Measuring Privacy Leaks in Online Social Networks

Agrima Srivastava
Department of Computer Science and
Information Systems
BITS Pilani, Hyderabad Campus
Hyderabad,India
Email: agrimasrivastava1@gmail.com

G Geethakumari
Department of Computer Science and
Information Systems
BITS Pilani, Hyderabad Campus
Hyderabad,India
Email: geethamaruvada@gmail.com

***Abstract*—Online Social Networking has gained huge popularity amongst the masses. It is common for the users of Online Social Networks (OSNs) to share information with digital friends but in the bargain they loose privacy. Users are unaware of the privacy risks involved when they share their sensitive information in the network. The users should be aware of their privacy quotient and should know where they stand in the privacy measuring scale. In this paper we have described and calculated the Privacy Quotient i.e a privacy metric to measure the privacy of the user's profile using the naive approach. In the starting of the paper we have given the detailed analysis of the survey that we have carried out to know how well do people understand privacy in online social networks. At last we have proposed a model that will ensure privacy in the unstructured data. It will make use of the Item Response Theory model to measure the privacy leaks in the messages and text that is being posted by the users of the online social networking sites.**

Keywords*—*privacy quotient;social networks;unstructured data privacy

I. INTRODUCTION

OSNs have moved from niche phenomenon to mass adoption. It provides an infrastructure so that people can communicate with each other, exchange information, express their feelings and build and maintain a relationship with other users on the internet. A huge number of people are a part of OSNs. Some of the popular OSNs are Facebook, Twitter, Flickr, Linked-in etc. [1]. One of the main concerns of Online Social Networks is data security. Privacy plays an equally important role in data security. Data protection essentially means certain sets of laws, policies and varying procedures that aim in making the data secure and reducing the intrusion into an individual's privacy. This intrusion can be caused by the collection, storage and dissemination of personal data [2]. Many developing countries do not guarantee the fundamental right to privacy but there are certain existing fundamental rights like the freedom of speech and expression and the right to life and personal liberty that relates to the right of privacy. In India, the Indian Information Technology Act, 2000 deals with the compensation and punishment in case of wrongful disclosure and misuse of personal data or the violation of contract with respect to the personal data [5].

The advancement of World Wide Web has led to the significant growth in the usage of the Online Social Networks (OSNs). This advancement of technology is accompanied by huge privacy concerns [3]. Privacy is a valuable concept but is a mere perception. Intrusion upon a person's seclusion or solitude, public disclosure of embarrassing private facts about an individual placing one in a false light in the public eye are some of the practices that can end up hampering an individual's privacy.

A profile is a digital representation of an individual. It is enriched with data like the name, phone number, address, work place, school, religious views, political views, relationship status, interests, photos etc. Some of this information may be sensitive and any kind of disclosure would significantly harm the individual's privacy. In the real world where the information is ephemeral, the information remains for an infinite time on the web thereby posing a great risk on the privacy of online users. Most of the time users are unaware of the potential risks involved when they are sharing any sensitive information online [4]. Whenever and wherever a personal identifiable information is shared and stored privacy concerns are bound to arise. OSN data is of great help to the researchers, analysts and any third party. These external entities can mine this data and use it for various purposes like spamming [5], fishing, targeted advertising, uncovering interaction pattern in business process to provide better services and develop innovative opportunities, identification of the influential person in the network, detection of implicit and hidden groups, sensing user's sentiments for proactive planning etc. [6].

Another important issue which has not received much attention is the privacy protection in exchanging, sharing, publishing, and disclosing unstructured data in an OSN. Based on the experiments we have carried out and the analysis of results we identify a few challenges that are promising and need to be addressed. The problem with unstructured data processing is that it is computationally hard. In general, it is hard to find a solution that provides sufficient privacy protection and retains enough data utility. The problem becomes even harder with unstructured data as they are usually sparser hence more vulnerable to attacks.

Our paper is organized as follows, Section II describes the related work, Section III of the paper deals with the detailed analysis of the survey on privacy in online social networks. In Section IV we have utilized this data and calculated the privacy quotient of the users using the naive approach. In Section V we have proposed a model that could cater the needs of privacy in an unstructured online social network data. At last in Section VI we have given the

978-1-4673-6217-7/13/$31.00 ©2013 IEEE

conclusion and stated future work.

