TITLE: PRIVACY POLICY ON SOCIAL NETWORKING WEBSITES

SUBJECT: COMPUTER SECURITY

TYPE OF WORK: DISSERTATION FULL

FILE NAME: GR9-DISSERTATION

PRIVACY POLICY ON SOCIAL NETWORKING WEBSITES

Table of Contents

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.0 Introduction

The Web, the Internet and the electronic mail, introduced revolutions in the way the world communicates and collaborates. Their mass adoption by different facets of the population is one of the major technological success stories of the 20th century. There are other issues to be dealt with right now which include problems like information overload that necessitates smarter and more fine-grained computer support for networked information. There is also a need to blend the boundaries between personal and group data. This should go hand in hand with safeguarding privacy and establishing trust online.

Social networks have become an important online service with a wide range of applications which include collaborative service rating, collaborative work; sharing of resources identifying new friends etc. these websites have become an important area of study both in computer and social sciences. There have been numerous literatures which have carried out in-depth studies on social networking sites. These websites often network users so they can publish and share information and services and thereby create a community of web users. The type of information published often includes personal data, blogs and other resources..

A recent survey published by PEW Internet and American Life Project indicated that 75% of US adult Internet users age 18–24 have a profile on an online social networking site (Lenhart 2009). This highly rated commercial potential and rapid growth of many more networking websites has been overshadowed by the privacy issues. Huge amounts of personally identifiable information is revealed and disseminated on these websites which has given rise to growing privacy concerns among various stakeholders. These

stakeholders include networking website providers, marketers, government, parents of children and other users on the social networks (Acquisti and Gross 2006, Dinev et al. 2009).

The right to privacy can be defined as "the right to be let alone" (Warren and Brandeis 1890). This has formed the basis on which other privacy laws all over the world have been developed. There are strict regulations enforced by many countries which impose rules for the collection, handling, and processing of personally identifiable data. The main objective of many networking experts is to guarantee users the control on the flow of their personal data (Bygrave 2002, Room 2007).

The wide and in depth display of personally identifiable information by users of social network applications on the Internet has raised concerns for a number of privacy advocates. While an increasing amount of privacy abuses occur via social network applications including unwanted exposure, badmouthing, identity theft, cyber-bullying, distortion, or reputational damage become known, the demand for serious controls to protect the individual user from any damage increasingly coming unknowingly from users themselves (Weiss, 2009).

1.1 Introduction to online networking

Online social networking has moved from niche phenomenon to mass adoption in the last decade. There has been a rapid increase in participation in very recent years and this has been accompanied by a progressive diversification and sophistication of purposes and usage patterns across a multitude of different sites by different user demands and user requirements (Newitz, 2003).

The boundaries describing these websites are blurred however most online networking sites share certain identifiable features: Each site offers an individual a "profile". The profile is a representation of their personal identity and, often, of their own social networks to identify their friends and acquaintances. It is also used by others to peruse, with the intention of contacting or being contacted by others and to make new friends or dates, find new jobs in specific work related networking sites, receiving or providing recommendations and much more (Liu and Maes, 2005).

1.2 Background of the study

1.2.1 Defining Social Networking Sites

Boyd and Ellison (2007) defined social network sites as web-based services that allow individuals to:

(1) Semi-public profile within a bounded system can be constructed

(2) A list of other users with whom they share a connection can be articulated.

(3) A list of connections and those made by others within the system can be view and traversed.

They allow individuals to meet strangers and also they enable users to articulate and make visible their social networks is the uniqueness of these social networking sites. This can result in connections between individuals that would not otherwise be made in day to day instances. Most connections made are latent ties who share some offline connection however distant they may be (Haythornthwaite, 2005).

Deleting Online Predators Act of 2006 (Fitzpatrick, 2006) has been proposed recently and this states the term "commercial social networking website". This indicates a commercially operated Internet Web site that:

"(i) allows people to create profiles or web pages which provide personally identifiable information about themselves and are available to others users who may or may not be linked to them and

(ii) May present a mechanism for keeping in touch with other users, such as a forum, chat room, email, or instant messenger." (Fitzpatrick, 2006).

1.2.2 Social Networking Sites (SNSs) - Architecture

The key repeating characteristics found across consumer social network sites are as follows:

- Description of an action through a visible profile within a bounded system.
- A semi public display of the inter connections and inter links between an actor and his friends
- A display of mutual friend lists.
- A system to display and identify methods for people to traverse those connections. This is seen in many websites which enable an actor to view profiles associated with the list of "friends" of his friend. (Boyd and Ellison, 2007)

Users can, create their 'profile' by giving vital information and upload a picture of themselves and can often be "friends" with other users. In most social networking services, both users are required to confirm that they are friends before they are linked and their information of each other can be viewed. Social networking sites typically have sections which are involved in dedicating comments from their different friends. This is indicated by different terminologies in different websites. This section is called "Testimonials" on Orkut whereas on Facebook, this section is called "The Wall". Initially this was a feature which encouraged people to write messages about the person in the profile so that more people could view the profile. But as time progressed the testimonials became a creative form of expressing ones wit and humor (Ellison et al., 2007).

1.2.3 Social Communication – for Internetworking

Much of the research on online communities assumes that individuals using these systems are often connected with users outside their pre-existing social group or location, liberating them to form communities around shared interests which make better ties as opposed to shared geography (Wellman et al, 1996).

