Monitoring and Recommending Privacy Settings in Social Networks

Kambiz Ghazinour
University of Ottawa
School of Electrical Engineering
and Computer Science
Ottawa, ON, K1N 6N5, Canada
kghazino@uottawa.ca

Stan Matwin
Dalhousie University
Faculty of Computer Science
Halifax, NS, B3H 4R2, Canada
stan@cs.dal.ca

Marina Sokolova
Electronic Health Information Lab
CHEO Research Institute
Ottawa, ON,K1H 8L1, Canada
msokolova@ehealthinformation.ca

ABSTRACT

Ensuring privacy of users of social networks is probably an unsolvable conundrum. It seems, however, that informed use of the existing privacy options by the social network participants may alleviate - or even prevent - some of the more drastic privacy-averse incidents. Unfortunately, recent surveys show that an average user is either not aware of these options or does not use them, probably due to their perceived complexity. It is therefore reasonable to believe that tools assisting users with two tasks: 1) understanding their social network behavior in terms of their privacy settings and broad privacy categories, and 2) recommending reasonable privacy options, will be a valuable tool for everyday privacy practice in a social network context. This paper presents early research that shows how simple machine learning techniques may provide useful assistance in these two tasks to Facebook users.

Categories and Subject Descriptors
K.4.1 [Computers and Society]: Public Policy Issues – Privacy

General Terms
Algorithms, Design, Experimentation.

Keywords
Social network, Privacy, Facebook, Recommender system, classification.

1. INTRODUCTION

1.1. Data Privacy

Modern social network and services have become an increasingly important part of how users spend their time in the online world. The social network is a proper vehicle for people to share their interests, thoughts, pictures, etc. with their friends or the public. While sharing information about the self is intrinsically rewarding [8], the risk of privacy violation increases due to disclosing personal information. Recent cases, such as Canada's Privacy Commissioner challenge to Facebook's privacy policies and settings, have shown a growing interest on the part of the public with respect to how social network and services treat data entrusted to them[1]. Some of the privacy violation incidents could be mitigated or avoided if people used more privacy setting options.

Facebook with current number of 955 million users[2] and still growing is the most popular social network and as such motivates work on privacy settings and issues. Over the past several years, Facebook has provided many privacy settings and options are for the users. Unfortunately most users do not know the importance of privacy settings, do not have enough time to read and comprehend tedious and long pages of privacy settings or simply do not understand how these settings available for them work. It also becomes more concerning when we realize that the default privacy settings for the posts, photo albums, etc. are set as *being visible to the public*.

1.2. Facebook

In a most recent survey (May 2012) by Consumer Report Magazine in the U.S., 2,002 online households, including 1,340 that are active on Facebook, were questioned and then the data was extrapolated to estimate national totals, hence the results are given in terms of absolute numbers with respect to the U.S. population (169 million monthly active users in the U.S. as of March 31, 2012). The results from privacy point of view raise some concerns as follows:

1) Some people are sharing too much. 4.8 million people have used Facebook to say where they planned to go on a certain day which is a potential tip-off for burglars, and that 4.7 million *liked* a Facebook page about health conditions or treatments (details an insurer might use against them).

2) Some people do not use privacy controls. Almost 13 million users said they had never set, or did not know about, Facebook's privacy tools. And 28% shared all, or almost all, of their wall posts with an audience wider than just their friends.

3) And problems are on the rise. 11% of households using Facebook said they had trouble last year, ranging from someone using their log-in without permission to being harassed or threatened. That projects to 7 million households -30% more than last year.

EDBT/ICDT '13 , March 18 - 22 2013, Genoa, Italy
Copyright 2013 ACM 978-1-4503-1599-9/13/03…$15.00.

[1] http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm, access date: July 30th, 2012.

[2] "Facebook Current Report, Form 8-K, Filing Date July 26, 2012". secdatabase.com. Accessed August 5th, 2012.

Although these results were inferred based on the data collected from the users in the United States, nothing suggests the results for the rest of the words would be less concerning.

