Overview of Privacy in Social Networking Sites (SNS)

Pallavi I. Powale
Research Scholar
Vishwakarma Institute of Technology
Pune, India

Ganesh D. Bhutkar
Assistant Professor
Vishwakarma Institute of Technology
Pune, India

ABSTRACT

Social Networking Sites (SNS) have become an integral part of communication and life style of people in today's world. Because of the wide range of services offered by SNSs mostly for free of cost, these sites are attracting the attention of all possible Internet users. Most importantly, users from all age groups have become members of SNSs. Since many of the users are not aware of the data thefts associated with information sharing, they freely share their personal information with SNSs. Therefore, SNSs may be used for investigating users' character and social habits by familiar or even unknown persons and agencies. Such commercial and social scenario, has led to number of privacy and security threats. Though, all major issues in SNSs need to be addressed, by SNS providers, privacy of SNS users is the most crucial. And therefore, focus of this paper is on 'privacy in SNSs'. Different ways of Personally Identifiable Information (PII) leakages from SNSs, information revelation to third-party domains without user consent and privacy related threats associated with such information sharing are discussed in this paper. This comprehensive overview on privacy in SNSs will definitely help in raising user awareness about sharing data and managing their privacy with SNSs. It will also help SNS providers to rethink about their privacy policies.

Keywords

Social Networking Sites, SNS, privacy, Personally Identifiable Information, PII, PII leakage, privacy related threats

1. INTRODUCTION

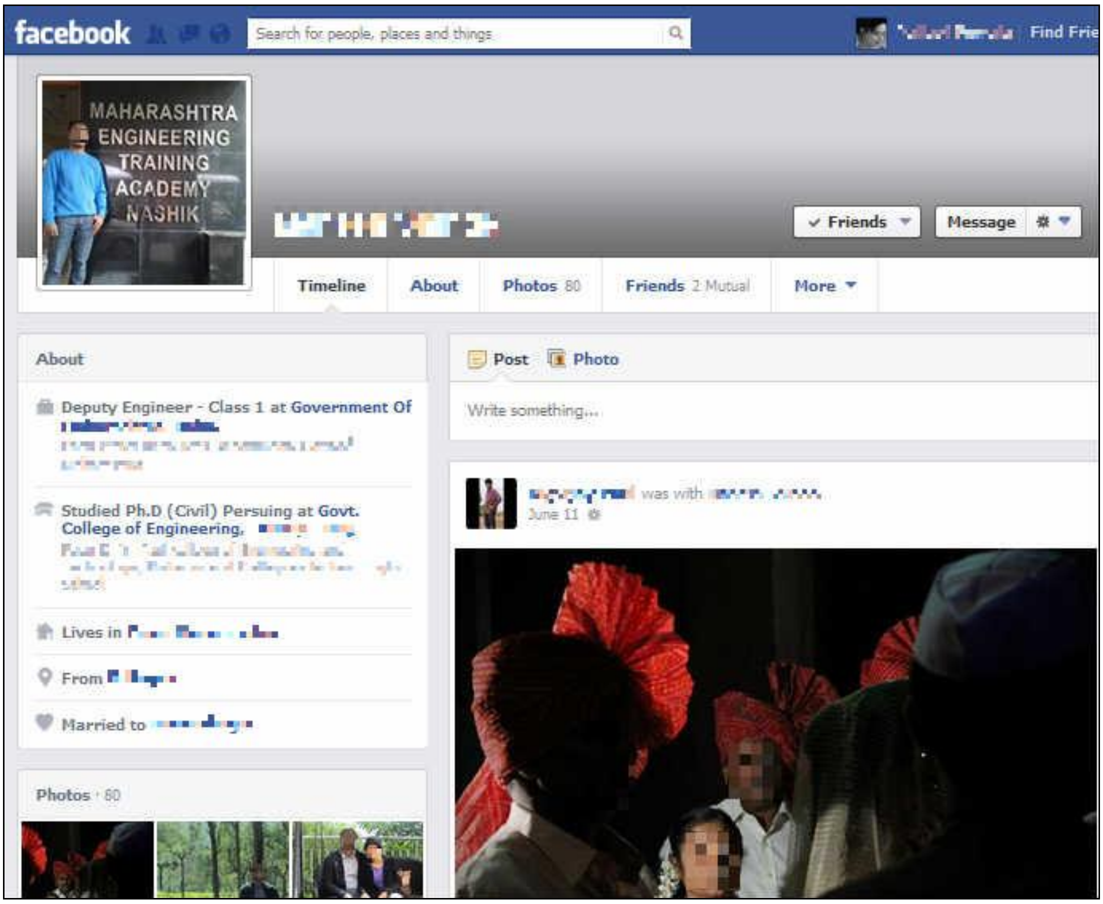
Human being is a social creature and likes to be in contact with others. Social Networking Sites (SNSs) provide a mean for connecting people all around the world. SNSs are becoming more popular because these sites allow users to connect with old buddies, to meet new people, to send messages, to upload and share photographs as well as videos. Most of the times, these services are provided free of cost.