Teenagers and young adults now use organized social networking web sites to meet others and explore identity formation. These sites can be viewed within a larger trend that shifts the influence of interpersonal correspondence and face to face communication to mediated messages.

Anderson (2001) has suggested that among college students and high school students, excessive Internet use might be related to developmental issues like establishing new relationships, peer group development and identity formation. Research on social networking sites is beginning to accumulate (Boyd and Ellison, 2007) and there are indications that they may be used to bridge online and offline social networks (Boyd and Ellison, 2007).

A survey of all incoming first year students at a major Midwestern university was conducted. It was seen that most students used Facebook for social purposes — to stay in touch with their friends from high school as well as to form interconnections with people they had met recently but do not know very well such as in their dormitories or in class (Lampe, Ellison and Steinfield, 2007).

These ties appear to have some positive benefits and greater social networking website use was associated with more perceived social capital. Social network sites use was related to all three kinds of perceived social capital:

- Resources that stem from one's weaker ties indicate bridging social capital.
- The resources that stem from one's more intimate ties indicating Bonding social capital,
- The resources that stem from one's prior ties indicated by maintained social capital. (Subrahmanyam et al., 2008).

1.2.4 Social Networking Websites – A Bridge Between Offline and Online Connections

The assumed online to offline directionality may not apply to today's social networking sites that are structured both to emphasize existing connections and enable the creation of new ones thereby blending online and offline networks. However, because there is little empirical research that addresses whether

members use social networking websites to maintain existing ties or to form new ones, the social capital implications of these services are unknown (Morgon and Cotton 2003). With regard to social networking sites high school students and college goers have been reported using the sites to keep in contact with peers from their offline lives. This is done to ensure that they make plans with friends that they see often or to keep in touch with the lives of friends they rarely see (Lenhart and Madden, 2007).

Emerging adults' online and offline worlds are connected can be very clearly gleaned from a qualitative and quantitative analysis of autobiographical essays written by young adult college students (Mcmillan and Morrison, 2008). The participants in this study did not use the Internet for identity exploration but instead used it to strengthen their offline links with friends and acquaintances. There has been determination by the authors that the participants used their online virtual communities to sustain and build their real communities that existed in real life, such as using online tools to plan social events with their day to day friends and colleagues (Lenhart and Madden, 2007).

1.2.5 Defining Privacy

Defining the term 'privacy' is a difficult task as the associated semantics differ from one individual to another across countries, cultures and also depend on the context under study. For rewards, usability, or other factors individuals are often willing to sacrifice their privacy. Privacy is often related to the idea of security, control, anonymity, and access and can be extended to other areas dependent on the field of study (Altman, 1975).

The right for privacy includes some degree of control over personally identifiable information that others view, collect and transmit, and emphasizes a right to verify the accuracy of this information. There are four privacy states which have been described by many authors which can be classified based on the different state of mind of the user. They are solitude, intimacy, anonymity, and reserve. There are five privacy functions which follow the same principle of identifying and disseminating personal information namely personal autonomy, emotional release, self-evaluation, and limited and protected communication which contribute to maintenance of privacy amongst the users.

Westin (1967) and Turn (1985) have defined privacy as ''the right of individuals to control the process of collection, processing, dissemination, storage, and use of their personally identifiable information.''

Culnan (2000) defines privacy as the ability of the people to control and determine the terms under which their personally identifiable information can be acquired and used by other users and marketers. The classical definitions of privacy can be interlinked with recent technological developments and experiences in the ubiquitous computing area and social networking trends and can be re defined by incorporation the following three factors:
(i) Solitude, or control over one's personal interactions with other people;
(ii) Confidentiality, or control over other people's access to personal information; and
(iii) Autonomy, or control over what one does.

1.2.6 Rise in Cybercrime Caused Invasion of Privacy

With the advances in the communications development and internet technology it is now very easily possible to connect practically any computer in the world to the Internet. While this is very useful for certain information dissemination purposes it is very difficult to contain privacy. Connecting to the Internet means connecting to millions of computers or computer networks locating in different part of the world and this makes access of personally identifiable information very easy. The Internet is available all over the world and can be accessed easily from anywhere at any time and at a considerably low cost. This has increased the issues of information hacking and privacy invasion.

'Personal space' has multiple dimensions and can be defined in particular privacy of the person which is concerned with the integrity of the individual's body, privacy of personal communications, privacy of personal behavior, and privacy of personal data (Lenhart and Madden, 2007). Information privacy indicates that the claims individuals make that the personal data input by them should generally not be available to other individuals and organizations unless indicated by the user, and that, where data is possessed by another party, the individual must be able to exercise considerable degree of control over that data flow, use and processing (Bern, 2007).

The Internet is like a gateway to an enormous level playing field for many criminals. Internet makes it possible for unsavory elements to access the information communication systems, and thus affecting lives of great numbers of people in different parts of the world. The access of personally identifiable information has become very easy with this new era of hacking and internet crime (Blakely 2007). The potential and impact of crime committed on, or facilitated by, the Internet especially over social networking sites is very big. People of different age groups and societies are affected by criminals using web postings or mass emails, and spreading harassing online messages containing sensitive personal information or threatening to harm the victims (Savona and Mignone, 2004).