Our approach to remedy this situation would be to develop a tool that monitors and suggests a privacy setting to the user rather than leaving the privacy settings as default or even setting them too loose that basically little privacy, if any is protected.

1.3. Our contributions

The purpose of this work in progress is to present two tools: Privacy *monitor* and *recommender* system. In other words:

- A tool that allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors and detects the possible privacy risks. It monitors by providing a brief review for the users (in their user interface).

- A tool that acts as a recommender system and shows the attributes that play important role in setting privacy preferences for individuals on a social network. Recommending a privacy setting occurs based on the notion of *collaborative filtering* and the similarity of the preferences chosen by the user who desires to set the privacy setting and the other users who share common preferences.

Our final goal is to demonstrate that a recommender system for privacy setting could be developed, in which the system would suggest privacy settings that have been "learned" for a given profile (cluster) of users.

2. RELATED WORK

The domains of privacy settings and recommender systems have started to attract researchers' attention in recent years. As more options are given to the users to set their privacy preferences, users are more confused, frustrated or sometimes simply ignorant about setting them. As in the Facebook case, the privacy settings are hard to be set and users with average knowledge about computers cannot easily find or set the privacy settings as they should be.

In 2011, Bejugam and Lefevre [1] introduced the privacy policy simplification problem and presented *enList*, a system that uses automatically extracted friend lists to concisely represent social network privacy policies. They also conducted a laboratory-based user study to evaluate the effectiveness of the concise representation compared to a verbose representation. Their study demonstrated that their method resulted in better accuracy for policy comprehension, recollection and modification tasks.

Li *et al.* [5] present a dynamic trust-based privacy assignment system which assist people select the privacy preference on-the-fly to the piece of content they are sharing, where trust information is derived from social network structure and user interactions. Their model using a cosine similarity function detects a two-level topic sensitive community hierarchy and then assigns privacy preference for users based on their personalized trust networks. They demonstrate the feasibility and effectiveness of their model on a social object network dataset collected from Flickr.

In another example, Li *et al.* [6] propose an intelligent semantics-based privacy configuration system, named SPAC, to automatically recommend privacy settings for social network users. SPAC learns users' privacy configuration patterns and make predictions by utilizing machine learning techniques on users' profiles and privacy setting history.

3. DATA PRIVACY

3.1. Internet privacy and preferences

Ideally, a definition for internet privacy would be the ability to control (1) what information one reveals about oneself, and (2) who can access that information. Essentially, when the data is collected or analyzed without the knowledge or consent of its owner, privacy is violated. When it comes to the usage of the data, the owner should be informed about the purposes and intentions for which the data is being or will be used. Last but not least, when a data collector wants to disclose the data to other individuals or organizations, it should be with the knowledge and consent of the data provider.

Information revelation and internet privacy becomes even more obvious in online social networks. Gross *et al*. [3] analyze the online behavior of more than 4000 Carnegie Mellon University students who are member of Facebook. The authors evaluate the amount of information the students disclose and study their usage of the site's privacy settings. Their study reveals that a large number of the participants are unconcerned or simply pragmatic about their privacy.

People have different privacy concerns and therefore there is no single privacy policy that fits every data provider/owner. For instance, one data owner may be concerned about revealing the home phone number to a potential third-party and another data owner may be unconcerned. Westin has conducted over 30 privacy surveys [4] and has classified people into three groups: *High and Fundamentalist, Medium and Pragmatist, Low and Unconcerned*. Privacy fundamentalists are described as unwilling to provide any data on web sites and are highly cautious about revealing their personal information. Privacy pragmatics are willing to compromise their privacy if they gain some benefits in return. And the third groups of people are those unconcerned with their privacy at all and are willing to reveal and disclose any information upon request. These surveys demonstrate that more people are getting concerned about their privacy because they feel they are losing control over their data.

3.2. Privacy elements

We review the key elements of data privacy. This helps to identify the predicates that should be involved in measuring a privacy preference, the *purpose, visibility* and *granularity* [2]:

- Purpose defines the intention of the data provider for how data can be used after collection (e.g., members provide their mailing address to Amazon.com for the purpose of "shipping orders").
- Visibility defines who is allowed to see the provided data (e.g., members of Facebook can specify what group of people can visit their profile, *friends*, *friends of friends* and etc.). Visibility of data is an important key in ensuring appropriate system utility.
- The granularity of data defines how much precision is provided in response to a query (e.g., data providers could define whether their exact age is shown or a range such as child, teenager, and adult).

