A Study on Retrieval of Information through Social Sites

Ashish Shah, Dr. A. S. Khandelwal

Abstract— Online social networking sites have become one of the greatest social technological advancement of the 21st century. However, most users of such Social Networking Sites are unaware of the privacy issues related to their profile. By placing personal information on the site, users make themselves available to online traders for selling of their personal information to third parties and in some instances, websites owning everything, an individual's places on their profile page or friend's page, including photos. The problem is intensified because of the fact that communicating online via social networking sites has become not only popular but fashionable and also a necessity for the youth in order to maintain their online social connection among friends. Because of this, young people are especially at risk of exposing themselves when sites are joined without any thought as to what may happen to personal information, photos and video. This paper looks to privacy issues of online social networking sites from around the world such as Myspace, Facebook as social site.

Index Terms— Social Networking Site; profile; friends; facebook;Myspace.

I. INTRODUCTION

One of the matchless techniques developed in this century is Social networking sites. More or less every young person aged 14 to 30 years participate and interact with their favorite social networking site from around the world on a day to day basis, such as well-liked sites Facebook and MySpace which are popular around the world including India. There are different range of social networking sites that offer a range of services from blogging, sharing photos and video and sites where planning different activity such as traveling[1]. However this paper restricts itself to those sites, that focus on individuals creating a personal profile, as it is this class of SNS which involves posting users personal information on public portal.

Once a user has created a profile he/she can invite others become friends and followers, usually agreement by both people is required for this to occur. Once associated, a light connection is established between there profiles, usually this connection is by users having same interest area common work place or city or some social link. While we, in our research mostly focus on the unconstructive side of online social networks, social networking site also have many benefits that people gain by interacting with others, on such social sites[2]. There is still research suggesting that social networking is a boon for some isolated, and that online social

Ashish Shah, Research Scholar, Department of Electronics & Computer Science RTM Nagpur University, Nagpur, India,

Dr. Abha Khandelwal, Department of Computer Science, Hislop College, Nagpur, India.

network sites can actually be of major benefit to them.

A. Why socialize online?

Today being social, equals to creating online personal profiles. A profile through which the user can connect with several people. Social Networking site have become very popular for people to communicate with family, friends and colleagues from around the globe. SNS is a new medium to exchange views and communicate and share data. While there are benefits from this approach of communicate there are information security and privacy concerns. Now a days for every youth, SNS has become a new place to 'hang out'. Youth continue to find a private space for hang out that are their own, not considering of what technologies are available. Socializing online is a place to connect, especially important to young people as it provides a virtual space irrespective of their identity.

B. Why are youth volunteering personal information?

When any user creates a personal profiles online, they often include identifiable information like full names, Date of Birth, home town, school, relationship status, sexual preference, mobile numbers, birth place and email addresses. PEW research on American teens showed that 82% of teens with online profiles post their first name, 79% a photo of themselves, 61% their city/town name, 49% include the name of their school and 29% their last name.

Why young people are so willing to share personal information with often complete strangers they met online is an interesting fact. A common delusion is that young people use social network sites to form new friends or relation, while most use it to keep connections that already exist. Today's youth are more willing to place personal information on their profiles as they believe or assume that most people who will view their page will be known 'friends.' However, it is much easier to become a 'friend' online than offline as many users do not restrict their privacy settings to only friends.

Today's changing culture is also one of the main reasons for personal to keep information and share them on social network sites. Increased familiarity and confidence in technology and lack of exposure or memory of misuse of personal data had led people to share their data online[3]. It was also obvious from the survey that 18-34 year olds are much more likely to be comfortable providing detailed personal information to join social network sites than those above 50 years old[4]. This is because young people have grown up with the internet where it has become usual to provide personal information to use certain online services.

II. PRIVACY ISSUES

Generally privacy concerns are common to all people who are using social networking websites, some show more privacy issues than others. We will try to focus on the following issues authorization, control of personal data, data collection and data deletion. Personal data is defined to mean any information or content which can be reasonably identifiable to an individual. We will try to cove the following issues in our research.

