2007 was 250,000 [8]. Open platform, one of Facebook's main features, attracts a large audience to Facebook from a variety of fields including multi-million dollar corporations, entrepreneurs, and student developers [8]. Facebook made its platform available to application developers in April 2007. As of May 2008, the number of applications available to users had grown to 24,800 [7].

3.1 Facebook Platform

Introducing open platform on a social networking site makes a breakthrough that gives both developers and companies creative freedom. As of June 2007. On the Facebook social network, there were 40,000 Facebook application developers, and it attracted 1,000 developers daily [9]. Three reasons may account for this. Firstly, using the open platform, advertising firms can exploit social graph of users to have a clearer understanding demographic of the users, so it is shown to be effectively way to distribute information to potencial customers using the social graphs [8]. Secondly, developers can develop applications quickly on the Facebook platform, making it attractive from a profit measure. Thirdly, the platform is available in many programming environments, such as PHP, ASP, ColdFusion, Java, C, C++, and Python, so the developers can select their comfortable environments [8].

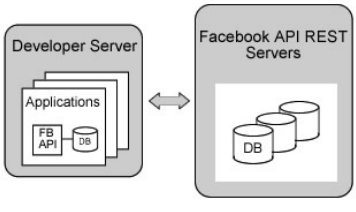


Fig. 1. Data transaction mechanism between Facebook platform and Facebook API REST servers

The Facebook platform is based on a representational state transfer (REST)-like interface. Figure 1 depicts a high-level architecture of the Facebook platform. Information resource is located at Facebook API REST server, and this information is retrieved by method calls in the Facebook API located on the developer's server. Data transaction between the REST server and the application uses either HTTP GET or POST request methods [8]. Using the Facebook API, applications can access a database of information as given in Table 1, can be considered as sensative information for some users. A complete list can be found at [8] [1].

[1] http://developers.facebook.com

Table 1. Using Facebook platform, application developers can access users' personal and social information

Tables	Description
user	User profile information first name, last name, birthday, sex, hometown location, current location, political preference, religion, work history, education history, interests, activities, etc.
friend	All friends of a user. Facebook API method returns list of user IDs (uid).
group	Groups a user belongs to along with group IDs (gid), names, group types, and descriptions.
group_member	Member list of a specific group
event	Upcoming event organized by group or friend along with that event's unique ID (eid).
event_member	Invited members' status of an event.

3.2 Facebook Privacy Policy

Facebook believes in openness of information on the its network. Its privacy setting is based on an opt-in policy, in which Facebook users' information is accessible to all of Facebook's SNS users and to platform applications by default. This means that Facebook considers its members to be legitimate users will not violate Facebook rules and policy. In reality, not everyone is legitimate user and obeys its policy. Therefore, Facebook does not enforce its privacy policy rigorously enough to protect its legitimate users from invasions of privacy and even criminal activity. As shown in Table 1, the amount of information available to strangers is high on Facebook. In default setting, miscreants can easily identify a user's first name, last name, birthday, email address, physical address, phone number, relationship status, political reference, religion, hometown, favorite music, TV shows, books, groups that user belongs to, and a variety of other personal information.

Facebook clearly publishes the following statements on its new users' term. First, Facebook does not review and approve any application before it is published on the network:

"... Platform Applications have not been approved, endorsed, or reviewed in any manner by Facebook, and we are not responsible for your use of or inability to use any Platform Applications, including the content, accuracy, or reliability of such Application and the privacy practices or other policies of Developers. YOU USE SUCH PLATFORM APPLICATIONS AT YOUR OWN RISK ..." [8].

Second, any application that is installed on user's friend's site can access all user's information that is allowed by the user: *"... If you, your friends or members of your network use any Platform Applications, such Platform Applications may access and share certain information about you with others in accordance with your privacy ..."* [8].

