IJCTA, 10(01), 2017, pp. 57-65

Sustainability Study of Privacy Suites for user Upload Images in the Online Social Networks

Hemalatha D* and Karthikeyan R**

Abstract : Presently, the growth of Social media is explosive among the users. Increasingly developed social websites like Flickr, Facebook, Google+, LinkedIn etc permits the users to create, share and view the post. Privacy is an important factor required in Online Social Networks. The social users upload their photos to the social sites that intend to gain public interest for social purposes. The exposure of personal information leads to slipping process like identity stealing, morphing etc, which are against the privacy violations.Relied upon the personal characteristics of users, the privacy settings of each user should be defined. In this paper, a relational study about the privacy settings in Online Social Networks is examined. Initiated bythe importance of social networks among the social users and their behavior towards Online Social Networks, which is followed by the privacy techniques suggested by other researchers are explored. At last, an overview about the merits and demerits of privacy designs and schemes for the user-uploaded images are presented. Results of this study can be used to develop a new privacy system which will help users to control their sensitive information easily from different devices, including mobile devices and computers.

Keywords: Online Social Networks, Social media users, Privacy, Images, and Sensitive information.

1. INTRODUCTION

With the advancements in the Online Social Networking, the growth of social media users is inclined. It assists the social users to make new contacts, old friends and sharing the common opinions with the group of people across the world.It acts as communication links among the users [1].As the increased usage of websites, the participation of user's rate is also increased. By this advent, the user's share their images and personal information to their communities.Without having prior knowledge about the privacy settings, the images are uploaded and shared among the group of people [2]. By doing so, a variety of risks are faced by the social users like identity stealing, morphing etc. Despite these risks, many privacy mechanisms of content sharing sites are very weak.

A profile of a user comprised of details like company details, educational details, residential address, common interest etc. In order to be a part of the networks, tagging concept is emerged. An image of a user is tagged [3] with several people to gain interests. This concept becomes riskier in the complicated environment. And also, the users are unaware about the consequences of tagging concept of an image. Instead of imposing restrictions over such incidents or increasing security, sites like FB and Instagram are encouraging people to get into such things.

Online Social Networking is still in developing stage, but it elegantly supports some eminent applications [4].As this technology grows, we, eventually, expect some advanced functionalities. It is not inconceivable that social networking systems will eventually become de-facto portals for both personal

* ME Student, Department of Computer Science, Vel Tech Multi Tech Engineering College, Avadi, Chennai, Tamil Nadu

** Head of the Department, Department of Computer Science, Vel Tech Multi Tech Engineering College, Avadi, Chennai, Tamil Nadu

and commercial online interactions [5]. Adjacent users in a social network tend to trust each other more than random pairs of users in the network, which is shown in fig.1.Users browse neighboring regions of their social network because they are likely to find content that is of interest to them [6]. Understanding how content diffuses through these networks and becomes popular over time is not only of academic interest, but is increasingly important in commercial advertising, in political campaigning, and ultimately to society.