1.3 Rationale for the Study

1.3.1 Privacy on the Internet

A survey entitled Harris Interactive for The Privacy Leadership Initiative had documented online user and online consumer concerns with regard to protection of privacy over the internet as well as security of personally identifiable information availability, storage, processing and dissemination. Individuals who have not bought over the Internet list security of information storage and transmission often indicate that they are worried that their information would not be safe online and would prefer not to give out such information (Harris, 2001).

In 2001 by an American Demographics survey documented very much in detail the fears of privacy violations. They indicated that children's privacy breaches were the most feared by parents and teachers which was very closely followed by misuse of private information, identity theft and financial theft (Paul, 2001).

Privacy issues online have many different features which include 'spam', usage tracking and data collection, obtaining credit card numbers, hacking of third party transfers and other choices. This information may then be shared with so many other sources thereby causing increase in issues of privacy. These areas of concern were discussed in detail in the survey which was described by Wang et al. (1998) and clearly seen and expressed the Federal Trade Commission's standard for privacy on the Internet. The FTC identifies notice, choice, access and security as elements of a desirable privacy policy.

Consumers' reassurance that the information shared will be subjected to proper privacy procedures and methodologies. Hoffman et al. (1999) has identified the significance of control over secondary use of information other than the purpose for which it was intended, concerns by consumers involved in Internet transactions.

1.3.2 Privacy in Relation to Social Networking Sites

On an average there is presence of vaster and weaker ties on online social networks than offline social networks. Millions of users can be classified as friends of friends of the user and can have umpteen opportunities to access her personal information. However these contacts have a very low threshold to

qualify as friend on somebody's network (Ellison et al., 2007). A different meaning is given to trust and privacy within these different and can have many different assignments (Bern, 2007).

The same information is provided to great number of friends and acquaintances connected to the subject through ties of different strength online social networks thereby making them more leveled. There is a decrease in intimacy trust while privacy is being considered conducive within the realms of an online social network (Bern, 2007).

1.4 Research Rationale

1.4.1 Research Aim

The aim of this research is to identify the various issues related to privacy policy on social networking websites.

1.4.2 Research Objectives

The major objective is to analyze the issues associated with the privacy policies on the websites of social networking.

1. To analyze the usage of the privacy settings of the site by the users
2. To investigate the nature of potential threats on various aspects of privacy of the users
3. To identify the extent of users who actually use or give importance to the limiting privacy preferences
4. To identify the factors driving the users to provide generous personal information and limited usage of privacy preferences.

1.4.3 Research Questions

A set of identified research questions should be framed so that a systematic process can be developed for the purpose of data collection. The research questions would contribute to the comprehension of the issues related to the privacy policies in the social networking sites. The following are the research questions framed for the present research for the dissertation work.

- What is the extent of use of privacy settings in the social networking sites and what proportion of users actually use these privacy preferences?
- What are the threats posed on the aspects of privacy?
- What are the factors that contribute to the generous provision of personal information and the limited usage of privacy preferences?

1.4.4 Research Methodology

In realizing the overall aims and objectives of the study, research methodology plays an important role. There are various methodologies existing for use in research. Qualitative methodology deals with analyzing huge mass of data that are reviewed in parts of literatures and also in case studies. Based on the data collected, conclusions on the research questions in the study could be arrived. Quantitative data involves the obtaining of empirical summaries from the information collected.

1.5 Conclusion

This chapter has introduced the study and explained the research processes to be undertaken in order to collect the necessary data. This data collected is to explain the rationale of the study and introduce the e research questions and meet the aims and objectives of the study. Based on the results of the data collected, the major issues involving the usage of privacy policies in the social networking sites would be identified. This would help the author recognize the areas where he needs to intervene and then recommendations for the same would be given. Chapter two records the findings of the literature review in relation to the study.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

For supporting the growth of business to consumer e-commerce there is a necessity to promote and the use of security, privacy and trustworthiness. These are important elements for supporting the growth of the internet industry. The extent to which privacy and security issues are indicated as distinctive and the lack of knowledge of how they are related is the two problems with the current social networking sites literature (Woodlock, 1999; 2000). Global terms such as safeguard assurances are used commonly to represent both privacy and security concerns. This conceptual error often causes discussion on the type of web features used: whether it is privacy or security. There is also an additional emphasis on how to place and convey these features on the site (Dayal et al., 1999).

2.1 Personally Identifiable Information

Personally identifiable information is defined as referring to Information which can be used to determine or find an individual's identity like their name, national insurance number, biometric records, etc. separately, or when joint with other intimate or distinguishing information which is linked to one separate individual, such as date and place of birth, father's name, etc. (Johnson, 2007).

There are three types of data namely *static, dynamic, and derived* data as classified by Corby, 2002 (see Table 1)

Table 1: Taxonomy of Data Types and Examples based on (Corby, 2002)