Facebook's privacy statement suggests that users who are agree to its terms, know that they are agreeing to make any of their information placed on the site accessible by any users on a same network and platform application. In our study, we find that most Facebook users are unaware of the default privacy setting they are agreeing to. In section 4, we discuss how this information can be exploited and how this exploitation can be implemented by the Facebook API.

4 Facebook Privacy Issue

Demographic factors, such as age, education level, and wealth, influence level of privacy concerns [5]. In this section we explore about how much information is revealed by different demographics. Having an open platform that makes it easy to access social and personal information means maintaining users' privacy must be in a careful consideration. In the case of Facebook, open platform creates a privacy hole. Many users post personal information without knowing that malicious users (hackers) can harvest and exploit their information. In addition, the application privacy setting by default is configured to allow all platform applications to access users' profile information. This, again, makes that information available to potentially dishonest hackers and other criminals. To find out how much information Facebook users reveal on their profile, we analyze sample of 4,919 Facebook users on the University of North Texas network. (The online SN has 34,790 registered members.) Gender ratio is 35% female and 65% male. Our research shows that 75% of the users reveal their education history after high school (Fig. 2); 70% disclosed their high school's name; more than 60% posted their favorite movies, music preferences, interests, relationship status,

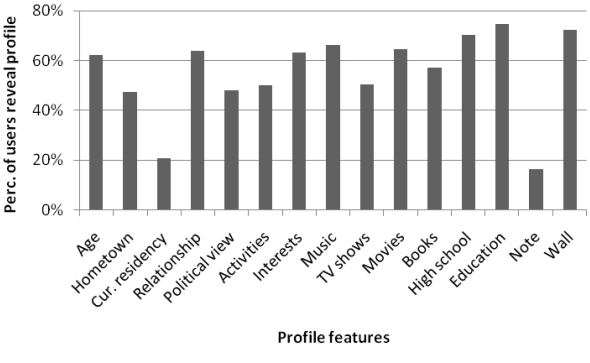


Fig. 2. Example of how much personal information is revealed on UNT social network site, and result is based on 4,919 users

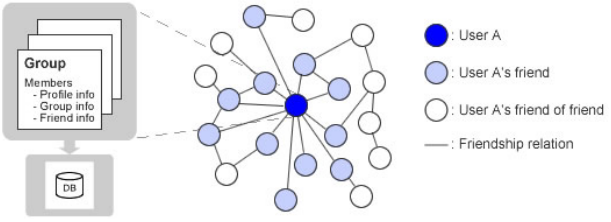


Fig. 3. Once a user installs an application, his social network is accessible by the application, which creates privacy hole in the social graph

and age; 57% listed books they like; between 45-51% revealed their hometown, their favorite TV shows, activities, and political preference which can be one of libertarian, apathetic, very conservative, conservative, moderate, liberal, or very liberal; and, 21% disclosed the city where they currently resided.

Facebook's policy of neither approving nor reviewing platform applications developed by third parties and high number of users uninformed about their privacy settings make Facebook users' personal and social information easily harvestable using Facebook API. An unscrupulous developer can exploit this vulnerability. Figure 3 shows the harvesting process. Each user's site carries information of profile, group, and friend. Information can be harvested based on this information.

Figure 3 shows a user's social graph. Exploiting Facebook's privacy hole, a malicious application harvests the user's personal and social information. In addition, the user's social information can be used for further information harvesting. The following is an example of a pseudocode to harvest a user's social graph: after $UserA$ installs an application, the application harvests profile information of $UserA$'s social network. G and F denotes groups and friends, respectively. A function $Get()$ returns profile information, group information, friend information, or group member information depending on one of the arguments: $profile, group, friend, or\ member$, respectively.