According to Ellison and Boyd [7], "A social networking site is a networked communication platform in which participants 1) have uniquely identifiable profiles that consist of user-supplied content, content provided by other users, and/or system-provided data; 2) can publicly articulate connections that can be viewed and traversed by others; and 3) can consume, produce, and/or interact with streams of user generated content provided by their connections on the site." SixDegrees.com was the first major SNS, which was launched in 1997 [30]. Afterwards many SNSs were launched for friendship and dating but not limited to the same, the area of focus varies depending on users' intention of socialization (e.g. LinkedIn and DeviantArt). Table 1 shows statistics about top 10 popular SNSs, which include the year of launching, the focus, number of monthly active users [26, 33] and minimum age limit for registration.

Users often without knowing the audience accessing their private information, share the personal indentifying information about themselves. Graham Cluley (Senior Technology Consultant at UK tech security firm- Sophos) says: *"Social networks are great fun, and can be advantageous but people really need to understand that it is complicated world, and you need to step wisely"* [28]. SNSs with more than billion users have dramatically raised concerns on privacy leakage. This article presents comprehensive overview about privacy in SNSs.

Table 1: Statistics about top 10 popular SNSs [26, 33]

Social Networking Site	Year of Launching	Focus	Number of Monthly Active Users	Min. Age for Registration (Yrs)
Facebook	2004	Friendship & Dating	1,000,000,000	13
Twitter	2006	Friendship & Dating	250,000,000	Open
LinkedIn	2003	Business Contacts	110,000,000	18
Pinterest	2011	Friendship & Dating	85,500,000	Open
MySpace	2003	Friendship & Dating	70,500,000	13
Google+	2011	Friendship & Dating	65,000,000	13
DeviantArt	2000	Art community	25,500,000	13
LiveJournal	1999	Blogging	20,500,000	Open
Tagged	2004	Friendship & Dating	19,500,000	Open
Orkut	2004	Friendship & Dating	17,500,000	18



About

Deputy Engineer - Class 1 at Government Of [redacted]

Studied Ph.D (Civil) Persuing at Govt. College of Engineering, [redacted]

Lives in [redacted]

From [redacted]

Married to [redacted]

[redacted] was with [redacted]
June 11

Figure 1: Facebook user profile page

1.1 Issues Related with SNSs

The previous section highlights the penetration of SNSs in today's world. In this section, major issues related with SNSs are depicted, as listed in Table 2.

Table 2: Issues related with SNSs

Privacy	**Authorization vs. Network Growth**
Potential for Misuse	**Risk for Child Safety**
Redress	**Social Network Fatigue**

1.1.1 Privacy

Users often disclose too much personal information on SNSs. The primary element of users' information like sex, nationality, friend lists, photos etc. constitute user profile on SNSs. Figure 1 shows the Facebook user's profile page; service provider of the Facebook has full access to all users' data. Users of SNSs are not aware of the fact that this data can be shared with strangers. This could lead to problems like identity thefts, sybil attacks, content based image retrieval, cyber bullies, privacy invasion etc. on large SNSs.

1.1.2 Authorization vs. Social Network Growth

As discussed by Bhutkar [1] and Boyd [2], the users can be categorized as: Friends (user's real-life friends), Friendster (friends of friends), Fakesters (users with fake personas) and Fraudsters (users with fake personas and involved in some fraudulent or sexual activity). Different types of SNSs users and their roles raise the necessity of authorization on SNSs. It is observed that, in order to deal with identity frauds, it is essential for the user account to reflect true identity of the user [16]. It is noticed that strictly authenticated SNSs will have authenticated friends or friendsters but will grow very slowly. Hence most of the SNSs favor the network growth by giving less preference to authentication.