II. Related Work

A lot of research exist for privacy preserving data mining and publishing but not much has been explored about measuring privacy [7][8]. Liu et al have provided an intuitively and mathematically sound methodology for computing privacy scores of users in the OSNs by making use of the Item response Theory [9]. Considering the problem of privacy settings and it's management Fang et al have proposed a template for the design of a social networking privacy wizard that could build a model to concisely describe the user's preferences and configure their privacy settings automatically [10]. Braunstein et al have suggested mechanisms for translating responses to indirect questions into privacy ratings and show that this mapping increasingly preserves relative rankings of content types from direct privacy surveys, as more privacy language is introduced [11]. Hiding all the information will make a person less social i.e the utility of the item goes away completely so Shumin et al have proposed a framework to tune the privacy settings keeping a trade off with the utility. They have given a algorithm that would help the OSN users to find the optimal privacy settings [12]. Many tools like PrivAware and systems like Footlight have contributed in the field of privacy too, Becker et al have presented PrivAware a tool to detect and report unintended information loss in Online Social Networks [13]. Anderson et al have described a system called Footlights that addresses the privacy problems in OSNs. It allowed users to control the sharing of private information [14].

III. Detailed Analysis of Survey

We have carried out an extensive survey on privacy in online social networks in the Indian context. Mainly people in the age group of 16-45 were asked to participate. All the participants had a good understanding of computers and social media as we wanted to know that how well do such people understand privacy. 63.33 % of males and 36.66 % of females participated in it.

Gender	Percentage
Male	63.33
Female	36.66

Online social networks plays an active role now-a-days. People often share their personal details like their phone number, email, address, DOB, relationship status, political and religious views etc. on social networking sites. Some of them share sensitive information about them unintentionally whereas some intentionally share their private details. When people were asked whether they share their sensitive information to improve their digital presence in the online social networking world. 21.7 % of people responded yes and 78.33 % of people responded no to the question.

Response	Percentage
Share intentionally (Yes)	21.7
Do not share intentionally (No)	78.33

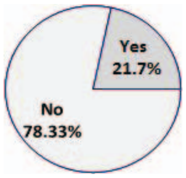

Fig. 1: Pie chart showing the percentage of people who share their information to improve their digital presence.

Posting pictures, videos and tagging friends is a common practice amongst the users in an online social networking media. Doing this without the person's consent can make them uncomfortable. The survey results tell us that 68.33 % of people do not like if some content related to them is made public without their knowledge, out of which 81.18 % were females and 60 % were males.

Response	Percentage
Do not like (Yes)	68.33
Like (No)	31.66

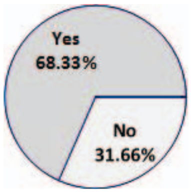

Fig. 2: Pie chart showing the percentage of people who do not like if some content related to them is made public without their knowledge.

With every activity the users do online they are telling the advertisers what to sell them. Social networking sites understands the user better. Many of them are using a software that can track and target the user's interests, likes, activities, relationship status, DOB etc. and suggest them the appropriate advertisements. Survey shows that 81.66 % of users are concerned about how the social media is making use of their information but 18.33 % of the people are not bothered about knowing this.

Response	Percentage
Concerned (Yes)	81.66
Not concerned (No)	18.33

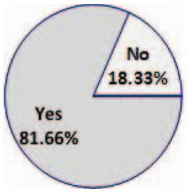

Fig. 3: Pie Chart showing the percentage of people who are concerned about how the social media uses their information.

About 56.66 % of people are not comfortable with social networking sites tracking their use of site and delivering targeted advertisement to them.

Response	Percentage
Comfortable (Yes)	43.33
Not Comfortable (No)	56.66

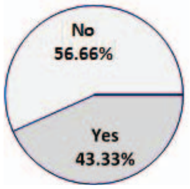

Fig. 4: Pie chart showing the percentage of people who are comfortable with targeted advertising.

Privacy of the users is not only important to them but is equally important to the online social networking sites. Loss of privacy can earn a bad name, loss of revenue etc.
83.33 % of people will stop the use of social networking sites if they find that their personal sensitive information is being used in a way they were not expecting.

Response	Percentage
Stop the use (Yes)	88.33
Continue using it (No)	11.66

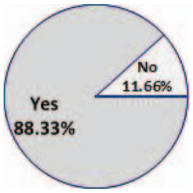

Fig. 5: Pie chart showing the percentage of people who will stop the use of social networking sites if they find that their personal sensitive information is being misused.