A malicious program installed by User A

```
A = Get (profile (User A)) // Input: User A's profile information
G = Get (group (A)) // Extract groups where A belongs
F = Get (friend (A)) // Extract A's friends
StoreData // Variable or database to store profile information
for f ∈ F do
    G += Get (group (f))
end for
Delete duplicating groups in G
for g ∈ G do
    V += Get (member (g))
end for
Delete duplicating data in V
```

13: **for** $v \in V$ **do**
14: StoreData += Get (profile (v))
15: **end for**

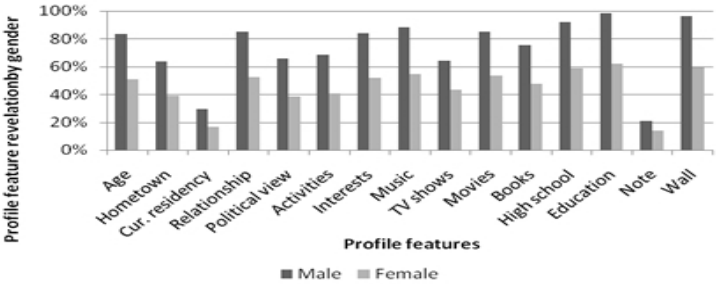
Once the user installs an application, the open platform's API gives the application access to the user's profile, friend, and group information. On Facebook, each user and group has unique ID (uid and gid). Once their harvesting program recovers these IDs, its developers can easily collect and use these information. As this example demonstrates, by writing a simple PHP code on top of the Facebook platform, developers can find harvesting information that users believe is private and personal to be a trivial task. In this section we demonstrated how much information can potentially be revealed by Facebook users using an SNS.

5 Analysis on Information Revelation

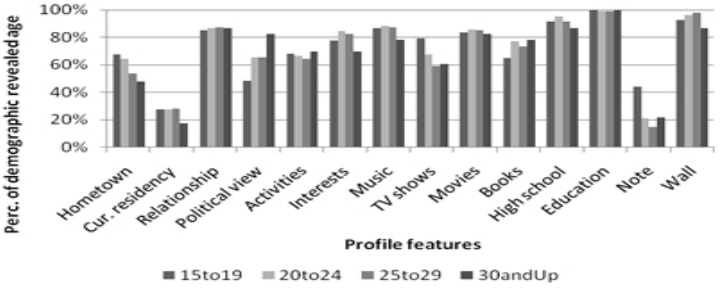
In Sect. 4 we demonstrated that Facebook users' information can be harvested because of the default privacy setting by platform applications. In this section, we report our analysis of data from four categories: gender, age group, relationship status, and political preference. In fact, we further investigated to build privacy protection system based on these results in Sect. 6. Each category exposes interesting results. The analysis is based on 4,919 Facebook users in the UNT social network. Although Facebook did not require that users reveal the information,

Table 2. Demographic of data revelation by gender, age, relationship, and politic preference

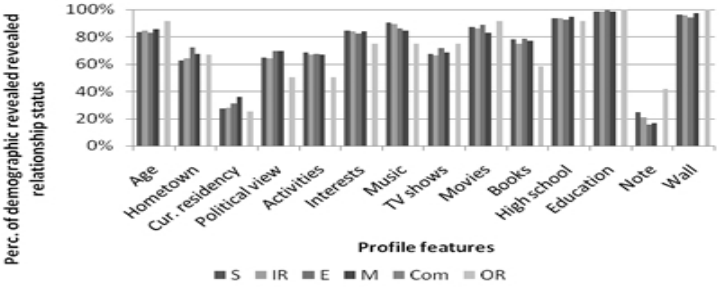
Category	Group	Revelation (%)
Sex	Male	35
	Female	65
Age	15-19	4
	20-24	82
	25-29	14
	30-up	0.5
Relationship Status	Singe	47
	In Relationship	35
	Engaged	6
	Married	12
	Complicated	0
	Open Relationship	0.4
Political Preference	Very Liberal	6
	Liberal	28
	Moderate	34
	Conservative	24
	Very Conservative	2
	Apathetic	4
	Libertarian	3