1.1.3 Potential for Misuse

SNSs users are further categorized into two groups: creators and curators. Creators group is made up of those who have shared photos they have taken themselves and those who have shared videos they have created themselves. The curators group is made up of those who have taken photos they found online and reposted them on a site that is used for sharing images with others and those who have taken videos they found online and reposted them on a video-sharing site that is used for sharing videos with others. Overall, 56% of internet users do at least one of these creating or curating activities and 32% of internet users do both creating and curating activities. Table 3 shows percentage of creators and curators [27], from which one can see that even if data is shared with friends that data can be reposted by them on other sites, which can be misused further.

Table 3: Percentage of creators and curators

	Creators (Image) %	Curators (Images) %	Creators (Video) %	Curators (Video) %
Internet Users (n=799)	45	35	18	25
Men (n=393)	43	31	17	23
Women (n=406)	47	40	18	27
Age (Years)				
18-29 (n=140)	67	52	33	44
30-49 (n=224)	50	38	18	21
50-64 (n=229)	28	26	8	18
65+ (n=182)	26	17	8	11
Education Level				
High School or less(n=238)	38	33	13	20
Some College (n=230)	48	44	23	32
College+ (n=329)	50	30	17	23

1.1.4 Risk for Child Safety

A 95% of all teens in the age group of 12-17 years, are now online and 80% of those online teens are users of social media sites. Table 4 shows statistics about SNSs usage by teens [31].

Table 4: SNSs usage by teens

	Internet Users	SNS Users	SNS Users %
Teen Internet Users	770	616	80
Boys	375	292	78
Girls	395	328	83
Age of Teen Internet Users			
12-13 Years	210	134	64
14-17 Years	560	448	88

Teens have a tendency to share information with their friends and connections. A profile on SNSs is like an opened window into their lives. Even though many SNSs use their Terms of Service (ToS) to restrict children under the age of 13 from creating account, children gain access to these services by lying. It can be proved by the results of the survey made by Boyd et al. [5]. The results are shown in Table 5, which shows that kids below 13 years, are also joining Facebook obviously through lying. From this table, it is also clear that, in many cases parents knowingly allow & assist their child getting involved in SNSs by circumventing age restrictions through lying. Parents are generally not aware about risks associated with child safety on SNSs. A survey on PewInternet [31] on Teens' experience of online cruelty shows that, 88% of social media-using teens have witnessed other people be mean or cruel on SNSs. Some 15% of teen social media users have experienced such harassment themselves in the past 12 months. From this, parents need to understand how important is to protect children's privacy and reputation diligently [14] & should restrict their child by violating ToS of SNSs.

Table 5: Mean age when child joined Facebook, and parental awareness, assistance of account creation among the parents who reported child with Facebook account (N=106) [5]

	Child's Current Age (Yrs)				
	10	11	12	13	14
Mean Age When Child Joined Facebook (Yrs)	8.9	10.0	11.1	12.1	11.7
Parent was Aware when Child Signed-up (%)	95	88	82	82	88
Parent Helped to Create the Account (%)	78	68	76	60	47

1.1.5 Redress

To be effective, SNSs should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress). But nowadays, SNSs policy does not include any type of compensation for these suffered users. Much like the other privacy principles, redress requires that customers be aware of ways in which they may be harmed. In the case of security breaches, there is no policy for negative notification of customers [24]. Therefore, user may feel insecure while using the SNSs and in order to make them trust on sites, some compensation related policy must be included.

1.1.6 Social Network Fatigue

Nowadays, people cannot be friends unless they are on same SNSs. In order to be a part of multiple SNSs, even though user's information is same, he has to create profiles on each of the SNSs. Such restrictions are fatigue for user and should be removed. Interoperable SNSs should be available in order to make social relationships without inviting friend to join your network, e.g. user should be able to send scrap or post from Facebook to Orkut etc. SNS providers should work on this.

2. PRIVACY IN SNS

Graham Cluley (Senior Technology Consultant at UK tech security firm- Sophos) says: *"The sites most likely to suffer from issues that are the most popular ones"* [28]. According to previous studies [3, 8] the protection of the users' privacy is the one of the major objectives for SNSs. Privacy is the ability of an individual or a group to seclude oneself or information about one self and thereby reveal details selectively [29]. The boundaries and contents of what is considered private differ among cultures and individuals, but share basic common themes.

Hofstede developed a number of cultural value indices to measure cultural differences between societies. According to him, India is a collectivist society with lower InDiVidualism index (IDV) (refers to an individual's independence from organizations or collectivity) compared to the US, which is an individualist society with higher IDV. Hofstede has shown that individuals in collectivist societies have more trust and faith in other people than individuals in individualist societies [25].