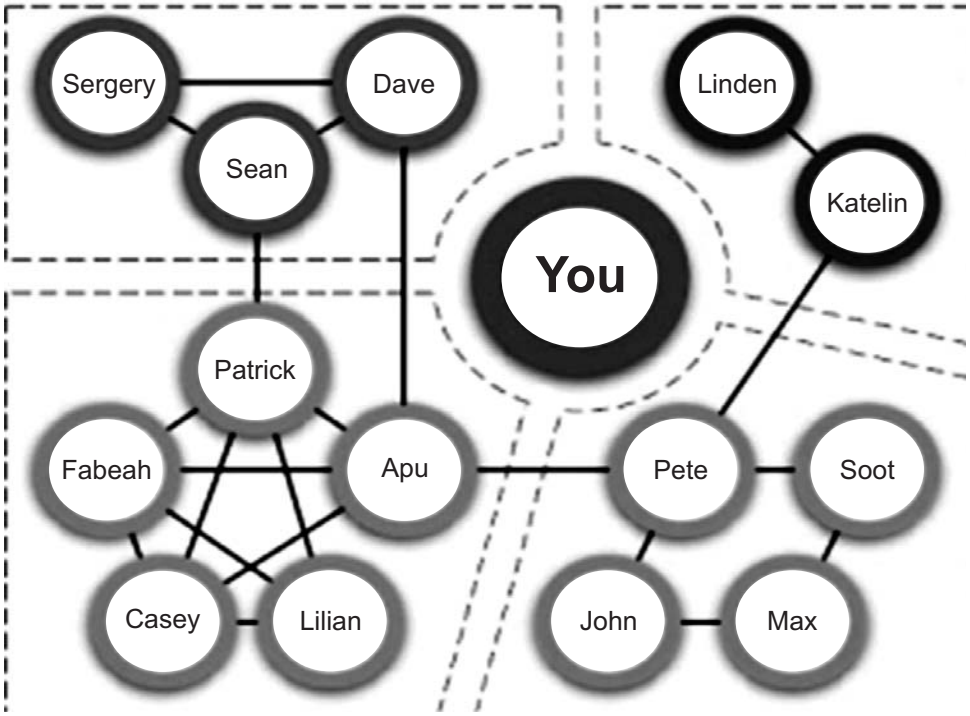

Figure 1: Community formation in Social networks [6]

The rest of the paper is organized as follows: Section II discusses about the existing schemes suggested by other researchers and Section III discusses with summary of the review findings made in our study.

2. RELATED WORK

In this section, we present a clear idea about the significance of the Online Social Networks, User's behavior in OSN and techniques involved.

2.1. Significance of Online Social Networks

In the midst of social media revolution, it is important that social media's is used as the communication medium. The primary benefit of the social media is the sharing and gaining of knowledge from wide range of people. This kind of growth develops the communication skills towards the online learners [7]. Social media have the potential to fundamentally change the character of our social lives, both on an interpersonal and a community level. Social networks grow from the personal interactions of human beings over time, as well as from the technological infrastructure that connects those humans. This means that growing a successful online social network requires social know- how as well as technical expertise's.

2.2. User Behaviour in Online Social Networks

The perception towards user behavior in Online Social Networks imposes a better interface design for improved content distributed systems. It is crucial to study about the behavior of users when they are associated to the social websites.Email is considered as important factor for associating with the networks [8].In current scenario, the social links are interlinked with each others. A single account of user is associated with different social websites.It assists the service providers to identify the attitudes of users. In

order to improve the user's experience, the behavior study is an important thing. In section 2.2, we explore the four orientations of defining the user behavior in social networks.The four orientations are as follows:

1. Finding the associations between users in OSN using Social Graph
2. Monitoring the events for predicting the network traffic
3. Development towards mobile platforms and applications
4. Security and privacy analysis based user's behavior

1. **Finding the associations between social users :** Social Graph is a mathematical model used for assessing the connections among the social users. It assists us to provide details about the characterization of users behaviors. The table 1 depicts the knowledge of five eminent social networks.

Table 1

Knowledge about five eminent social networks [9]

Social Sites	*No. of Users*
Facebook	billion
Twitter	500 million
Google +	450 million
Linkedin	200 million
Foursquare	30 million

Social graph is modeled into two ways, namely, undirected graph model and directed graph model. The four fundamental graphsare listed in Table 2. Relied upon these sorts of graph, the associations among the OSN users are studied. In addition to this, it imposes to research about the efficacy of social graphs. To resolve this issue, the authors in [10], proposed crawling techniques. The friendship graph and interaction graph belongs to the class of undirected graph and directed graph model includes latent graph and following graph. Friendship graph is defined that every user is considered as nodes and edge is represented as the connections between users. Therefore, friendship in OSNs can hardly be viewed the same as friendship in the real world [11]. Interaction graph is definedto find the communication between the users in real- world entities.

Then, the conventional measurement approaches are used for understanding the behaviors from browsing. Latent graph is built from the friendship graph and interaction graph. The overall system architecture is given in fig.2.