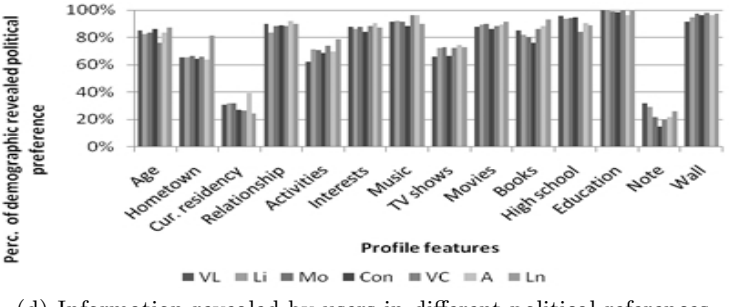
(a) Information revealed by different genders



(b) Information revealed by different age groups



(c) Information revealed by users in different relationship status



(d) Information revealed by users in different political references

Fig. 4. Informtion revelation based on gender, age, relationship status, political preference

62% (3,045) revealed their age; 64% (3,143) exposed their relationship status; and 48% (2,358) showed their political preference.

In Table 2, we further analyze the data by gender, age, relationship status, and political preference. From 4,919 users profiles examined, 65% revealed the user as female and 35% male. We find that 82% of 3,045 are between 20 and 24 years old and 18.5% of 3,045 are in age group of 15-19, 25-29, or 30-Up. Table 2 (Relationship Status) shows that majority of the users who reveal their relationship are singles. However, no one was in complicated relationship. Table 2 (Political Preference) shows that 84% of 2,358 reveal their political preference are conservative, moderate, or liberal.

From Fig. 4(a), we find that female users are less likely to reveal their personal and social information than male users. Figure 4(b) shows that on average age group between 20 and 29 reveals more personal and social information than any other age groups. In addition, Fig. 4(c) illustrates on average that users are engaged or married reveal more information than any other status. Apathetic and libertarian users disclose more information than any other political references as shown in Fig. 4(d).

6 Privacy Protection Mechanism

In this research, we attempt to mathematically formalize users' data revelation behavior on social network sites. The preliminary model is developed to facilitate privacy protection mechanism. Facebook users can configure what information to be available to platform applications. However, Facebook privacy setting is configured after opt-out. In other words, all of a user's profile information is accessible unless the user knows that specific information must configure as inaccessible. As we can see from Sec. 4 and 5, an opt-out model does not provide sufficient protection against data harvesting. In this section, we address this issue and develop a privacy-protection system (PPS) that automatically configures a user's privacy settings based on the user's profile information. Figure 5 shows the model of our privacy-management system. The system uses three components: profile information (PI), privacy manager (PM), and profile zoning (PZ).

Profile Information (PI) contains two types of information: personal and social information. The personal information contains age, relationship status, and political views. On the other hand, social information consists of hometown, current residency, activities, interests, music, TV shows, movies, books, high school information, education history, profile note, and wall postings. We select personal information as our main features that can characterize users' personality and can be easily obtained from profile information.

In profile zone (PZ),PPS divides the user's profile information into two zones. One zone carries information which is accessible by platform application. The other zone carries information, which can not be accessed by plateform application.

Privacy configuration takes place in the privacy manager (PM). PM performs its task in two phases. Phase 1 is sampling the network to discover information —revelation behavior. Sampling should not take place every time a new user

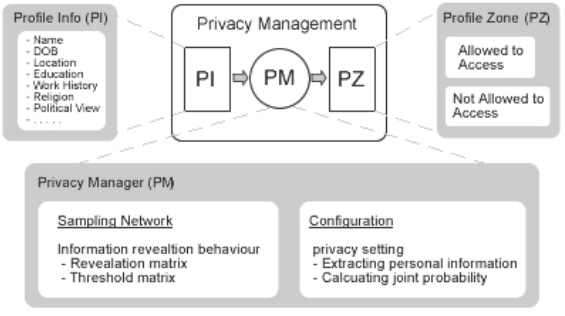


Fig. 5. Privacy management system for configuring users' privacy setting for applications

joins the network, but it only after a significant change in network population or substantial number of users changing their personal information. In this study, we randomly selecte 4,919 users in the University of North Texas (UNT) network. In phase 2, PM configures the user's privacy setting using *revelation matrix* and *threshold matrix*. With this system, users would have to opt-out of privacy rather than opt-in to making all their information public.