Kumaraguru and Cranor [12] conducted an exploratory study to gain an initial understanding of attitudes about privacy among the Indian high tech workforce. Results of this survey demonstrate an overall lack of awareness about privacy issues in India than that has been found in results of similar studies conducted in the United States.

2.1 Flow of Information

Figure 2 shows the flow of information among SNSs, external applications, third-party servers and traditional websites. One can see that a single user can be member of multiple websites including SNSs as seen in Figure 2. At the same time, some third-party servers are active on many of these sites. A third-party server can collect user information from multiple sites and can link user profiles over multiple SNSs or websites in order to track user's behavior. The figure also shows the information flow between external applications and SNSs. This information sharing is often hidden from the user. It is difficult for the user, to know and control the various entities, which can gain access to one's information and limit oneself in such a way that one does not get the full advantage of various features of SNSs.

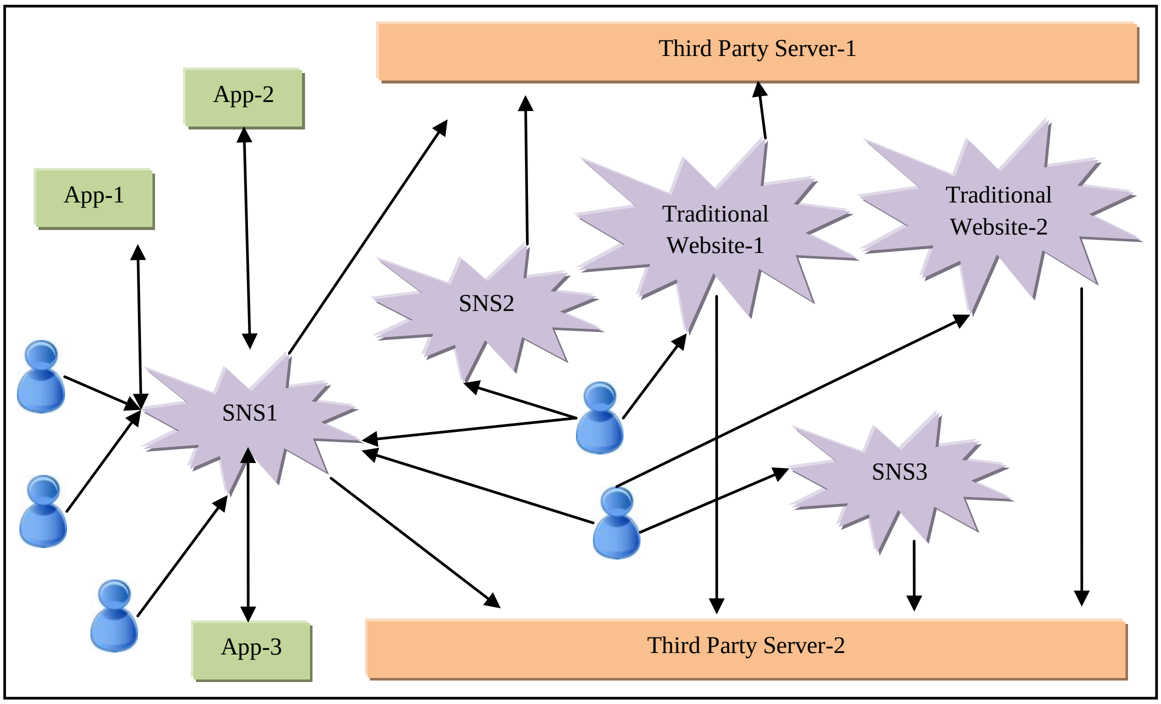


Figure 2: Flow of information

2.2 Personally Identifiable Information (PII) Availability on SNSs

According to Krishnamurthy and Wills [11], Personally Identifiable Information (PII) can be defined as, the information which can be used to distinguish or to trace an individual's identity either alone or when combined with other information which is linkable to a specific individual. Table 6 shows, the results of analysis made by Krishnamurthy and Wills [11] by considering twelve SNSs - Bebo, Digg, Facebook, Friendster, Hi5, Imeem, LiveJournal, MySpace, Orkut, Twitter, Xanga and LinkedIn. It shows the count of SNSs, exhibiting the given degree of availability for each attribute of PII. In table 6, the rows are sorted in decreasing order of availability and thus, leakage of PII attributes. One can see that personal photo, location, gendor and name are widely available thus more chances of their leakage, while email address, zip code, phone number and street address are rarely available, hence less chances of their leakage. Boyd and Hargittai [4] observed that, the users of SNSs who fall under less skilled users and cannot set up privacy settings to their accounts, are most likely to be exposed if default settings are open. Hence the values in the first two columns raise more privacy concerns.