Type of Data			Sub-Type & Example
Static	Identity	Offline	1. *Bio-identity*: fingerprints, race, colour, gender, height, weight, physical characteristics, retinal pattern, DNA 2. *Financial identity*: bank accounts, credit card numbers 3. *Legal identity*: government ID numbers (SSN, Passport #, Driver's Licence) 4. *Social identity*: membership in church, auto clubs, ethnicity 5. *Relationships*: child of, parent of, spouse of 6. *Real Property Associations*: home address, business address
		Online	*Digital ID*: pseudonym, E-mail address, Username, IP address, Password
	Assets	Tangible	*Property*: buildings, automobiles, boats, mobile phones *Personal Worth*: credit balances, stock portfolios, debt balances
		Intangible	*Non-real property*: insurance policies, employee agreements
Dynamic	Historical		*Low Resolution: Transactions*: financial, travel, mobile phone records *High Resolution: UbiComp Sightings log (Time, Place)*
	Real-Time		*UbiComp Sightings ([Now], Place)*
Derived	Analyzed		**Data derived by analyzing trends over time** ***Financial behaviour*** 1. *Trends and changes*: month-to-month variance against baseline 2. *Perceived response to new offerings*: matched with experience ***Social behaviour*** *Behaviour statistics*: drug use, violations of law, family traits ***Tastes*** *Buying patterns*: purchase of item in a certain class suggests desire to buy other items in same class
	Composed		**Linking Data about person to other data** 1. *DNA analysis:* DNA linked to human genome database infers tendency to disease, psychological behaviour 2. *Multi-Data linking*: e.g. knowing a device with a given MAC address was seen at a given place/time and knowing that the number is registered to a person infers person was at place/time

Table 1: Taxonomy of Data Types and Examples Modified from (Corby, 2002)

2.2 Patterns of Personally Identifiable Information Revelation on Social Networking Sites

There are variable patterns of personal information revelation. There is a change in the type of identifiability across different types of social networking websites. There is encouragement of the use of real names to epitomize an account profile to the rest of the online social networking websites. Websites like Facebook have social norms like technical specifications, registration requirements which require different personal information. Thus the public identities of different participant profiles can be connected by these different aspiring websites. The dating and connecting sites like Friendster make sure to filter the

use of actual user names and profiles. This is important in the creation of a thin shield of weak pseudonymity between the public identity of a person and the personality one chooses to depict online. One way of doing is this is by making only the first name of a user visible to others in the website. This helps in hiding of the vital information and helps bring about privacy. Most sites encourage the publication of identifiable and personal photos which show clear shots of one's face without paying enough credit to different approaches to identifiability software available in the market (Gross et al., 2005).

Hobbies and interests are the main type of information revealed or elicited but can stride from there in different directions. Current and previous schools and employers, organizations involved and other semi personally identifiable information is available on some websites like the Friendster. Private information such as drinking and drug habits and sexual preferences and orientation are also some other semi-public information available in websites such as Nerve Personals. This also includes some open-ended entries available in LiveJournal (Gross et al., 2005).

The information visibility is highly variable. In certain sites especially those which include ostensibly pseudonymous information there are conditions to enable any member to view any other member's profile This kind of visibility tuning controls become even more refined on some sites which make no pretense of pseudonymity, like the Facebook (Gross et al., 2005).

2.3 Privacy Control Models

Privacy risk models to analyze how well a system meets such principles or avoids pitfalls are described by Hong et al. (2004). These risk models involve a set of questions on information sharing also indicating results pertaining to the social and organizational context in which the system is situated. The technology used in the model which is used to implement the system is also given special consideration. Hong et al., 2004 and Adams and Sasse (1999) provided a privacy model based on, information receiver, information sensitivity and information usage, in which each of the three factors interacts with the others to incorporate user perceptions.

2.4 Privacy Control by Users

In highly open network calendaring environments socio-technical mechanisms controlled privacy (Palen, 1999). Privacy partly via technical access control, partly via practices such as cryptic entries, partly via the norm of reciprocity, omissions, defensive scheduling was achieved by users.

Explicit user control of privacy in ubiquitous computing and its need was described by Bellotti and Sellen, 1993 and Palen and Dourish, 2003 described in depth the privacy requirements the complicated nature of user choice regarding what to disclose to whom in a networked world . Dawson et al., 2003 described the sensitivity is highly individual ranging from "naive and completely open" to "ultra paranoid and non-revealing". Ackerman and Cranor, 1999; ATandT, 2003 and Lederer et al., 2002 along with numerous literature is available to guide users on their privacy risks or suggest interface metaphors which encapsulate privacy preferences between one user and another

A user's policy may have been generated in a number of ways. This includes choosing a representative template from a community of peers providing suitable policies or from a trusted third party like as a consumer advocate as indicated by Yee and Korba, 2005. Support for user control over personal privacy policies is provided by Lederer et al.(2002). There is indication in the author's note that users require different personal privacy policies at the same time depending on the recipient of the data. The metaphor of *situational faces is used to* allow a user to show an anonymous "face" instead of his original face i.e., an anonymous identity is provided.

Users want to know how their personal information is being used and to have complete and absolute control over this type of usage. Applications should have clear cut information to explain to users what facts and assumptions about them are being stored in their databases and how these are going to be used or revealed to others. Users should be given ample control over the storage and usage of this data as it brings about increase in trust amongst the users. Langheinrich, 2002 indicates that trust in a social networking web site is a very important motivational factor for the disclosure of personal information

Applications should allow users to incrementally supply more information as their trust in the application increases as trust is built on positive past experience. The authentication and privacy control mechanism should make the process involved in the applications transparent to the end user. This direction is to give the user complete control over the partial models which are to be made available to which applications. The user model data required by any social networking site and the terms of use of the data are to be made aware to the user. This information plays the key role in the user being able to decide to whether or not to allow the site to access and use user data (Xiang et al., 2002).