6.1 Building Revealation Matrix

Revelation matrix is built using statistical analysis on personal information of 4,919 UNT users. Personal information is categorized as follows: gender with two subgroups of male and female; age with four subgroups of ages range 15 to 19, 20 to 24, 25 to 29, and 30 and up; relationship status with five subgroups of single (S), in relationship (IR), engaged (E), married (M), and open relationship (OR); and political preference with seven subgroups with very liberal (VL), liberal (Li), moderate (M), conservative (Con), very conservative (VC), apathetic (A), and libertarian (Ln). On each subgroup, the same statistical analysis is applied. Let's take an example of male subgroup. First step is finding all male users from the sample of 4,919 users, and than calculate percentage of the users who reveal age, hometown, current residence, etc. Equation 1 is applied for each subgroup. $R_{i,j}$ is percentage of users who are in j subgroup reveal their feature i, where $i = \{Age, Hometown, Cur.resident..., Wall\}$, $j = \{Male, Female, 15-19, ..., Ln\}$, n_i and N_j are total number of users corresponding to i and j, respectively.

$$R_{i,j} = \frac{n_i}{N_j}. \tag{1}$$

An element of the revelation matrix can also be interpreted as a probability of users revealing profile features based on their personal information.

6.2 Building Threshold Matrix

The second step in sampling network phase is building threshold matrix. Threshold matrix shows what is average feature revelation for each subgroup. Using

Table 3. Demographic of features revelation by gender, age, relationship, and politic preference

	Gender		Age				Relationship status					Political preference						
	Male	Female	15-19	20-24	25-29	30-Up	S	IR	E	M	OR	VL	Li	Mo	Con	VC	A	Ln
Age	0.83	0.51	x	x	x	x	0.84	0.84	0.83	0.86	0.92	0.85	0.82	0.84	0.86	0.76	0.84	0.87
Hometown	0.64	0.39	0.68	0.64	0.54	0.48	0.63	0.64	0.72	0.67	0.67	0.65	0.65	0.66	0.64	0.66	0.64	0.81
Cur. resident	0.29	0.16	0.28	0.28	0.28	0.17	0.27	0.28	0.31	0.36	0.25	0.31	0.32	0.31	0.27	0.26	0.39	0.24
Gender	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Relationship	0.85	0.53	0.85	0.86	0.87	0.87	x	x	x	x	x	0.90	0.83	0.88	0.89	0.88	0.92	0.90
Political view	0.66	0.38	0.48	0.65	0.66	0.83	0.65	0.64	0.70	0.70	0.50	x	x	x	x	x	x	x
Activities	0.68	0.40	0.68	0.66	0.65	0.70	0.68	0.67	0.67	0.67	0.50	0.62	0.71	0.70	0.68	0.74	0.69	0.79
Interests	0.84	0.52	0.78	0.85	0.83	0.70	0.85	0.84	0.83	0.84	0.75	0.88	0.86	0.88	0.84	0.88	0.91	0.87
Music	0.88	0.55	0.87	0.88	0.87	0.78	0.90	0.89	0.86	0.85	0.75	0.91	0.92	0.91	0.88	0.96	0.96	0.90
TV shows	0.64	0.43	0.79	0.67	0.59	0.61	0.68	0.66	0.72	0.69	0.75	0.66	0.72	0.73	0.66	0.72	0.74	0.73
Movies	0.85	0.54	0.83	0.86	0.85	0.83	0.87	0.86	0.89	0.83	0.92	0.88	0.89	0.90	0.86	0.88	0.89	0.91
Books	0.75	0.47	0.65	0.77	0.73	0.78	0.78	0.75	0.78	0.77	0.58	0.85	0.82	0.80	0.76	0.86	0.88	0.93
High school	0.92	0.59	0.92	0.95	0.92	0.87	0.93	0.93	0.92	0.95	0.92	0.96	0.94	0.94	0.95	0.84	0.91	0.89
Education	0.98	0.62	1.00	0.99	0.99	1.00	0.99	0.99	0.99	0.99	1.00	1.00	1.00	0.99	0.98	1.00	0.96	1.00
Note	0.21	0.14	0.44	0.21	0.15	0.22	0.25	0.21	0.15	0.17	0.42	0.31	0.29	0.22	0.14	0.20	0.21	0.26
Wall	0.96	0.60	0.93	0.96	0.98	0.87	0.96	0.96	0.94	0.98	1.00	0.91	0.94	0.97	0.96	0.98	0.96	0.97