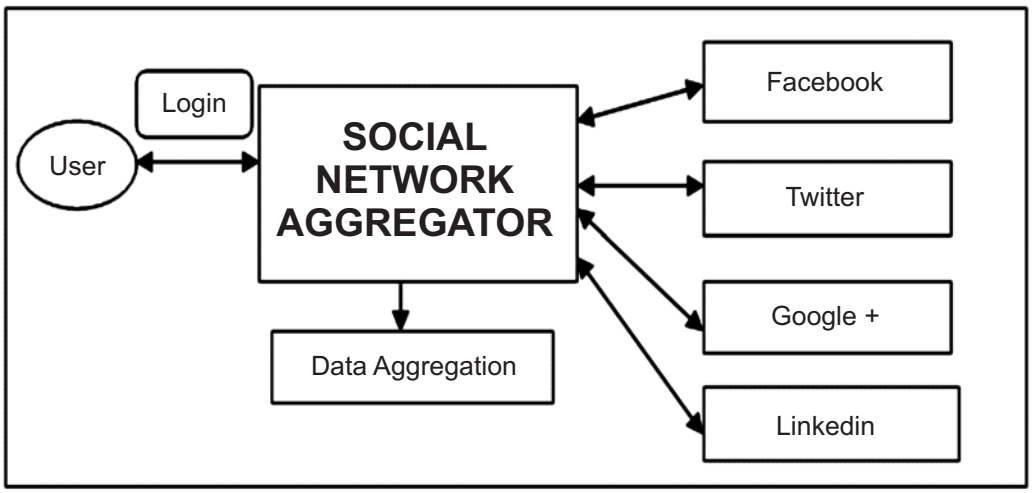

Figure 2: Profiling data through social network aggregator [11]

Table 2
List of different social graphs [12]

Sorts of Graph	*Edge*
Friendship Graph	Depicts the associations or connections between users
Interaction Graph	Depicts the posting behaviors
Latent graph	Depicts the browsing profile
Following graph	Depicts to obtain the messages

2. **Network Monitoring analysis :** A variant kind of social graphs intimates the associations between the users. In some cases, the user's activities can't be predicted due to restricted information about them. Furthermore, for ISPs, they have strong incentive to get better understanding of how the traffic pattern between end users and OSN sites will evolve, and take optimization actions according to the distribution and activities of OSN users. Instead of using crawling techniques, the network events also plays a vital role to predict the user's behavior.As in fig.2, Clickstream data is used for analyzing the behavior from Social Network Aggregator (SNA). Benevenuto et al studied about the user behavior from Clickstream data analysis. The author in [13] collected user data for a week of time that intended to study about the behavioral aspects of social users. Atlast, they concluded that the user's browsing data contain: (*i*) Frequency of data access in OSN (*ii*) Aggregate time spent on OSN (*iii*) Session monitoring in OSNs. From their study, they encountered 40 types of user's activities with their traffic bytes [14]. And they also discussed about the user's transition using markov chain model. Clickstream data contributes a lot in the user behavior study of OSNs. However, it can be incomplete, which restricts its usage and performance. First, click-stream data is limited by the collection duration, and the behavior of inactive users in the duration is not monitored. Moreover, the data is restricted by the monitoring locations.That is, only the behavior of users using certain monitored ISPs is captured.
3. **Mobile Application Developments :** Mobile platforms are also depicts the behavior of user. A variant number of web applications are emerged, so it is necessary to study about the mobile social networks. Some social websites also permits to access the data from mobile networks. In order to design mobile systems, the behavioral study of user is also important. By the advent of Bluetooth [15], the nearby users are recognized and the data is shared among them. This is referred as the social serendipity.For instance, internal collaboration in large companies can be facilitated by Serendipity for introducing people who are working on similar projects. It is emphasized that privacy issues are important and fundamental in serendipity, and privacy-protecting tools should be designed carefully.
4. **Anomalies Behavior :** Due to the interlinkage of different social websites, there is a chanceof exhibiting the threats. By the assistance of OSN service providers, user-user interaction is possible. The user may share their data like photos, articles, private messages etc. A Sybil attack is the most common threats found in the OSN. Some user's acts like original users and steal the account information. In [16], theypresented the types of attacks, such as untrusted third-party applications, cross-site profile cloning, social spamming, and phishing prevails in OSN. In order to protect the sensitive information, decentralized OSN architectureis required. Furthermore, the recipients of shared information should be controlled by the users themselves. Instead of sharing information based on the virtual links in OSNs, real-life relationship between users should also be taken into account. Finally, Sybil defense is still a hot topic and more solid work are expected to conduct in this area.