2.5 Privacy Invasion Issues in Social Networking Sites

Albrechtslund, 2008; Boyd and Ellison, 2007; Gross, Acquisti, and Heinz, 2005 have made reports of exponential adoption and use of social networking sites which have been replaced by stories concerning the dangers and problems of digitally networked individuals operating in a global villages like the social networking sites. Social networking sites like facebook, orkut, MySpace etc have been used extensively by organizations to determine privacy issues. The high-profile failure of Facebook's advertising tool, Beacon, attracted excessive protest over the inappropriate transfer of personal information and claims of privacy invasion (Blakely, 2007; Sweney and Gosden, 2006).

Oxford University used Facebook to identify and fine graduating students for disorderly conduct on and off campus (Pavia, 2009) while in New Zealand the police published CCTV footage on Facebook which was an innovative maneuver to identify and catch a suspected burglar (Topping, 2009). These are some of the examples amongst thousands used by different organizations all over the world to achieve a sense of broader trends in privacy abuses typified by reputational damage, unwanted exposure and cyber-bullying. Parameswaran and Whinston, 2007 indicate that all these activities have highlighted an urgent need for greater research, and understanding about this emerging but important area.

Children being exposed to pedophiles (Lenhart, 2005); Teenagers being raped by people they meet on social networking sites (Antone, 2006;);Teenagers revealing too much information about themselves online (Bahrampour and Aratani, 2006; Downes, 2006); companies using the sites to collect marketing information (Hempel and Lehman, 2005; Verini, 2006); and, children under the age of 14 using social networks (Antone, 2006) are some of the number of social concerns associated with social networking sites.

Marketers who target teen consumers can use stated, personal information gathered from social networking sites for purposes other than what users intend. The commoditization of information has made it necessary to consider the invasion of privacy by corporations as indicated by Barnes, 2006. Schement and Curtis (1995) state that "information is gathered so that the economy can support its participants" and this information is used for wrong purposes by a number of marketers.

Schools can also access and use the information posted on social networking sites and cause privacy los issues to students. Chicago's Loyola University told numerous athletes to get off Facebook and MySpace or risk losing their scholarships (*Sports Illustrated*, 2006). In May 2006, a number of hazing photos

appeared on a site called badjocks.com which showed athletes from Princeton, Michigan, Fordham, and UC–Santa Barbara indulging in bad behaviour. This has led a number to schools to start investigations into student athlete behavior (Barnes, 2006).

2.6 Privacy Invasion Using Identifiable Images

The vast majority of profiles contain an image. There is no absolute requirement to provide a facial image, the majority of users do so in order to build their social popularity. These images can be classified into four categories:

1. Identifiable

Image quality is good enough and there is enough clarity available to enable person recognition. This can easily lead to access of other personally identifiable elements of the individual.

2. Semi-Identifiable

The profile image shows an image of the person but due to clarity issues or the image composition the person cannot be immediately indentified. However other aspects like hair colour, body shape, type of clothes worn etc can be identified.

3. Group Image

This image consists of a group shot or a number of people in the same picture thereby making it slightly more difficult to identify the actual user. However other information can still be gleaned from these images.

4. Joke Image

These images are clearly not related to a person and are usually celebrity images, animated or cartoon pictures. These images do not pose any privacy invasion issues (Weiss, 2009).

2.7 Public versus Private Boundaries

The private versus public boundaries of social media spaces are very hazy. The illusion of privacy creates boundary problems on the Internet. This illusion is felt most strongly by new users and those engaged exclusively in recreational domains (Katz and Rice, 2002). Teenagers, who often think their lives are private as long as their parents are not reading their journals have indicated that social networking tools, have become indispensable in life (Bern, 2007).

Teen use of social networking sites has increased to an average of one hour 22 minutes per day (Hempel and Lehman, 2005). Social networking sites are "already creating new forms of social behavior that blur the distinctions between online and real–world interactions." (Hempel and Lehman, 2005).

The sites deserve some blame for the release of personal information as there are some sign–up process which ask for e–mail addresses, pincodes and other vital personable information. This type of information demads and setting up requirements for membership tends to make people think it is safe to reveal personal information online. This indicates breaks in the public private boundaries and people unknowingly fall prey to this kind of privacy invasion (Sullivan 2005).

2.8 Privacy Implications

The level of identifiability of the information provided its possible recipients, and its possible uses are associated with privacy implications online social networking. Identification of the profile's owner is

possible in some social networking websites that do not openly expose their users' identities may inadvertently provide enough information. Face re-identification is one such example (Gross, 2005).

It is estimated that in a 25% overlap in 2 of the major social networking users often re-use the identical photos across different sites, an identified face can be used to identify a pseudonym profile with the same or similar face on another site. Similar re-identifications are possible through other demographic data and category-based representations of interests that reveal unique or rare overlaps of hobbies or tastes (Liu and Maes, 2005).

It would appear that the most of the users of Facebook are by large, quite oblivious, and unconcerned or are just pragmatic about their personal privacy (Newitz, 2003). Personal data is generously provided and limiting privacy preferences are sparingly used by most users. Users may put themselves at risk for a variety of attacks on their physical and online persona due to the variety and richness of personal information disclosed in Facebook profiles, their visibility, their public linkages to the members' real identities, and the scope of the network.These risks are common also in other online social networks, while some are specific to the Facebook and the Friendster (Phillips et al., 2005).