revelation matrix, threshold is calculated as Eq. (2), where T_j is average profile —feature revelation for subgroup j and $|i|$ is size of the feature set.

$$T_j = \frac{1}{|i|} \sum_i R_{i,j}. \tag{2}$$

Threshold matrix shows that what is average probability for each subgroup.

6.3 Configuring Privacy Setting

To find a suitable privacy setting for profile features, we use joint probability technique on the four —main features: age, gender, relationship status, and political prefernce. Because the statistical analysis is done on main features with replacement (*independent variables*), the probability that users reveal their profile features is the product of the main features.

After completing phase 1: building revelation and threshold matrices, configuration of privacy settings can take place. Unlike phase 1, phase 2 takes place every time a new user joins a network. Probability of revealing a feature is calculated by joint probability of four main features of personal information, and it is compared against joint probability of threshold value of given subgroups. If the value is greater then threshold's value, the feature is set to be accessible by platform applications (3), otherwise the feature is not accessible (4), where U_p is a set of person p's personal information e.g., $U_1 = \{Male, 24, S, Mo\}$.

$$if \left(\prod_{k \in U_p} R_{i,k} \right) > \left(\prod_{k \in U_p} T_k \right), accessible. \tag{3}$$

Table 4. Threshold matrix is built for categories of gender, age, relationship status, and political preference

	Gender		Age				Relationship status					Political preference						
	Male	Female	15-19	20-24	25-29	30-Up	S	IR	E	M	OR	VL	Li	Mo	Con	VC	A	Ln
Threshold	0.73	0.46	0.73	0.73	0.71	0.69	0.73	0.73	0.74	0.74	0.71	0.76	0.77	0.77	0.74	0.76	0.78	0.79

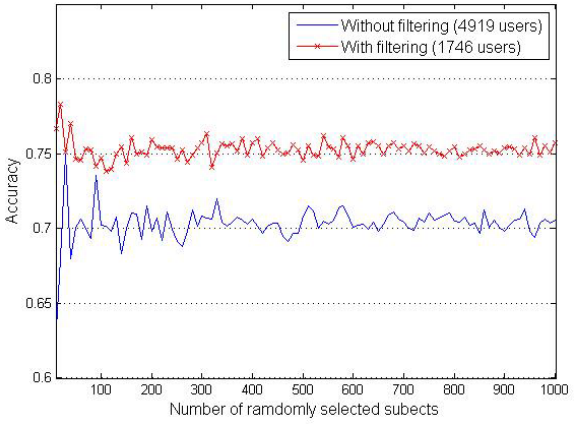


Fig. 6. Comparing accuracy of privacy management system using filtered dataset of 1,746 users with unfiltered dataset of 4,919 users. The system shows notable high error tolerance.

$$if \left(\prod_{k \in U_p} R_{i,k} \right) \leq \left(\prod_{k \in U_p} T_k \right), not\ accessible. \tag{4}$$

Let's take an example to show how automatic configuration of privacy setting works. A new user who is male, 24 years old, single, and moderate-political preference joins the UNT network. By default, all features are inaccessible. Based on Tab. 3, we observe that probability of the user's revealing age is comparing joint probability (revelation matrix) of 83% (Male), 84% (S), and 84% (Mo) against joint probability (threshold matrix) of 73% (Male), 73% (20-24), 73% (S), and 77% (Mo). Result is 59% (revelation matrix) $>$ 30% (threshold matrix), so the user's age is accessible by the applications.