A. Authorization

A reoccurring issue is 'consent' which states that the way in which data will be used should be open and accessible and the Purpose Specification Principle which states that data should only be used in ways in which are expressed at the time of agreement. The issue of consent can be considered at several stages. Firstly, at time of registration, secondly, what is *done* with the registration information and lastly, whether the information that users *voluntarily* provide on their profile pages is within the boundaries of what was originally 'consented' to.

Consider facebook which asks users to type in their current email account password so the site can access the account's contact list in order to find email addresses that are not already registered as user to their site. However the issue is that the site is indirectly accessing personal email accounts and passwords. While it is possible to skip this step, but many users would assumingly do this without much thought as it is towards the end of the registration process. Consent in relation to information voluntarily offered on profile pages.

Amount or limit of information uploaded on Social networking site is up to user as they have a right to do. However users of such sites are simply not aware of what may happen to the information they place on these profiles.

B. Consent and third parties

SNS such as Facebook and MySpace both allow third parties widgets to access its core functions. Facebook, for example, permits any company or person to develop an application that will end up looking as though it is part of Facebook itself and users can opt-in to use the additional feature. In order for the application to be added it requires access to personal information. It is not all clear to the user exactly what information the application may be gaining access to. Also implicated is the fact that many users may not be aware that third parties or related partners of the social network sites may be able to obtain information about a user.

C. Authority of Personal Information

Although in many ways a user offers authority when they sign up to an online site, most are unaware of the implications of voluntarily providing personal information on profiles as well as not being aware of how this information may be processed. An individual can lose control of their data when a digital dossier of personal information is generated. This occurs when profiles on social networks sites can be downloaded and stored over time by site operators for back up purposes so as to incrementally create a digital dossier of personal

information[5]. This can also occur out of the control of the user, as user's 'friends' on their sites can write a comment about them on another friends profile or 'tag' the individual in photos. It is in this way that profile information has the potential to be used in ways that the user did not intend and stored for indefinite periods. The main threat associated with digital dossier aggregation for young users is when future employees or colleges are able to perform searches that may bring up data or even compromising photos that an individual thought either no longer existed or not possible for that source to obtain.

D. Data Collection

On registration, online social networking sites require certain pieces of information such as birthdays and addresses which are debatably not vital to creating and maintaining the service. For example, Facebook, Orkut, Cyworld and MySpace all require a full name, date of birth and email address [6]. The data which is uploaded can be used to hamper the user. Users of such social networking site do not realize how they provide their important data online. Consider Facebook as site, this has many applications which asks for some question to be answered. Question such as your pets name, school first attended etc. Analyzing them carefully and we realize that these question are the same, which are asked for your password recovery.While this may be a breach of the Collection Limitation Principle, it process assists in protecting minors from joining the website and keeps the site relatively free of illicit material and cyber predators due to the fact that offenders are highly identifiable [7].

E. Data Deletion

Online data uploaded on social networking cannot be deleted completely, while individuals have a right to have their personal data completely deleted. Most social network sites have an option for user to de-activate their profile. But it was noticed that de-activating account does not actually erase the total information uploaded by the individual. Features of SNS such as post comments and mainly chats with friends are never deleted. This practically volatile the fact of de-activation the users account. This means personal information can be stored indefinitely even though a user may believe that all aspects of their account have been deleted[5].
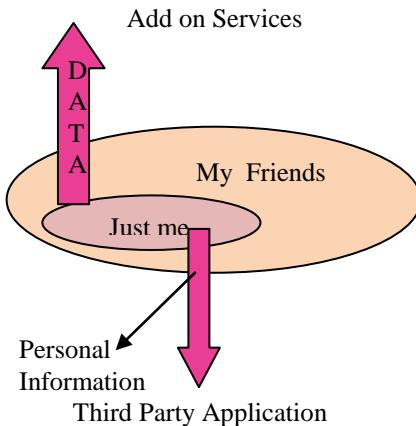
III. EFFECT OF PRIVACY ISSUES

The rate at which the social networking sites users are increasing has also increased the risk on such sites. Teen users

are creating their profile without considering the privacy issues related to their data. Such users are not concerned with the sensitive data that they are uploading, are valuable to others and can be misused by anyone with access to them. Personal photos and videos that they share can be used as a raw material to damage them. The advancement in the techniques to store bulk amount of data online has increased the ability of digital dossier. A full bio-data of any user can be kept online. A fact is that, now techniques such as digital dossier know more about us and can track us. The fact is all users of online networking sites think that it is impossible for someone to be eager to access or hack our data, thus most users don't care about their profile security. The fact is anybody can be on the target to be hampered online.