2.9 Online Privacy Policy Technologies

2.9.1 Platform for Privacy Preferences (P3P) Project

The Platform for Privacy Preferences Project (P3P) was developed by World Wide Web Consortium (W3C) to integrate machine-readable privacy policies into web browsers (Cranor, 2002). The W3C's Platform for Privacy Preferences (P3P) Project as indicated by Cranor 2002 enables websites to encode their data-collection and data-use practices in a machine readable XML format which is known as P3P policies. The W3C has also designed a P3P Preference Exchange Language which allows users to specify their privacy preferences. This usage of P3P and APPEL, a user agent which involved a program working on the user's behalf should be able to check a website's privacy policy against the user's privacy preferences, and thus automatically determine whether the website's data-collection and data-usage practices are acceptable to the user even if the user is unaware of his short comings. P3P appears to be the most widely used language for encoding enterprises' privacy policies for consumption by end-users (Anton, 2007).

2.9.2 Enterprise Privacy Policy Enforcement

Researchers at IBM are developing enterprise privacy architecture solutions as discussed by Karjoth et al., (2002) and Ashley et al., (2003) proposed a privacy-centric access control language i.e. the E-P3P and its successor EPAL. EPAL which stands for Enterprise Privacy Authorization Language is an abstract-level access control language, with features devoted to privacy protection, e.g., data accessing purposes.

2.10 A Framework for Online Privacy Protection Policy

To support the complete life-cycle of a privacy policy, the framework's enterprise side is organized according to a three-tier model suggested by Anton et al (2007):

Top tier which includes principles of privacy practices: An enterprise's high-level privacy promises are specified in privacy policies. This takes place by using formal and/or natural languages. Policies in this tier are intended for general Internet users without going into many specific areas. Dedicated privacy officers who are familiar with both the enterprise's business practice and relevant privacy law and regulations should specify these privacy issues.

Middle tier which includes security policies: In this layer, traditional security policies, access control and information flow are needed to enforce high- level privacy policies. Policies at this tier are indicated by

security officers who are familiar with high- level privacy policies and with the business processing needs of specific application domains.

Bottom tier which are enforcement made in the physical layer: Policy configurations in the underlying information are used to materialize access control and auditing policies. The privacy policies tends to be fine-grained, e.g., each individual user may allow different usages of her data and this the nature varies with every end user. Thus, fine- grained access control is needed in different sections as indicated in the following example , if relational databases are used, then it may require row- level or even cell level access control to support privacy constraints.

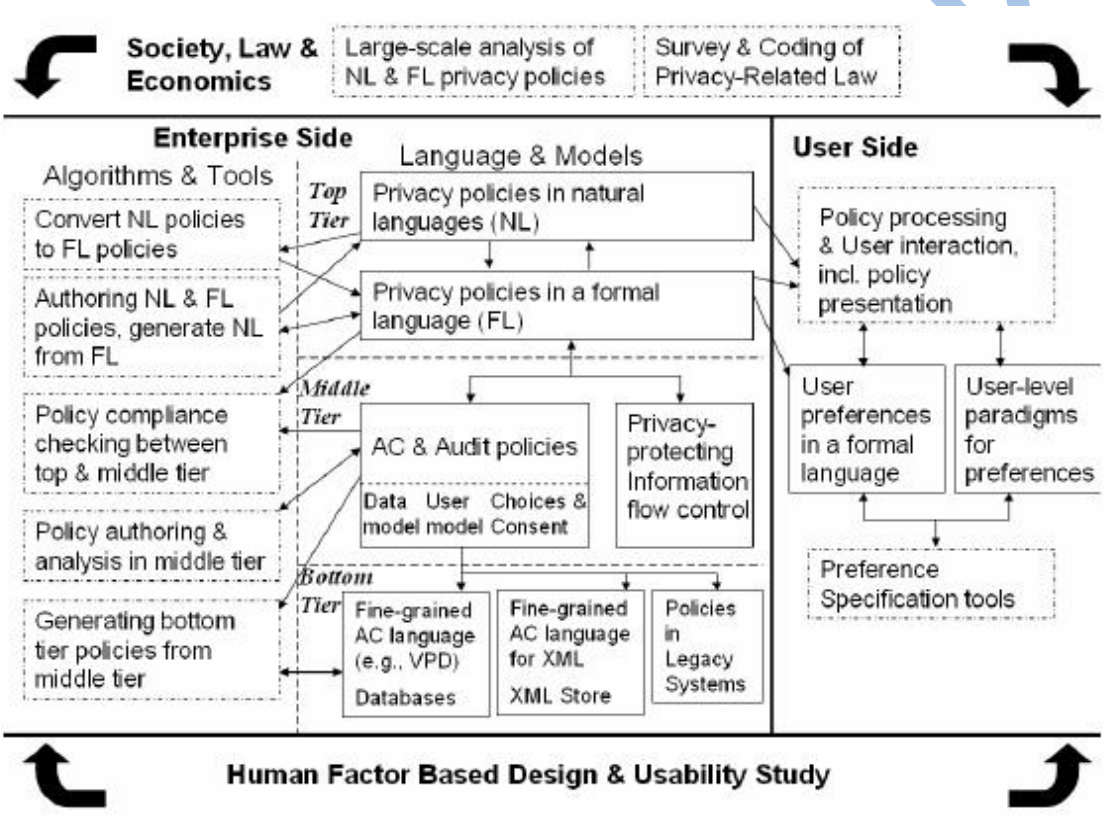


Figure 1: Architecture of an online privacy framework (adapted from Anton et al., 2007).