2.3. Image Sharing- Privacy Analysis

Privacy [17] is the most important parameter to be considered for web design. The association between privacy and user's network imposes a variety of privacy challenges. Nowadays, the images are being shared by most of the users. Sharing takes place both in group of people and in social circles. The sensitive information is mostly presented in the semantic enabled images. Relied upon the user's characteristic, the privacy setting of each user should be defined [18]. In this section, we explore the privacy analysis towards user uploading the images. The need for automatic privacy settings is inadequate. In order to resolve this, several authors studied about the privacy suites for the uploaded images.The web applications developed by the software programmers are inadequate to provide automatic privacy settings. Internet privacy is the subset of data privacy. The large scale computing systems involves large number of privacy settings.

Normally, the data privacy derives in two ways: a) Settings of self- privacy and b) Design of recommendation systems. The thought of issuing privacy to the users can be given for their uploaded data, profile information and associations and Meta data of the user uploaded images. Thus, the user uploaded images are classified into hierarchical structure, to define a priority set.Then, the concept of 'privacy by design' was introduced by [19].Their purpose was to improve the applications design by including the privacy concepts. Each application involves different level of privacy design with more authentic systems. The personal details of a user is shared by giving response to the received request was studied by [20].

In other words, privacy is characterized for self-representation of the online social networks i.e sharing their images and comment from others[21] [22]. In extending to privacy concern, [23] suggested a solution to its in three ways, namely, protective technologies, social awareness and legislative support. Protective technologies include authentication and access control mechanisms according to time. Then, creating knowledge about the privacy of the uploaded images is known as social awareness. Atlast, the shared images are enacted under the privacy law enforcement [24]. A general usage survey of facebook users was studied by [25].They depicted that users share their 92% ofprofile pictures, 95% of data of birth,and 20% shows their contact details. And the similar study was conducted by [26] with information about the hacked users.

Table 3
Taxonomy of social networks (Rosenblum, 2007)

Region	*Social websites*
Africa	Hi5, Facebook
America(North)	MySpace, Facebook, YouTube, Flicker, Netlog
America (Central and South	Orkut, Hi5, Facebook
Asia	Friendster, Orkut, Xianonei, Xing, Hi5, YouTube, Mixi
Europe	Badoo, Bedo, Hi5, Facebook, Xing, Skyrock, Ployaheod, Odnoklassniki.ru.V Kontakte
Middle East	Facebook
Pacific island	Bedo

The usage of internet services was mostly adopted by the youngsters. In reality, most of the young users are unaware about the privacy risks of sharing the images.Irrespective of the age, information sharing in the online environment causes dangerous to the social users [27].The confidence of the users is increased by the level of privacy settings. It should also be simple and easy to be used[28] [29].The major risks faced by the users, identity theft i.e stealing the user's personal information like images, contact address etc).The different ways of stealing the user's information was analyzed by the[30][31][32].

Table 4
Analysis of real identities (Gross and Acquisti, 2005)

Category	*% of social users*
Real name	90%
Partial name	4%
Fake name	6%

Some recent works investigated theself- configuring of the privacy settings. The privacy policies are preferred for the authorized users were studied by [33].The communication was enabled among the authorized group of users. A machine learning models were used to obtain the data accord to its context was studied by [34].This research study was further extended by forming clusters from partitioned users by [35]. Privilege based privacy settings was initiated by *Ravindran et al*, that predict user's privacy based on preferences. It was extended by [36], which assigns label to the selected group of users. His work enables to form privacy labels for unauthorized friends. The tagging concepts were improved by using access-control policies. The uploaded images contain keywords and labels for representing the images. A vast amount of study was conducted in Image Content Analysis [37, 38, 39, 40, 41, and 42].

Table 5
Top shared media of websites

Websites	*Shared media*
YouTube	Videos
Flicker	Images
Digg	Bookmarks
Metacafe	Videos