Currently in Facebook and other social networks, the privacy settings (not the privacy policies) which are available for the users to set their privacy preferences, only visibility and in rare cases granularity of the data can be defined and there is absolutely no control on the purpose for which the data can be seen. For instance, in Facebook the users can choose that only the day and month (and not year) of their date of birth be visible to their friends. Hence in this research we focus on the visibility feature of data and the way it has been set by the user as an indicator about how important the privacy is for that individual. Other than *posts* that Facebook provides a very limited access to them for the researches, we focus on *photo albums* and study the privacy settings chosen by the users on their photo albums as a measurement scale for the individuals' attitude towards serving their privacy.

4. DATA PRE-PROCESSING

4.1. Representing data in a vector space

Regarding the data collection, we were interested in building our training set with the following four groups of data from the users:

- *User's profile*; There are several attributes stored in a user profile, ranging from user's ID and name to the work experience and even time zone. Table 1 shows the attributes we collected from Facebook user profiles, their formats and pre-defined values.
- *User's interests*; on each Facebook profile users have the option of expressing what they are interested in. For instance, what kind of movies they watch, books that they read, music they listen to, sport they do or watch, and many other activities. We collected the interest id and its category that it belongs to. There are around 196 distinct categories defined in Facebook. Since each item has a unique ID it can be compared among people to realize who shares the same interest(s). Table 2 shows the attributes we collect from Facebook regarding the user's interests and their descriptions.
- *User's privacy settings on photo albums*; The Album object has several attributes including the title, description, location, cover photo, number of photos, created time, and etc. We only collected the name and privacy settings of the album which had predefined values as shown in Table 3.
- *User's privacy settings on posts*; User's posts have several different attributes depending on the type of the post. For instance, if the post is a link, then: The link attached to this post, the name of the link, the caption of the link (appears beneath the link name), a description of the link (appears beneath the link caption), a URL to a Flash movie or video file to be embedded within the post, and etc. However, as illustrated in Table 4, we are only interested in post type, privacy setting of the post and the created time.

These collected data will be utilized by the recommender system to find the similarities between the individuals. For each user *u*, we represent the profile as a vector V_u as follows:

$$V_u = [D_u ,PR_u]$$

$$\text{where } D_u = [P_u ,I_u].$$

D_u consists of the set of P_u (user's profile attributes) and I_u (the set of user's interests). PR_u is the set of user's privacy setting for their photo albums and posts. For instance:

P_u= [gender, age, location, relationship_status, education, political view];

I_u = [interest categories: interest instances];

PR_u=[number of photo albums, number of albums visible to public, number of albums visible to friends of friends; number of posts, number of posts visible to public, number of posts visible to friends of friends].

Example 1 – The vector *V* for a user, John, might appear as follows:

V_{John}=[Male, 30, USA, Single, Grad, Liberal, TV: The Big Bang Theory, Sport: Basketball - Golf; 20,4,5; 15,0,0].

Several points that should be noted:

1) There are some attributes that are not defined on Facebook by the users in their profiles. It is not that they have not let our application see the value; they simply have not entered any value for that. Although this makes the job of our training set and the similarity function hard, it has a hidden message in that which will help us later when our recommender system, suggest a proper privacy setting for an individual whose profile is examined against our set. For example, Sandrine has not entered any value for her relationship status, which clearly demonstrates that she does not feel comfortable sharing that which is a privacy protection gesture. When nothing is shared, no privacy violation occurs too!