Changing the privacy settings could solve the problem of privacy up to a greater extent but is often a confusing, complicated and time consuming task [15]. 63.33 % of the people agreed to it out of which 59.09 % were females and 65.78 % were males. Most of them often tend to skip it. Around 54 % of the people skip the step in which they are asked to change their default privacy settings. We found that around 24% of the users had never changed their privacy settings and were using the default privacy settings.

Response	Percentage
Time consuming and confusing (Yes)	63.33
Comfortable with the procedure (No)	36.66

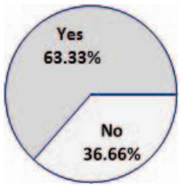

Fig. 6: Pie chart showing the percentage of people who find changing the privacy settings a time consuming and confusing task.

IV. Calculation of the privacy quotient using the naive approach

A lot of research exists for privacy concerns in Online Social Networks that deals in publishing the social network data without revealing the identity of an individual. But not much attention has been paid for the privacy risk that comes by the information that has been shared by the users on their profile i.e an approach towards privacy from the user's point of view [13].

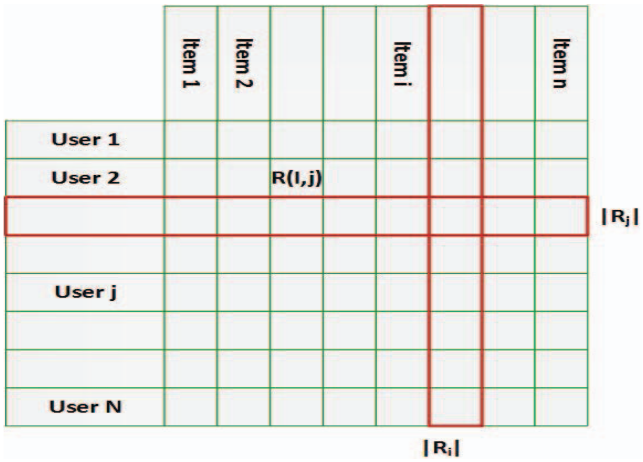

Fig. 7: Response Matrix of size N X n.

We will be working out the on the naive privacy quotient to model our data sets [9]. If there are N number of users and n number of profile items then we can form a response matrix of the order N X n where the range of items i.e i varies from $1 \leq i \leq n$ and the range of users i.e j varies from $1 \leq j \leq N$. Figure 7 shows the response matrix of N number of users and n number of profile items. We have carried out a survey and gathered information about online social networking users over the following lists of 11 items. The cronbach's alpha for all these 11 items is 0.7228, which is ≥ 0.7 and hence will be able to measure the attitude of the user correctly.

TABLE I: List of profile items

Response	Percentage
1	Contact Number
2	E mail
3	Address
4	Birthdate
5	Home Town
6	Current Town
7	Job Details
8	Relationship status
9	Interests
10	Religious Views
11	Political Views

We will be dealing with the dichotomous response matrix which can either take the value of 0 or 1. If a particular user j has shared information about the profile item i, then R(i,j)=1 i.e the information i is made public by the user j. If a particular user j has not shared information about the profile item i, then R(i,j)=0 i.e the information i is made private by the user j. Privacy quotient can be measured on two parameters i.e the sensitivity of the information and the visibility of the information.

A. Calculation Of sensitivity

Sensitivity is the property of an information which makes it private. As sensitivity increases, privacy risks involved in sharing the item also increases. Hiding of such kind of information makes the user more private. Sensitivity (β_i) of an item i can be calculated using the formula

$$\beta_i = \frac{N - |R_i|}{N} \tag{1}$$

where $|R_i|$ = $\sum_j$ R(i,j) i.e the summation of all the cells of the column of profile item i where it has been made public. Figure 7 explains the same. On the basis of the data collected we have calculated the sensitivity of the profile items. The following table illustrates the same.

TABLE II: Sensitivity of the profile items

SNo	Profile Item	Sensitivity
1	Contact Number	.6
2	E mail	.1833
3	Address	.85
4	Birthdate	.1166
5	Hometown	.15
6	Current Town	.1166
7	Job Details	.2
8	Relationship status	.4166
9	Interests	.3
10	Religious Views	.5666
11	Political Views	.6833

We can clearly see in the table II that address is the most sensitive attribute followed by political views, contact number, religious views and relationship status. Whereas birthdate, current town and hometown details are shared by most of the users and are not highly sensitive.