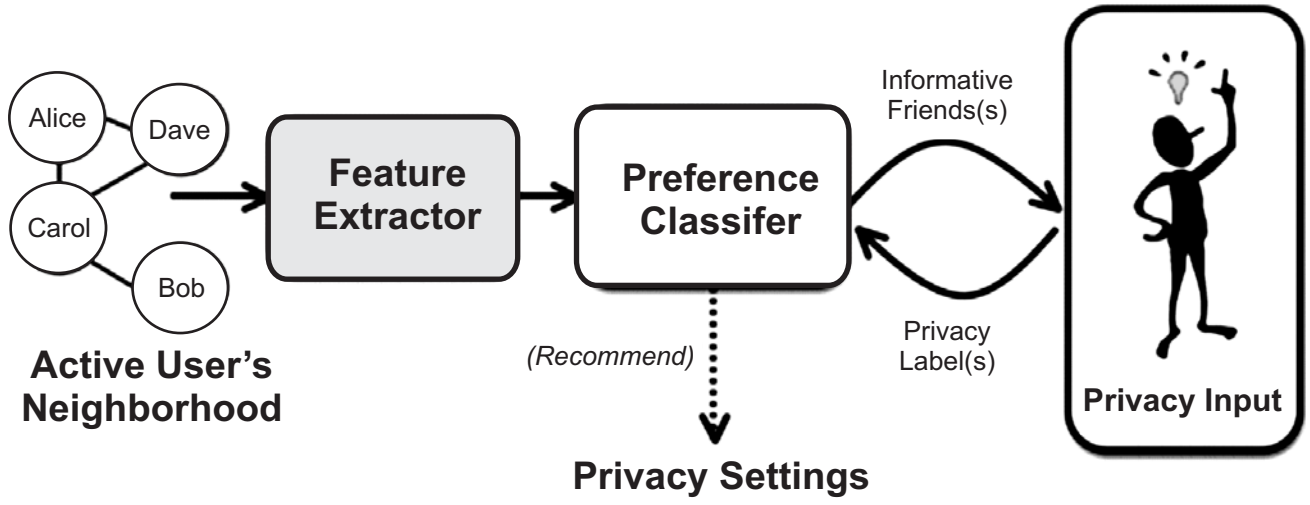

Figure 2: Preferences based privacy settings [46]

A text-based image retrieval system was examined by [43]. They designed discriminative model that stores and retrieves the image based on the ranking system. The Latent Dirichlet Allocation (LDA) was proposed to align and arrange the image in an unsupervised fashion. Based on the topics, the images are represented. Then the semantic model was encouraged by [44].They have also presented the results of an extensive experimental evaluation, under various previously proposed experimental protocols, which demonstrated superior performance with respect to a sizable number of state-of-the-art methods, for both semantic labeling and retrieval.In [45],studied a new image feature called the color correlogram and use

it for image indexing and comparison. This feature distils the spatial correlation of colors, and is both effective and inexpensive for content-based image retrieval. The correlogram robustly tolerates large changes in appearance and shape caused by changes in viewing positions, camera zooms, etc.

Table 6

Example friend data with extracted features, including community-based features

	R_0	R_1	R_2	R_{20}	R_{21}	R_{22}	R_{23}	*Privacy settings (Images)*
Alice	0	1	0	0	0	0	0	Allow
Bob	0	0	1	1	0	0	0	Refuse
Carol	1	0	0	0	0	0	0	Allow

Table 7

Relational study of merits and demerits of privacy analysis

Techniques for privacy	*Merits*	*Demerits*
Design oriented privacy suites	Design policies are transparent in nature.	Difficult to understand by normal users
Study on social circles	Flexible for finding association among the users.	Unable to process for higher number of users.
Compression schemes for images	Simple to use	Overhead in computational process
Privacy protector tools	Transparent process	Highly difficult to understand
Tagging concepts	Transparent process	Inefficient handling of large set of users.
Linked data to the tags and keywords	Link with multiple sites	Limited set of connecting the linked data
Image classification and search for privacy schemes	Performs direct search for protected data	High complexity

3. SUMMARY

Nowadays, a vast amount of private data is being shared in the social networking sites. The private data includes sensitive information and images, in which images are being mostly shared by most of the social users. In order to eliminate the malicious events, a well-reputed privacy schemes are required. But, in most of the cases, applying privacy schemes on the data is a cumbersome task. In this paper, relational study of privacy settings in Online Social Networks is examined. In specific to, we studied about the privacy settings for the user-uploaded images. From this study, we summarized that the privacy oriented importance given to the user-uploaded images are not yet flourished. It is wisely recommended that a privacy design for user-uploaded images need to be developed.The privacy systems of Online Social Networks should accommodate their users with different levels of privacy settings for their images irrespective of location and time.