Table 6: Personally Identifiable Information (PII) availability count in 12 SNSs (Bebo, Digg, Facebook, Friendster, Hi5, Imeem, LiveJournal, MySpace, Orkut, Twitter, Xanga and LinkedIn) [11]

Attribute of PII	Level of PII Availability			
	Always Available	Available by Default	Unavailabl e by	Always Unavailable
Personal photo	9	2	1	0
Location	5	7	0	0
Name	5	6	1	0
Gender	4	6	0	2
Activities	2	8	0	2
Age/ Birth year	2	5	4	1
Friends	1	10	1	0
Photo set	0	9	0	3
Schools	0	8	1	3
Employer	0	6	1	5
Birthday	0	4	7	1
Email address	0	0	12	0
Zip code	0	0	10	2
Phone number	0	0	6	6
Street address	0	0	4	8

Table 7: Top Third-party domains used by SNS sessions [10] (1- Bebo, 2- Digg, 3- Facebook, 4-Friendster, 5- Hi5, 6- Imeem, 7- LiveJournal, 8- MySpace, 9- Orkut, 10- Twitter, 11- Xanga)

Third-party Domains	Social Networking Sites										
	1	2	3	4	5	6	7	8	9	10	11
doubleclick.net	Y	Y	N	Y	Y	Y	Y	Y	N	N	Y
2mdn.net	Y	Y	N	Y	Y	Y	N	Y	N	N	Y
advertising.com	Y	N	Y	Y	Y	Y	N	Y	N	N	N
atdmt.com	N	Y	Y	Y	N	Y	Y	Y	N	N	N
quantserve.com	N	Y	N	N	Y	Y	N	N	N	N	Y
google-analysis.com	N	N	N	Y	N	Y	N	N	N	Y	Y
adbrite.com	Y	N	N	Y	N	Y	N	N	N	N	N
yeildmanager.com	Y	N	N	N	Y	N	N	N	N	N	Y

2.3 Third-party Domains Used by SNSs

Privacy leakage to other users / parties in SNSs, due to privacy settings, is discussed in previous sub-section. Another potential source of privacy leakage is the third-party advertisers or data aggregators who can tack the users' actions. If SNSs are making use of third-party domains that are tracking user visits to these sites and other websites, then there is a greater potential for privacy loss. Table 7 shows key results of the analysis made by Krishnamurthy and Wills [10] with the most widely used third-party domains. Here, letter 'Y' indicates situations, where the third-party domain was used in the majority of the five sessions, executed at the given SNS. The eight third-party domains with at least three Y's are shown in the table 7 and it can be observed that, the overall high usage third-party domains are doubleclick.net, 2mdn.net, advertising.com and atdmt.com across most SNSs, highlighted in red. The next sub-section, describes how the information is leaked to these third-party servers.

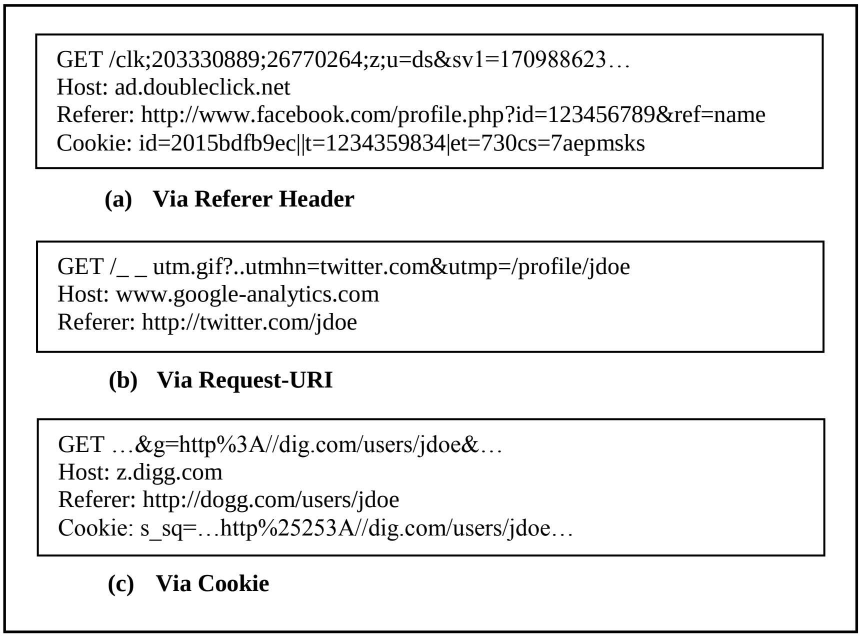
2.4 Leakage of User Information to Third Party

Krishnamurthy and Wills [11] examined the results of actions performed while logged onto each of the 12 SNSs in their study. They found four types of PII leakages involving:

- Transmission of the SNS identifier to third-party servers from the SNS,
- Transmission of the SNS identifier to third-party servers via popular external applications,

- Transmission of specific pieces of PII to third-party servers and
- Linking of PII leakage within, across, and beyond SNSs.