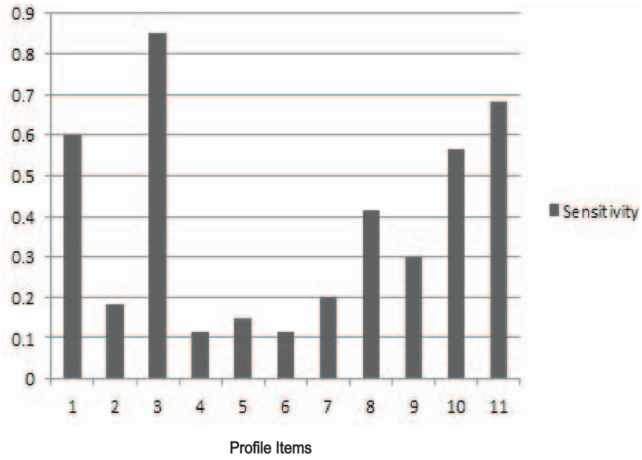

Fig. 8: A bar graph showing the sensitivity of the various profile items.

B. Calculation of visibility

Visibility is the property of information that captures the popularity of an item in the network. The wider is the spread of information the more visible it is. V(i,j) i.e the visibility of a profile item i by the user j is calculated as;
V(i,j) = Pr[R(i,j)=1] X 1 + Pr[R(i,j)=0] X 0;
V(i,j) = Pr[R(i,j)=1] + 0;
V(i,j) = Pr[R(i,j)=1];
where Pr[R(i,j)=1] = Probability that the value of R(i,j)=1;
and Pr[R(i,j)=0] = Probability that the value of R(i,j)=0;

$$V(i,j) = \frac{|R_i|}{N} X \frac{|R_j|}{n} \tag{2}$$

C. Calculation of privacy quotient

If β_i is the sensitivity of the profile item i and V(i,j) is the visibility of the profile item i for a user j. PQ(i,j) is the privacy quotient for a profile item i for user j and is calculated as;

$$PQ(i,j) = \beta_i * V(i,j) \tag{3}$$

To calculate the overall privacy quotient of the user j

$$PQ(j) = \sum_i PQ(i,j) = \sum_i \beta_i * V(i,j) \tag{4}$$

where the range of items i.e i varies from $1 \leq$ i $\leq$ n.

TABLE III: No of users with the Privacy Quotient in the given range

SNo	Range of Privacy Quotient	No of users
1	0.0 - 0.5	0
2	0.5 - 1.0	1
3	1.0 - 1.5	1
4	1.5 - 2.0	5
5	2.0 - 2.5	3
6	2.5 - 3.0	0
7	3.0 - 3.5	6
8	3.5 - 4.0	11
9	4.0 - 4.5	9
10	4.5 - 5.0	8
11	5.0 - 5.5	0
12	5.5 - 6.0	6
13	6.0 - 6.5	8
14	6.5 - 7.0	2

We can see in table III that most of the users are having the privacy quotient in the range of 3.5 - 4.0. Where the highest and the lowest Privacy Quotient obtained are 6.8164 and 0.619672727 respectively.

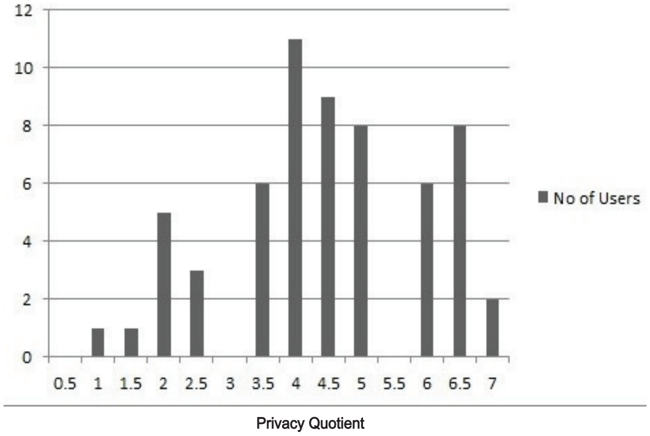

Fig. 9: A bar graph showing the number of users and the range of privacy quotient.

V. Privacy Armor - The Proposed Model to ensure privacy in unstructured data

We now propose a model that will measure privacy in the unstructured data in OSNs. The status updates, tweets and posts are all unstructured in nature. To calculate the percentage of privacy leaks in such data sets we have proposed Privacy Armor- a model that will warn the users if they are intentionally or unintentionally sharing some sensitive content online.