4. REFERENCES

1. Takeshi Sakaki, Makoto Okazaki, and Yutaka Matsuo; “Earthquake shakes Twitter users: real-time event detection by social sensors”. In Proceedings of the 19th international conference on World wide web (WWW ‘10). ACM, New York, NY, USA, 851-860.
2. Lampos, Vasileios; Cristianini, Nello; “Tracking the fl u pandemic by monitoring the social web,” Cognitive Information Processing (CIP), 2010, pp.411-416.

3. White, T.; Chu, W.; Salehi-Abari, A.; "Media Monitoring Using Social Networks," Social Computing (SocialCom), 2010 IEEE conferences on Social networking sites, 2010, pp.661-668.
4. Rodrigues, E.M.; Milic-Frayling, N.; Fortuna, B.; "Social Tagging Behavior in Community-Driven Question Answering," Web Intelligence and Intelligent Agent Technology, 2008, pp.112-119.
5. Li, G.; Li, H.; Ming, Z.; Hong, R.; Tang, S.; Chua, T.; "Question Answering over Community Contributed Web Video," Multimedia, IEEE, 2010, pp.1-1.
6. Jian Jiao; Jun Yan; Haibei Zhao; Weiguo Fan; "ExpertRank: An Expert User Ranking Algorithm in Online Communities," New Trends in Information and Service Science, 2009, pp.674-679.
7. Walenz, B.; Gandhi, R.; Mahoney, W.; Quiming Zhu; "Exploring Social Contexts along the Time Dimension: Temporal Analysis of Named Entities," IEEE conference on Social Computing (SocialCom), 2010, pp.508-512.
8. Nielsen Online Report, " Social networks & blogs now 4th most popular online activity", 2009.
9. C. Wilson et al., "User Interactions in Social Networks and Their Implications," Proc. EuroSys, 2009.
10. J. Jiang et al., "Understanding Latent Interactions in Online Social Networks," Proc. IMC, 2010.
11. H. Kwak et al., "What Is Twitter, a Social Network or a News Media?," Proc. WWW, 2010.
12. M. Gjoka et al., "Practical Recommendations on Crawling Online Social Networks," IEEE Trans. Commun. Special Issue on Measurement of Internet Topologies, vol. 29, no. 9, Oct. 2011.
13. B. Ribeiro and D. Towsley, "Estimating and Sampling Graphs with Multidimensional Random Walks," Proc. IMC, 2010.
14. F. Benevenuto et al., "Characterizing User Behavior in Online Social Networks," Proc. IMC, 2009.
15. F. Schneider et al., "Understanding Online Social Network Usage from a Network Perspective," Proc. IMC, 2009.
16. M. Wittie et al., "Exploiting Locality of Interest in Online Social Networks," Proc. CoNext, 2010. [9] C. W. Dunn et al., "Navigation Characteristics of Online Social Networks and Search Engines Users," Proc. WOSN, 2012.
17. L. Backstrom, E. Sun, and C. Marlow, "Find Me If You Can: Improving Geographical Prediction with Social and Spatial Proximity," Proc. WWW, 2010.
18. E. Cho, S. Myers, and J. Leskovec, "Friendship and Mobility: User Movement in Location-Based Social Networks," Proc. KDD, 2011.
19. Cavoukian, A, " Privacy by design…Take the Challenge. Information and Privacy Commissioner of Ontario", Canada, 2009, pp. 3-6.
20. Bae, S. H. & Kim, J., "Development of Personal Information Protection Model using a Mobile Agent, "Journal of Information Processing Systems, vol.6, no.2, 185-194,2010.
21. Weichao Wang; Cheng Cui, "Achieving configural location privacy in location based routing for MANET," Military Communications Conference, 2008.pp. 16-19.
22. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M. & Rao, J, "Understanding and capturing people's privacy policies in a mobile social networking application, "Personal and Ubiquitous Computing,13, pp. 401-412.
23. Passant, A., Kärger, P., Hausenblas, M., Olmedilla, D., Polleres, A., Decker, S. & Telefonica, R. "Enabling trust and privacy on the social web".W3C workshop on the future of social etworking, 2009.pp. 15-16.
24. Campisi, P.; Maiorana, E.; Neri, A., "Privacy protection in social media networks a dream that can come true?,", 16th International Conference on Digital Signal Processing, vol., no., pp.1,5, 2009
25. Rosenblum, D., "What Anyone Can Know: The Privacy Risks of Social Networking Sites," Security & Privacy, IEEE, vol.5, no.3, pp.40,49, May-June 2007.
26. Gross, R. & Acquisti, A. "Information revelation and privacy in online social networks,"Proceedings of the 2005 ACM workshop on Privacy in the electronic society (WPES '05). ACM, New York, NY, USA, 2005, pp.71-80.
27. Zukowski, T. & Brown, I. "Examining the influence of demographic factors on internet users' information privacy concerns", Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries(SAICSIT '07). ACM, New York, NY, USA, 2007, pp. 197-204.
28. Samavi, R. & Consens, M. P. "Towards Smart Privacy on the Personal Web,"Proc. of the First Symp. on the Personal Web, Co-located with CASCO, 2010, Markham, Ontario, Canada.