Table 1 – Some of the attributes collected from user's profile

Attribute	Description
Name	The user's full name. `string`.
Gender	The user's gender: `female` or `male`. ’string`.
Birthday	The user's birthday. `user_birthday` or `friends_birthday`. Date `string` in `MM/DD/YYYY` format.
Education	A list of the user's education history. `user_education_history` or `friends_education_history`. `array` of objects containing `year` and `type` fields, and `school` object (`name`, `id`, `type`, and optional `year`, `degree`, `concentration` array, `classes` array, and `with` array).
hometown	The user's hometown. `user_hometown` or `friends_hometown`. object containing `name` and `id`.
relationship_status	The user's relationship status: `Single`, `In a relationship`, `Engaged`, `Married`, `It's complicated`, `In an open relationship`, `Widowed`, `Separated`, `Divorced`, `In a civil union`, `In a domestic partnership`. `user_relationships` or `friends_relationships`. `string`.
religion	The user's religion. `user_religion_politics` or `friends_religion_politics`. `string`.

Table 2 - Attributes collected from users interests

Attribute	Description
Interest ID	ID of the interest. ‘string’
Interest Category	Name of the category that the interest belongs to such as artist, car, restaurant, movie, etc. ‘string’

Table 3 – Attributes collected from photo albums

Attribute	Description
Name	Title of the album. ‘string’
Privacy value	EVERYONE, FRIENDS, FRIENDS_OF_FRIENDS, NETWORKS_FRIENDS CUSTOM. ‘string’

Table 4 – Attributes collected from posts

attribute	Description
Post type	A string indicating the type for this post (including link, photo, video, status)
Privacy value	May specify one of the following strings: EVERYONE, ALL_FRIENDS, NETWORKS_FRIENDS, FRIENDS_OF_FRIENDS, CUSTOM.
Created time	String containing ISO-8601 date-time

2) Another important aspect of finding the similarity is the importance and weight of the attributes. For instance, does gender play a bigger role or age? Are Alice and Sandrine as two ladies more similar or John and Sandrine as two 30 year old individuals?

To answer these questions we will check the similarity of the privacy settings as well which will be tested from two different perspectives: *existence of the values*(e.g. if the photo album exist) and *value closeness* (e.g. is it set to be visible to the public or friends of friends).

The privacy preferences of the users are measured by examining the privacy settings they have chosen for their photo albums and posts as mentioned earlier. We count the total number of albums and check to see if there any of them are set visible to *public, friends of friends, friends* or simply *customized* otherwise and also calculates the ratio. For instance, assume John has 25 photo albums and only one of them is set visible to the public and Alice has 2 albums from which one is set visible to the public. We can predict that probably John is more cautious about his privacy of the albums than Alice. Furthermore, if Sandrine has put no photo albums this might indicate that she is even more cautious than John. Since posting photo albums on Facebook is a very common act and very easy to be done the assumption that Sandrine did not know how to put photo albums on her profile to justify why she has 0 photo albums does not seem to be a valid reason.

4.2. Recommend to hide the values

We would like to advance one step further and review the data that the user did not provide on their profile (P_u), what we have previously referred to as *the existence of the values.* For instance, the *relationship status* and *political view* were not provided by Sandrine and Alice respectively. Although this is partially captured by the difference that it causes in the vectors and their result in similarity functions, this can be used as a recommendation to the individual who is seeking advice from the system to how to set their privacy settings. For instance, if John is more similar to Sandrine in terms of the user profile, then the system not only recommends that John should have a privacy setting similar to Sandrine for the photo albums and posts, but also advices John not to reveal his relationship status (the same pattern that Sandrine followed).

4.3. Classification

In the first step, we need to perform a profiling task to profile the users based on their attitude toward privacy. As discussed in Section 3.1, Westin categorizes people into three different groups of fundamentalists, pragmatics and unconcerned [4]. In this research work we examine the users' attitude towards sharing their photo albums as an indication of their privacy values and to which group they more likely belong too. We use photo albums since users treat them as a very personal and tangible type of personal identifiable information. Furthermore, it is one of the data items that Facebook allows us to check its privacy settings using the Facebook API functions.