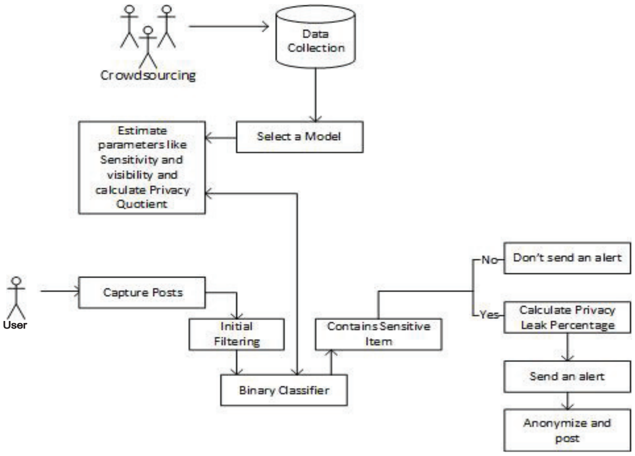

Fig. 10: Module 1 : Proposed model of Privacy Armor.

A. Crowdsourcing and Data Collection

Initially using the crowdsourcing method we will gather the information about the items being shared on the user's profile. If they have willingly shared the data we will take it as 1 otherwise we will consider it as private entry and mark it as 0. The resultant will be a N X n dichotomous response matrix. Where N will be the number of users and n will be the number of profile items.

B. Selecting a Model and calculating the Privacy Quotient

The advantage of naive approach is that it is a fairly simple approach and one can follow it easily as it has more practical implications. The disadvantage is that the sensitivity values obtained are significantly biased by the user population. If the users by nature are introverts and do not like to share a lot of information then the estimated sensitivity will be high, on the other hand if the users of the group are extrovert then the sensitivity will be low [9]. The real world data is too messy to fit the data effectively hence Liu et al have calculated the privacy scores by choosing the Item Response Theory model. To measure some trait of a person, there has to be a measurement scale [16]. An assumption that is made here is that every individual has some attitude, i.e either the individual is an extrovert or an introvert. So users will have some attitude score that will place them somewhere on the attitude scale. This is denoted by θ. The probability that the j^{th} individual having an attitude of θ will share their sensitive content i is denoted by P(θ_{ij}).
If we plot a graph with θ on the x axis and P(θ_{ij}) on the y axis. It will a smooth S shaped curve, that is called as the Item Characteristic Curve. This curve has two properties, one is the sensitivity that is denoted by β and the other is the discrimination constant denoted by α. Privacy quotient can be calculated as stated in equation 4. Using the item response theory model the V(i,j) is calculated as

$$PR(\theta_{ij} = 1) = \frac{1}{1 + e^{\alpha_i(\theta_j - \beta_i)}} \tag{5}$$

where β_i is the sensitivity of the ith profile item, α_i is the discrimination constant of the ith profile item, θ_j is the ability of the jth user. The calculated values of the parameters like the sensitivity, visibility are highly intuitive. This computation can also be parallelized using the Map Reduce technique, which can thereby increase the performance of the algorithm as well. After calculating the sensitivity and visibility. We can compute the privacy quotient of each of the users using the equation 4.

Sharing of messages in the form of status updates, tweets etc is very common now-a-days. Such information may contain some sensitive information about the user [17]. Some users intentionally share it whereas some users are not aware of the privacy risks that follows. Privacy armor will warn such users and send them an alert showing the privacy leakage percentage.
In Figure 10 the message posted by the user is first analyzed by the privacy armor to check for any sensitive information such as their phone numbers, email, address , location etc. By making use of a binary classifier the posts are either classified as sensitive or not sensitive .
Also a percentage of privacy leakage is shown to the users. Privacy leakage is calculated as

$$\vartheta = \frac{\sigma}{\beta} * 100 \tag{6}$$

where σ is $\sum_k \sigma_i$ here k are number of sensitive items in the post and σ_i is the sensitivity of the i^{th} profile item.
β is the total sensitivity of all the n items.
ϑ is the percentage of privacy leakage.
For eg: If the user shares "Having lunch with Congress supporters".
Here the user is sharing the political view. A certain amount of privacy leak is associated with this post which can be calculated using equation 6. As calculated by the naive approach the sensitivity of political views is .6833 and the overall sensitivity is 4.183.
ϑ = (.6833/4.183)*100; ϑ = 16.33 %; Privacy leakage associated with this post is 16.33 %.