7 Performance

To evaluate the performance of PPS, we test PPS with two sets of data. Based on our dataset, we find that 3,173 (65%) of 4,919 users do not provide one or more of the main features (age, relationship status, or political views). One dataset has all 4,919 members without any alteration, and the other one is filtered such that there are only users who have all four main features provided. The performance of PPS in terms of accuracy rate is shown in Fig. 6 where the accuracy rate is measured by correctly configured privacy settings of randomly selected users from the dataset. After the system configures the users' privacy settings for each feature based on the their personal information, we compare the configuration with the user's actual setting. Without filtering the data, the accuracy converges to 70%. On the other hand, with filtered the data, the accuracy of privacy configuration converges to 75%. Even though 65% of 4,919 users lack one or

more of the personal information, PPS still able to perform 70% accuracy. In other words, only five percent less than 75% indicates that system has *high error tolerance*.

8 Conclusion

Social networking boundaries appear to have been pushed in every way possible to allure new users and to keep current users. Open platform gives great flexibility to application developers to be creative and innovative as possible. Even though it gives benefit to both Social Network Sites and to application developers, customers' private information can be unawarely accessed. Not all developers are legitimate. Without careful consideration of privacy management, open platforms result in information harvesting for illegal or unethical purposes. We purpose a privacy management system as a solution to the privacy problems on SN sites. The system uses probabilistic approach based on information revelation of users to recommend a more appropriate privacy setting for the user. The system restricts access to users' personal information unless they wish to make the information available. Our experiment shows that our approach can achieve 75% accuracy. In addition its high error tolerance makes it a suitable technique for user content management environment.

It is arguable to apply opt-out privacy model, where all profile information are inaccessible as default. However, from business point of view, the users' profile information are asset. This could be a reason that Facebook uses opt-in privacy model. Disadvantages of using opt-in model are that new users trust the system and platform applications, that all profile information are accessible as default, and that inexperienced users are unaware of their personal information are being harvested. Thus, we believe that the PPS can facilitate new user's profile settings by not having to reveal all personal information which are not intended to share with unknown users.

Acknowledgments

This work is supported by the National Science Foundation under grants CNS-0627754, CNS-0619871and CNS-0551694. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. We would like to thank our anonymous reviewers for their insightful and helpful comments and suggestions.

References

1. Hargittai, E.: Whose space? differences among users and non-users of social network sites. Journal of Computer-Mediated Communication 13(1) (2007)
2. Nie, N., Hillygu, S.: Where does internet time come from?: A reconnaissance. IT & Society 1(2), 1–20 (2002)

3. Acquisti, A., Gross, R.: Imagined communities: Awareness, information sharing, and privacy on the facebook. In: Danezis, G., Golle, P. (eds.) PET 2006. LNCS, vol. 4258, pp. 36–58. Springer, Heidelberg (2006)
4. Boyd, D.: Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. Massachusetts Institute of Technology, Cambridge, MA (2008)
5. Zukowski, T., Brown, I.: Examining the influence of demographic factors on internet users information privacy concerns. In: SAICSIT Conf., pp. 197–204 (2007)
6. Barnes, S.B.: A privacy paradox: Social networking in the united states. First Monday 11(9) (August 2006)
7. Alexa: Facebook.com - facebook. Technical report, alexa.com (2007)
8. Facebook: Facebook developers. Technical report, facebook.com (2007)
9. McCarthy, C.: Facebook platform attracts 1,000 developers a day. Technical report, CNET News.com (2007)