To perform the profiling phase, we look at each individual's ratio of albums visible to *public*, *friends of friends*, *friends*, and *custom*. For simplicity we use the following rule to determine to which of the Westin's three privacy groups the user belongs to:

```
If # of photo albums shared == 0 then:
        The user's privacy_category = Fundamentalist.
Else if ratio of photos visible to friends + ratio of photos
visible to custom > %50 then:
        The user's privacy_category = Pragmatic.
Else:
        The user's privacy_category = Unconcerned.
```

After obtaining values for the privacy_category attribute of each user, we then use the standard decision tree to infer the profile type of each user.

For the recommendation task, we use the k-nearest neighbor algorithm. Due to a relatively small data we have, we use a K=3.The idea is that when a user joins the Facebook we put them in the KNN classifier and determine to which privacy setting class they belong to. Then, considering the specifications of that class, the recommender system suggests the user what data should be disclosed and which ones should not be shared.

5. EMPIRICALEVALUATION

5.1. Facebook application

We implemented a Facebook application written in JavaScript and PHP in order to access the Facebook user`s profile and settings.

We asked 50 undergraduate students from three universities (two in Canada and one in Brazil)via email to participate in this research if they have a Facebook profile.

We informed them that the overall goal of this research is to assist people with using privacy settings in popular social networks, and specifically in Facebook, by developing a recommender system for privacy settings. They were told that in this project we wanted to investigate if there is a relationship between the personal information and interests of the Facebook users, and the way they choose their privacy settings. They were informed that this research requires some basic data collected on a voluntary basis from Facebook users. We explained that as the project was done in a university environment, we naturally focused on students and that was why we asked their help with data collection. They were also informed about the following procedures:

They do not need to answer any questionnaire or survey. After they log in to their Facebook account and enter the address https://apps.facebook.com/privacy_check they just need to give their consent for this application to access to their information and privacy settings.

They needed to run this application only once – since the data collection phase happened just for one time. The application extracted some basic information that discussed in Section 4.1 and the information was stored in a comma separated text file on the server which was password protected.

In the next phase, the application went through the photo albums of the participant and retrieved the number of albums and the privacy setting of each album.

The application gave a brief report to the participant, listing the photo albums which were visible to *everyone (public)* or *friends of friends*. The application assumed that when the user created a photo album and uploaded photos, they intended their friends (or friends in their network) to see them, so if the privacy setting was set to *friends of friends* or everyone then the application notified them to tighten their privacy settings by referring them to the name of the photo album.

For example, the application may find two problems in the photo albums of a user who runs this app. The album "wall photos" are set visible to the *public* and the album "mobile uploads" are set visible to *friends of friends*. The application recommends that the user tightens the privacy setting of these two albums to reduce potential privacy breaches.

The participants were also told that the collected data will not be disclosed to any third-party and will be anonymized to be used for research purposes only.

5.2. Recommending privacy settings

We have used a simple approach to recommend a binary privacy setting based on the use of the k-nearest neighbor (KNN) classifier to suggest that value. Note that the use of KNN makes this classifier work like a collaborative filtering recommender system [7].

We used the KNN in Weka with K=3 to classify the participants based on their common personal information they have disclosed, such as *age*, *education*, *hometown* and their preferences such as *political views*, *religion* and etc. Hence, our training data set would be the individuals with binary values of their profile attributes they have disclosed or not. Due to our small set data, we performed five replications of twofold cross-validation. In each replication, our collected data set were randomly partitioned into two equal-sized sets in which one was the training set which was tested on the other set. Then we calculated the average and variance of those five iterations for three different attributes of *education*, *location* and *relationship status*. Table 5 shows the results of this 5X2-fold cross validation.

Table 5 – 5X2-fold cross validation

Attribute Average 5X2	Education	Location	Relationship status
Correctly classified instances	87%	82%	60%
Mean absolute error	0.1772	0.2488	0.4274

The following example clarifies the way the recommender system suggests user's privacy settings to disclose an attribute or not.

Example 2 – Alice has entered her information on her Facebook profile. Her profile shows that she has disclosed the following attributes: name, gender, hometown, education, relationship status and age (year of birth). The system also recognizes that Alice has not disclosed her political views, religion, location, degree and month of birth. The model puts the information through the 3-nn classifier and recognizes that she should not disclose her education attribute.