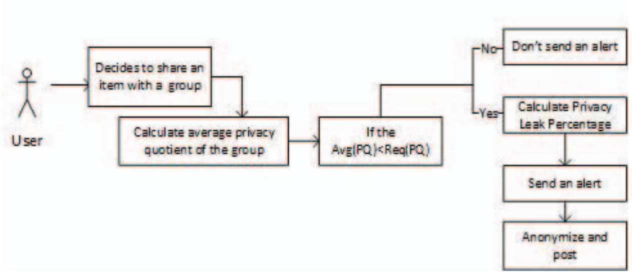
User
Decides to share an item with a group
Calculate average privacy quotient of the group
If the Avg(PQ)<Req(PQ)
No
Don't send an alert
Yes
Calculate Privacy Leak Percentage
Send an alert
Anonymize and post

Fig. 11: Module 2 : Proposed model of Privacy Armor.

People with low privacy quotient, are likely to share the information without considering the privacy risk. Sharing information with such users is often risky and will have a high percentage of privacy leak. Figure 11 explains that before sharing an information to the group of people, the privacy armor will calculate the average privacy quotient of the users. We can calculate the average privacy quotient by the formula

$$\frac{1}{N}(\sum_j PQ(j)) \tag{7}$$

where j varies from $1 \leq$ j $\leq$ N
PQ(j) is the privacy quotient of the user j.
Crowdsourcing will provide the privacy quotient for N number of users. We can calculate the required privacy quotient using the mean value theorem.

$$Req(PQ) = \frac{1}{b-a} \int \sum_i \beta_i * V(i,j) \tag{8}$$

where the range of items i.e i varies from $1 \leq$ i $\leq$ n; a is the lowest Privacy Quotient obtained; b is the highest Privacy Quotient obtained; θ is the ability of the user. If Avg(PQ) $<$ Req(PQ) then the privacy armor will send an alert to the user showing the privacy leak percentage which can be calculated using the formula

$$\vartheta = \frac{Req(PQ) - Avg(PQ)}{Req(PQ)} * 100 \tag{9}$$

Knowing the privacy risks involved the user can chose not to post the message at all or can anonymize the message before posting it online to reduce the privacy risks.

VI. Conclusion and Future Work

We have covered three aspects in this paper. First we have carried out a survey that gave a clear picture of privacy in today's world. Next we have calculated the privacy quotient i.e a metric to measure the privacy of users by the naive approach using the data collected from the survey. At last we have proposed- Privacy Armor : a model to ensure privacy in the unstructured data. In future we will be implementing privacy armor. We will extend our survey to various groups belonging to different nationalities and model their data and rank them according to the privacy quotient obtained.

Acknowledgment

We would like to thank KP Krishna Kumar our co-researcher for his help.

References

[1] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM, 2005, pp. 71–80.

[2] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography," in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 181–190.

[3] J. DeCew, "Privacy," in *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed., 2012.

[4] Y. Altshuler, Y. Elovici, N. Aharony, and A. Pentland, "Security and privacy in social networks." Springer, 2013.

[5] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch, "Exploiting social networking sites for spam," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 693–695.

[6] P. Gundecha and H. Liu, "Mining social media: A brief introduction."

[7] B. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Computing Surveys (CSUR)*, vol. 42, no. 4, p. 14, 2010.

[8] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *ACM Sigmod Record*, vol. 29, no. 2. ACM, 2000, pp. 439–450.

[9] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," in *Data Mining, 2009. ICDM'09. Ninth IEEE International Conference on*. IEEE, 2009, pp. 288–297.

[10] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proceedings of the 19th international conference on World wide web*. ACM, 2010, pp. 351–360.

[11] A. Braunstein, L. Granka, and J. Staddon, "Indirect content privacy surveys: measuring privacy without asking about it," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011, p. 15.

[12] S. Guo and K. Chen, "Mining privacy settings to find optimal privacy-utility tradeoffs for social network services," in *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*. IEEE, 2012, pp. 656–665.

[13] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," Ph.D. dissertation, University of California, Davis, 2009.

[14] J. Anderson, "Privacy engineering for social networks," 2013.

[15] H. R. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view." *UPSEC*, vol. 8, pp. 1–8, 2008.

[16] F. Drasgow and C. L. Hulin, "Item response theory," *Handbook of industrial and organizational psychology*, vol. 1, pp. 577–636, 1990.

[17] H. Mao, X. Shuai, and A. Kapadia, "Loose tweets: an analysis of privacy leaks on twitter," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM, 2011, pp. 1–12.