IV. DISCUSSION

The study on privacy concern in SNS reveals that data deletion is in fact is myth. Even though users delete their profile and assume that the data is not online anymore but the fact is that the data is still available in the form of comments or message on the web. Online services have a loop hole to access user's personal information. This proves the fact that data is retrieved in a hidden form. Latest technologies are capturing market with each passing day which facilitates for boundless extraction of data, which in turn directly hamper confidentially of data. The very concept of maintaining confidentially of information is badly damaged.

V. CONCLUSION

It is difficult to balance the right of privacy and control of personal information when individuals voluntarily place personal information on their profile. Once information is placed on public domains users can easily lose control over who sees their data and how it may use it. While there are privacy settings to protect users, in practice users are least bother about the privacy concern.

The underlying issue is that young people are simply not concerned or aware of issues concerning their personal data on social networking sites or placing detailed information on their profile pages. Because a change in teen culture is unlikely, the corporations behind social networking sites must act with more responsibility. Action must be taken on a multilateral scale such as cross border agreements on privacy standards to reduce the, identity theft and other types of privacy concerns as there is a obvious difference between privacy regulations between countries such as Australia and the US compared to Brazil. Organizations such as the OECD, APEC and other regional organizations have the potential to be instrumental in developing tighter cyber privacy laws. This must be encouraged and insisted upon in order to ensure social networking sites better protect people who are connected with it.

REFERENCES

[1] Danah Boyd, 'Why the Youth (Heart) Social Networks Sites: The Role of Networked Publics in Teenage Social Life' (2007) Youth, Identity, and Digital Media Volume,MacArthur Foundation Series on Digital Learning, 6.
[2] Danah Boyd, Identity Production in a Networked Culture: Why Youth Heart MySpace (Speech to be delivered at the American Association for the Advancement of Science, USA, February 19, 2006).
[3] Unisys, 'Minimising Risks of Online Social Networking' (Press Release, 11 December 2007).
[4] Definition adapted from the Privacy Act 1988 (Cth) Section 6.
[5] <http://www.facebook.com/policy.php> at 3 December
[6] Information gathered by beginning the registration process from the respective homepages; facebook.com, cyworld.com, myspace.com, orkut.com.
[7] Facebook, *Platform Application Terms of Use* (24 May 2007) *<http://www.developers.facebook.com/user_terms.php>* at 17 January 2008.

INTERNET RESOURCES

Facebook, Facebook's Privacy Policies (6 December 2007) <http://www.facebook.com/policy.php> at 6 January 2008.

Facebook, About Facebook (no publish date specified) < http://www.facebook.com/about.php> at 14 January 2008.

Facebook, Terms of Use (15 November 2007) <http://www.facebook.com/terms.php> at 3 December 2008.

Google, Google Terms of Service (2007) <http://www.google.com/accounts/TOS?hl=en-US > at 3 December 2008.

Google, Google Privacy Policy (14 October 2005) <http ://www. google.co.uk/privacypolicy.html> at 3 December 2008.

Orkut, Orkut Privacy Policy (2006) <http://www.orkut.com/Privacy.aspx> at 3 December 2008.

Orkut, *Orkut Privacy Notice* (21 May 2008) <http ://www. orkut.com/privacy.aspx> at 3 December 2008.

LinkedIn, Privacy Policy (July 14 2006) <http://linkedin.com/static?key=privacy_policy> at 11 January 2008.

Mixi Home Page: <http://mixi.jp>

MySpace, About Us (2007) < http ://www. myspace.com/index. cfm?fuseaction=misc.abo utus> at 14 January 2008.

MySpace Privacy Policy (26 August 2005) <http://collect.myspace.com/misc/privacy.html at 10 January 2008> at 3 December 2008.
Wong, Grace, Personal Info on Sites like MySpace is a Bait for Cybercrime (October 4, 2006) CNNMoney, <http://money.cnn.com/2006/10/03/technology/social_net working_risks/?postversion=2006100406 > at 21 December 2007.

https://eview.anu.edu.au/anuuj/vol1_09/pdf/11.pdf