In brief, based on the information she has disclosed and the topics that she has shown interest in, the system uses a 3-nearest neighborhood classifier and finds the three closest profiles in which they have disclosed same attributes. Knowing those three records, the system identifies if those profiles disclose education level or not and recommends Alice to do so.

It should be pointed out that the recommender systems is only interested to tighten the privacy setting and for example never recommends that an attribute that the user has decided not to share, should be disclosed.

6. CONCLUSION AND FUTURE WORK

In this research work, we introduced a tool that works as a monitoring and recommending system for privacy settings in a social network, Facebook. We described that since a large portion of Facebook users do not change their privacy settings on Facebook the system is beneficial that monitors and suggests a privacy setting to the user rather than leaving the privacy settings as default (which is set visible to public) or even setting them too loose that basically little privacy, if any, is protected.

Next, we performed an empirical study on real world data to demonstrate the feasibility of our model and proof of concept.

We plan to perform our experiment with a larger dataset to demonstrate the scalability of our model with a larger training set. We have already started publicizing the Facebook application that we have developed to be also used as a tool to raise awareness and educate Facebook members about the possible weakness of the privacy settings of the photo albums that were unwillingly shared with public or friends of friends. Due to space limit we briefly presented our findings and plan to publish a comprehensive set of results with a larger target of Facebook users in the future.

Our vision for the future deployment and use of the recommender part is as follows. In a given population (e.g. High-school students) a group of privacy-aware volunteers would make their profiles available as a training set for our system. Note that just a one-time read of the profile of the volunteer participants is involved in building the training set. Subsequently all other members of this population could use suggestions from the system for their settings of profile elements (disclose/do not disclose). As these suggestions would be based on informed decisions of more privacy-aware but otherwise similar members of the same population, they would appear reasonable to the users while being at the same time privacy-aware.

It will also be an interesting project to study the sensitivity of data disclosed. Some information are more sensitive than others, for example, personal health information or exam grades are more sensitive that the photo albums for certain individuals.

As another future research direction we would like to perform a deeper analysis on the profiling phase of our study. We understand that existence of photo albums that are set visible to public by itself may not be a good indicator of a privacy unconcerned user. It is possible that the user takes pictures of the nature or his art works and set it visible to the public which does not imply any privacy violations. In the next step we would examine if the user or other individuals closely related to them are tagged or mentioned in the pictures that sharing them may result in privacy violations.

7. REFERENCES

[1] R. Bejugam, K. LeFevre: "enList: Automatically Simplifying Privacy Policies", *Data Mining Workshops (ICDMW), 2011 IEEE 11th International Conference on* , vol., no., pp.620-627, Dec. 2011.

[2] K. Ghazinour & K. Barker: "Capturing P3P semantics using an enforceable lattice-based structure". PAIS 2011: 4.

[3] R. Gross & A. Acquisti. "Information revelation and privacy in online social networks". The WPES'05, Alexandria, Virginia. 2005.

[4] P. Kumaraguru and L.F. Cranor. "Privacy indexes: A survey of westin's studies". Technical Report CMU-ISRI-5-138, Carnegie Mellon University, CMU, Pittsburgh, PA, USA, December 2005.

[5] Q. Li, J. Li, H. Wang, and A. Ginjala: "Semantics-enhanced privacy recommendation for social networking sites". In Proc. TrustCom, pages 226–233, Nov. 201

[6] L. Li; T. Sun; T. Li: "Personal Social Screen-A Dynamic Privacy Assignment System for Social Sharing in Complex Social Object Networks," Privacy, security, risk and trust (passat), 2011 vol., no., pp.1403-1408, 9-11 Oct. 2011.

[7] J.B. Schafer, D. Frankowski, J. Herlocker, S. Sen: "Collaborative filtering recommender systems". In: Brusilovsky, P., Kobsa, A., Nejdl, W. (eds.) The Adaptive Web, pp. 291–324. Springer, Berlin, 2007.

[8] D. I. Tamir and J. P. Mitchell. "Disclosing information about the self is intrinsically rewarding". PNAS 2012: 1202129109v1-201202129.