The possession of SNS identifier, allows a third-party to gain much PII information about a SNS user, to join with the third-party profile information about a user's activity on non-SNS sites. Analyzing the request headers via the 'Live HTTP Headers' extension, it is found that the SNS identifier is transmitted to a third-party in at least three ways: the referrer header, the Uniform Resource Identifier (URI) or a cookie. Examples for these three types of leakages are shown in Figure 3(a), Figure 3(b), Figure 3(c) respectively (SNS identifier of '123456789' or 'jdoe' is substituted for the actual identifier. Cookies and other strings are also anonymized). Accesses to third-party servers are often triggered without explicit action on the user's part.



```
GET /clk;203330889;26770264;z;u=ds&sv1=170988623…
Host: ad.doubleclick.net
Referer: http://www.facebook.com/profile.php?id=123456789&ref=name
Cookie: id=2015bdfb9ec||t=1234359834|et=730cs=7aepmsks
```

(a) Via Referer Header

```
GET /_ _ utm.gif?..utmhn=twitter.com&utmp=/profile/jdoe
Host: www.google-analytics.com
Referer: http://twitter.com/jdoe
```

(b) Via Request-URI

```
GET …&g=http%3A//dig.com/users/jdoe&…
Host: z.digg.com
Referer: http://dogg.com/users/jdoe
Cookie: s_sq=…http%25253A//dig.com/users/jdoe…
```

(c) Via Cookie

Figure 3: Leakage of SNS identifiers to third-party [11]

3. PRIVACY-RELATED THREATS

There is a trend in SNSs culture that the more contacts you have, the more popular you are and more influence you have. SNSs members broadcast information much more widely, either by choice or by mistake [9]. Previous section discusses the information leakage. This section focuses on most important privacy threats due to such information sharing and thus leakage.

3.1 Digital Dossier Aggregation

It is feasible to take regular snapshots of an entire network and to store the profiles of users, because cost associated with disk storage and Internet downloads is greatly diminished, but complete deletion of the data which is no longer necessary is very costly and technically challenging which results in digital dossier of personal data by the owner of SNSs and third-parties. This information can be very embarrassing or even damaging as some reports shows that due to review on SNSs, people are missing out employment opportunities [20]. The Miss New Jersey was threatened with publication of images taken from her SNSs profile [15]. Two tennis stars were suspended because of revelations made on an SNS [32].

3.2 Secondary Data Collection

It is found that often willingly users share the personal information, but unknowingly some information is disclosed using network itself: data such as time and length of connections, location, IP Address, other users' profiles visited, messages sent / received and so forth. Currently data collection policies are not transparent.

The following is an example of a privacy statement: "We also receive other types of information about you: We receive data from the computer, mobile phone or other device you use to access Facebook, including when multiple users log in from the same device. This may include your IP address and other information about things like your internet service, location, the type (including identifiers) of browser you use, or the pages you visit. For example, we may get your GPS or other location information so we can tell you if any of your friends are nearby.

We receive data whenever you visit a game, application, or website that uses 'Facebook Platform' or visit a site with a Facebook feature (such as a 'social plug-in'), sometimes through cookies. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.

Sometimes we get data from our affiliates or our advertising partners, customers and other third parties that help us (or them) deliver ads, understand online activity, and generally make Facebook better. For example, an advertiser may tell us information about you (like how you responded to an ad on Facebook or on another site) in order to measure the effectiveness of - and improve the quality of – ads" [22].

Privacy policies are not clear in specifying what is personal information and what is not. The above policy statement does not specify, which elements of profile information are disclosed to third-parties.

Furthermore, intrusion becomes most crucial in this case, as aggregated data can be leaked to intruders. Hence, network security tools are of great importance to meet enhanced privacy of user & security of network. As discussed by Patil et al. [13] IDS systems, an important subset of network security tools, available today are not easy to use and thus, can affect the security of entire network badly. The users of IDS system are mainly classified as LAN administrators, security professionals and network programmers but, not limited to them and are increasing from network administrator to daily computer users. Hence, improvement of usability in network security tools discussed by Patil et al. will definitely help in the process understanding and usage of not only IDS systems but also of other network security tools and thus, effectively maintaining users' privacy.