29. Casarosa, F, “Child Privacy Protection Online: How to Improve It through Code and Self-Regulatory Tools”, Available at SSRN: http://ssrn.com/abstract=1561570, 2010.
30. Novak, E. & Li, Q, “A Survey of Security and Privacy in Online Social Networks”, College of William and Mary Computer Science Technical Report, WM-CS-2012-2
31. LEE, R., NIA, R., YE, S., HSU, J., LEVITT, K.,ROWE, J. & WU, S, “Design and Implementation of FAITH, An Experimental System to Intercept and Manipulate Online Social Informatics”, Advances in Social Networks Analysis and Mining (ASONAM), pp.195- 202, 25-27 July 2011.
32. Gharibi, W. & Shaabi, M, “Cyber threats in social networking websites”, Arxiv preprint arXiv: 1202.2420, 2012.
33. J. Bonneau, J. Anderson, and L. Church. Privacy suites: shared privacy for social networks. In Symposium on Usable Privacy and Security, 2009.
34. J. Bonneau, J. Anderson, and G. Danezis, “Prying data out of a social network”, In ASONAM: International Conference on Advances in Social Network Analysis and Mining, pages 249– 254, 2009.
35. A. K. Fabeah Adu-Oppong, Casey Gardiner and P. Tsang, “Social circles: Tackling privacy in social networks”, In Symposium On Usable Privacy and Security, 2008.
36. A. Mazzia, K. LeFevre, and A. E., “The PViz comprehension tool for social network privacy settings,” in Proc. Symp. Usable Privacy Security, 2012
37. M. Rabbath, P. Sandhaus, and S. Boll, “Analysing facebook features to support event detection for photo-based facebook applications,” inProc. 2nd ACM Int. Conf. Multimedia Retrieval, 2012. pp. 11:1–11:8.
38. R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, “Capturing social networking privacy preferences,” inProc. Symp. Usable Pri-vacy Security, 2009.
39. A. Singhal, “Modern information retrieval: A brief overview,” IEEE Data Eng. Bullet., Special Issue on Text Databases, vol. 24, no. 4, pp. 35-43, Dec. 2001.
40. A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, “A3p: Adaptive policy prediction for shared images over popular con-tent sharing sites,” inProc. 22nd ACM Conf. Hypertext Hypermedia, 2011, pp.261–270.
41. K. Strater and H. Lipford, “Strategies and struggles with privacy in an online social networking community,” inProc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.
42. X. Su and T. M. Khoshgoftaar, “A survey of collaborative filtering techniques,”Adv. Artif. Intell., vol. 2009, p. 4, 2009.
43. C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, “Providing access control to online photo albums based on tags and linked data,” inProc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.
44. J. Yu, D. Joshi, and J. Luo, “Connecting people in photo-sharing sites by photo content and user annotations,” inProc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1464–1467.
45. S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, “Privacy-aware image classification and search,” in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 35–44.
46. S. Zerr, J. H. Stefan Siersdorfer, and E. Demidova, Picalert! data set, 2012.
47. N. Zheng, Q. Li, S. Liao, and L. Zhang, “Which photo groups should I choose? A comparative study of recommendation algo-rithms in flickr”, J. Inform. Sci., vol. 36, pp. 733–750, Dec. 2010.
48. J. Zhuang and S. C. H. Hoi, “Non-parametric kernel ranking approach for social image retrieval,” inProc. ACM Int. Conf. Image Video Retrieval, 2010, pp. 26–33.