2.11 Privacy Policy Management for the End-User

Privacy policies need to be communicated to end-users. This enables them to make meaningful decisions about whether to provide personal data on the social networking websites. Having the privacy policy in machine readable form is only a first step towards enabling end-users to control their privacy. There are other objectives to be noted as indicated by Anton et al., 2007:

Development of a paradigm for specifying privacy preferences:
The paradigm should be close to user's privacy objectives without paying much attention to the data collection policies. Users often find it difficult to fully comprehend technical aspects of data collection and usage. Users' preferences should not be indicated in terms of sharing specific data items, but rather in achieving privacy objectives as indicated by Li et al., 2003. This paradigm should take into consideration users' limitations and it should be able to protect users from their own errors even if they are unaware of

them. The paradigm will account for privacy preferences that may vary with different types of websites which offer pseudonymity (Anton et al., 2007).

Methods and tools to present privacy policies to end-users in a uniform and accessible way:
Privacy policies are too difficult for the average user to understand; thus they are encoded in machine-readable form. This form is then automatically processed by tools and presenting users with pages of text that are laden with legal terms which can be understood by the majority of Internet users (Antón et al., 2004). Privacy policies should be presented in summary form for the users to make it user friendly. Once the most significant axes of users' privacy concerns and goals are determined there can be determination of how to have good structure, organization and presentation of this information to end-users (Karjoth et al., 2004).

2.12 Privacy Policy Engineering

Privacy Engineering is emerging spurred by the realization that IT systems must comply with privacy regulations (Kenny and Borking, 2002). It has always been difficulty to bridge the gap between legal language and computer language. This is more important when legal obligations have to be converted into requirements to be enforced by IT infrastructures. Invasions of privacy may not necessarily be due to malicious intents, but they were found to be inadvertently supported by technologies available on social networking websites (Adams, 1999).

Privacy Engineering is defined as a systematic effort to embed privacy relevant legal primitives into technical and governance design (Kenny and Borking, 2002). Privacy Engineering is thus the discipline which addresses the development of models, tools, processes, and methods needed to design systems that guarantee privacy protection according to privacy regulations. Privacy Engineering has been dealt with by several research communities, such as Privacy Requirements Engineering research carried on by Earp, (2001), Privacy Policy and User Preference Specification carried on by Cranor et al., (2002), Privacy-Aware Access Control carried on by Ashley et al., 2002 , Identity Management carried on by Barth et al., (2004) and Digital Rights Management research carried on by Feigenbaum, et al (2004), for example.
Hilty and Basin, (2005) have indicated that when IT systems are being built, and when programs that store and process personal data are developed, designers need to define system requirements to ensure that personal data are handled in accordance with applicable laws and regulations to the government. Privacy engineering must be fed in at each of the four stages which include initiation, planning, execution and closure. All the components of a generic project lifecycle; the requirements and level of detail must be in accordance with the objectives of each output of the project lifecycle stage to ensure timely information is made available to the project (Dumortier and Goemans, 2004).

The area of policy specification includes several contributions addressing privacy. They provide language constructs for representing privacy requirements. They do not give different methodological tools for supporting organizations in the design of their policies (Guarda and Zannone, 2009).

2.13 Requirements for Privacy-Preserving Social Network Applications

The rising use of Social networking applications on the Internet is a phenomenon that left lots of privacy advocates puzzled over the attitude of users. Users of social network sites provide personally identifiable data that was sought to be at the core of any privacy-enhancing technology and needed to be encrypted, hidden or anonymized (Kolbitsch and Maurer, 2006).

Recent privacy studies for online communities, however, reveal the fact that most users are unaware of specific risks of privacy-invasive activities. They have no idea to what degree their online profiles and the personally identifiable information is connected to it is visibility and exposed to others (Acquisti and

Gross, 2006). Users often say they are clearly concerned about their own privacy but then make decisions to reveal personally identifiable information data about themselves which are clearly contradictory to their concerns for privacy (Flinn and Lumsden, 2005). This dichotomy between privacy attitude and behaviour indicates that individuals are neither able to calculate the probabilities and amounts of risks nor are they able to
perceive the long-term risks and losses while acting in privacy sensitive situations (Acquisti and Grossklags, 2004).

Privacy is affected by the users' inability to control impressions and manage social contexts, for example with the early introductions of such features like "News Feed" and "Beacon" in the Facebook application (Boyd and Ellison, 2007). The experts often see a major concern for the information privacy of users in the combination of an immature technology on one side of the coin and providers on the other side who need to proof their business model by expanding ways to exploit the value of their users' personally identifiable information (Boyd and Ellison, 2007).

There are requirements set for ubiquitous computing systems where a comprehensive set of guidelines are required for designing privacy-aware ubiquitous systems (Langheinrich, 2001). Requirements for fostering a privacy-preserving social networking applications were transparent and open privacy handling practices and options for the user to easily report privacy invasions.

Other frameworks for analyzing requirements for privacy preserving social networks have been suggested by different authors (Preibusch et al., 2007). There is an indication of a need to concentrate on privacy in the sense of data protection. There should be restriction on data access and data processing and not so much transparency and control mechanisms that need to be developed (Preibusch et al., 2007).