3.3 Face Recognition

Photo sharing is one of the most important and popular feature of SNSs. As an example, Facebook hosts in excess of 220 billion photos, as of Dec. 2012. These images are associated with users' profiles and thus with identity of users (e.g. through tagging). Hence one can correlate the profiles across services using face recognition through mash-ups. For example, profile on friendship and dating site- Facebook can be linked with highly professional site- LinkedIn [17].

3.4 Content-Based Image Retrieval (CBIR)

The information can be disclosed also through Content Based Image Retrieval (CBIR). By looking at contents of images, CBIR engines can provide fine grained results, matching features such as identifying aspects of a room [6, 18]. Many SNSs have not employed privacy control over information leakage through CBIR. One can look at a privacy related statement: "When you post things like photos or videos on Facebook, we may receive additional related data (or metadata), such as the time, date, and place you took the photo or video." [22].

From above privacy statement, it is clear that along with face recognition other aspects of images can also raise concern about threats due to CBIR. For example, CBIR can link locations of user through recognition of common objects in images of users' homes, which raises concern regarding threats related with disclosure of location information and many more such as black mailing, unwanted marketing etc.

3.5 Linkability from Image Metadata and Tagging

Many SNSs allow users now to tag images with metadata such as the name of the person in the photo, a link to their SNS profiles [23]. Another aspect of image metadata is that many cameras embed metadata (in many cases serial number of camera also) about the camera in the image. Because of warranty registration cards these cameras are linked with addresses also, giving out threat to users' privacy. For example, posting of full illegal copy of Harry Potter and the Deathly Hallows which included embedded versions of the serial number of the camera used to take it, as well as the exact date and time the images were taken [19].

3.6 Deletion of Account

A SNS such as Facebook send an email to the user, telling one about steps to reactivate one's account which was deactivated by user. It indicates that even after deactivating the account, user's information is maintained with SNS. Further, in order to delete complete information, even if user deletes account, user can only delete primary pages easily. Unless user manually removes all secondary information like public comments made on others' profile, it remains there with user identity. Hence deletion of secondary information is not feasible for user. Moreover, in general, there is ambiguity as to whether information will be deleted upon account closure. As an example, the Facebook privacy policy makes the statement:

"When you delete an account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it.

Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains even after you delete your account."[22].

Users cannot exercise their fundamental right to control over their own personal information. This means that sites which do not provide easy means for deleting or rectifying information may be in contravention of the European Privacy Directive 95/46, which states: 'Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified'. 'Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.' 'Member States shall guarantee every data subject the right to obtain from the controller: as appropriate the rectification, erasure or blocking of data because of the incomplete or inaccurate nature of the data.' [21].

4. CONCLUSION

Facebook, Twitter and LinkedIn are most popular SNSs today with more than 1.3 billion users. Privacy of such SNS users is of main concern today. The sensitive information like user's personal photo, name, gender and location are more prone to leakage until proper privacy settings are applied by user. The different types of PII leakages show that knowingly or unknowingly user can leak information to other users or services, which can misuse the information further. Due to this information leakage, threats related to digital dossier aggregation, face recognition and CBIR can harm users' privacy. Hence, there is a need of improvement in code development from SNS providers. Different privacy policies of SNSs available today are inadequate in order to maintain users' privacy and SNS providers have to work on this aspect.

5. ACKNOWLEDGMENTS

We thank Mr. Jayesh Saindane for proof reading of the paper.

6. REFERENCES

[1] Bhutkar, G. 2009. Users on Social Networking Sites, Journal of HCI Vistas, Volume V (2).

[2] Boyd, D. 2004. Friendster and Publicly Articulated Social Networking, ACM Conference on Human Factors and Computing Systems (CHI), Vienna, Austria.

[3] Boyd, D. 2008. Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence, International Journal of Research into New Media Techchnologies, Volume 14, pp. 13–20.

[4] Boyd, D. and Hargittai, E. 2010. Facebook Privacy Settings: Who Cares? , Journal of First Monday, Volume 15 (8).

[5] Boyd, D. and Schultz, E., Schultz, J. and Palfrey, J. 2011. Why Parents Help Their Children lie to Facebook about Age: Unintended Consequences of the 'Children's Online Privacy Act', Journal of First Monday, Volume 16 (11).

[6] Chin, Y., Roussev, V., Richard III, G. and Gao, Y. 2005. Content-Based Image Retrieval for Digital Forensics, The International Federation for Information Processing, Volume 194, pp 271-282.

[7] Ellison, N. and Boyd, D. 2013. Sociality through Social Networking Sites, The Oxford Handbook of Internet Studies (Ed. William H. Dutton). Oxford: Oxford University Press.

[8] Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networks, ACM Workshop, Privacy Electronic Society, pp. 71–80.

[9] Hogben, G. 2007. Security Issues and Recommendations for Online Social Network, European Network and Information Security Agency (ENISA), Position Paper.

[10] Krishnamurthy, B. and Wills, C. 2008. Characterizing Privacy in Online Social Networks, ACM Workshop on Online Social Networks, Seattle, USA, pp. 37–42.

[11] Krishnamurthy, B. and Wills, C. 2009. On the Leakage of Personally Identifiable Information via Online Social Networks, ACM workshop on Online Social Networks, pp. 7-12.

[12] Kumaraguru, P. and Cranor, L. 2005. Privacy in India: Attitudes and Awareness, Workshop on Privacy Enhancing Technologies, Dubrovnik, Croatia.

[13] Patil, T., Bhutkar, G. and Tarapore, N. 2012. Usability Evaluation Using Specialized Heuristics with Qualitative Indicators for Intrusion Detection System. Advances in Computing and Information Technology, Springer Berlin Heidelberg, pp. 317-328.

[14] First European agreement of Social Networks - A Step Forward to Child Safety Online, available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/46&format=HTML&aged=0&language=EN&guiLanguage=fr , accessed on 26th Apr. 2013.

[15] Blackmail Claim Stirs Fears over Facebook, available at http://www.guardian.co.uk/business/2007/jul/16/usnews.news, accessed on 4th Apr. 2013.

[16] Validation, Authorization: the Next Steps to Identity Management, available at http://business.highbeam.com/409220/article-1G1-214562083/validation-authorization-next-steps-identity-management, accessed on 14th Apr. 2013.

[17] Campus Police Use Facebook, available at http://badgerherald.com/news/2006/01/25/campus_police_use_fa.php, accessed on 14th May. 2013.

[18] CBIR Demonstration, available at www.cs.washington.edu/research/imagedatabase/demo/, accessed on 20th Apr. 2013.

[19] Defending Your Rights in the Digital World- Harry Potter and the Digital Fingerprints, available at https://www.eff.org/deeplinks/2007/07/harry-potter-and-digital-fingerprints, accessed on 10th May. 2013.

[20] Delete Your Bad Web Reputation, available at www.wired.com/science/discoveries/news/2006/11/72063, accessed on 23rd Feb. 2013.

[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT , accessed on 12th May. 2013.

[22] Facebook - Data Use Policy, available at https://www.facebook.com/about/privacy/your-info, accessed on 15th May. 2013.

[23] Facebook - Tagging Photo, available at http://www.facebook.com/help/463455293673370/, accessed on 5th Feb. 2013.

[24] Facebook: Threats to Privacy, available at http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf, accessed on 27th Apr. 2013.

[25] Hofstede Analysis, available at http://www.cyborlink.com/besite/hofstede.htm, accessed on 20th Apr. 2013.

[26] List of Social Networking Sites, available at http://en.wikipedia.org/wiki/List_of_social_networking_websites, accessed on 10th Feb. 2013.

[27] Photos & Videos as Social Currency Online, available at http://pewinternet.org/Reports/2012/Online-Pictures/Additional-Material-and-Demographics/Demo-Portrait.aspx, accessed on 18th Apr. 2013.

[28] Privacy and Security Issues in Social Networking, available at http://www.fastcompany.com/articles/2008/10/social-networking-security.html?page=0%2C0, accessed on 7th Nov. 2012.

[29] Privacy, available at http://en.wikipedia.org/wiki/Privacy, accessed on 3rd Oct. 2012.

[30] Social Network Service, available at http://en.wikipedia.org/wiki/Social_network_service, accessed on 4th Feb. 2013.

[31] Teens Kindness & Cruelty on Social Network Sites, available at http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx, accessed on 18th Nov. 2012.

[32] Tennis LTA Suspends Top Junior Players, available at http://news.bbc.co.uk/sport2/hi/tennis/7010983.stm, accessed on 3rd May. 2013.

[33] Top 15 Most Popular Social Networking Sites, available at http://www.ebizmba.com/articles/social-networking-websites, accessed on 10th Feb. 2013.