Major concerns	Possible solutions	Requirements
Having no control over usage and proliferation of PII	Complete transparency over the usage of one's own PII	Privacy-by-design practices for web designers and developers
No transparency on what happens with PII	Privacy policies with an automated compliance assurance function	Transparent and open privacy handling Practices
Unauthorized third party use of PII	Proactive and automated communication techniques on risks	Options for the user to easily report privacy invasions

Table 2: Factors influencing the development of privacy-preserving social network applications (Weiss, 2009)

2.14 Privacy Threat Model for Social Network Portability

Potential threats to an individual's privacy exist whether that individual provide personally identifiable information (PII) to someone or not. In order for protection mechanisms to effectively work in social network applications at the foremost the application developers, need to understand the potential threats that exist to the end users. Those could not only be threats to the individual user and the related identifiable information but also to the business model of the social network application provider. The

variety of privacy threats in using social network sites have been pointed out in research papers and have especially addressed the inherent openness of social network applications (Weiss, 2007).

Berkovsky et al. (2007) has carried out research related to the setting of privacy preferences using semantic schemata . The context aware personalization is achieved by augmenting past experiences by the user with additional context-rich data. This might also be applied in deriving context-aware privacy preference rules. This could help in reducing the input the user has to give in each transaction (Berkovsky et al., 2007).

2.15 Privacy Homomorphisms for Social Networks

The availability of information on relationships which includes trust level, relationship type and others has increased with the advent of the semantic web and raise privacy concerns amongst users. Knowing who is trusted by a user and to what extent discloses a lot about that user's thoughts and feelings is very important. These privacy issues have motivated some social networks to enforce simple protection mechanisms. These mechanisms help users to decide whether their resources and relationships should be public or restricted to themselves or to those users with whom they have a direct relationship this information can be revealed (Stabb et al., 2004).

Carminati et al., (2009) described a more flexible access control scheme. Here a request or can be authorized to access a resource even if he has no direct relationship with the resource owner, but he is within a specified depth in the relationship graph. Access rules are used very clearly. This specifies the set of access conditions under which a certain resource can be accessed. Access conditions are a function of the relationship type, depth and trust level in relation to the user.

Wang et al., (2006) described a mechanism to protect personal information in social networks. Here the nodes in the network are anonymous and cannot be linked to specific user. However the data and the relationships are public, which might facilitate user re-identification by different programs.

An innovative privacy-preserving approach was described by Carminati et al., (2007) which leans on the access model in Carminati et al., (2006). This gives deep focus on relationship protection. A user can keep private that he has a relationship of a given type and trust level with another user. Relationship certificates are encrypted and are treated like a resource in their own right. The access to a certificate is granted using a distribution rule for that certificate. The distribution conditions to be satisfied by users wishing to access the certificate are specified very clearly. If a user satisfies the rule for a certificate, he receives the corresponding symmetric certificate key allowing him to decrypt the certificate thus enabling privacy.

2.16 Privacy Requirement Engineering

Requirement Engineering can be defined as the branch of software engineering concerned with the real-world goals for functions of, and constraints on software systems. It also deals with the relationship of these factors to their evolution over time and across software families and to precise specifications of software behavior" (Zave, 1997).

A Privacy Requirements Engineering methodology provides a language for representing privacy and data protection requirements in the organization domain. It also gives systematic methods for eliciting and analyzing these requirements (Gaurda and Zannone, 2009).

A requirements specification language consists of a set of primitive constructs that allow one to express and relate the privacy policy. From a methodological perspective, the framework should comprise the

activities to represent, capture and analyze privacy requirements along functional and security requirements (Gaurda and Zannone, 2009). Accordingly, besides the traditional activities provided by Requirements Engineering frameworks, the following activities have been identified:

- The structure of organizations is to be captured and their environmental setting identified by the different users defined by the privacy regulations;
- The purposes for which personal data are collected and link permissions to them are determined.
- The kind of data involved in the processing are identified.
- The obligations that shall be fulfilled by the user are to be Capture
- To link them to the permission that has generate them (Kavakli et al., 2003).

2.17 Privacy Solutions

Solutions to protecting privacy in online social networking sites is done in three different ways: technical solutions, social solutions and legal solutions. Social networking sites and other online business tools are working on various social solutions to the privacy problem (Barnes, 2007).
Sullivan (2005) had identified that the initial step in building protections for teenage bloggers starts with parents. A representative from Wired Safety.org remarked that parents need to be much more involved with their kids' computer use than they are right now (Sullivan, 2005). A growing gap is evolving between parent and teenage use of new technology. Parents need to spend time learning about these differences between the use of internet by them and their children. The Federal Bureau of Investigation and the National Center for Missing and Exploited Children offer parents advice for detecting whether their child is engaging in appropriate behavior as indicated by Downes, (2006).

Schools have also taken action to protect the safety of young individuals in social networking sites and they are trying to come up with policies on social networking sites. In many cases, schools are being forced to respond to real world problems which only came to their attention because this information was so publicly accessible on the Web (Jenkins and Boyd, 2006).

Teachers have written, sent e–mail to parents and called, about students placing too much personal information on the Internet. Some schools have banned social networking sites and asked students to take their information off the network (Kornblum, 2005). Other educational institutions have refused to let students register for social networking sites with a school official e–mail address. Schools are issuing warnings to students that college admissions officers and future employers are checking social networking sites to read what applicants have written online as indicated by Bahrampour and Aratani, (2006).

Colleges and universities have taken action as a result of incriminating photographs of students appearing on the Internet. Students are being warned that they will be reprimanded for pictures posted on the Internet that reveal misbehavior or misconduct (Wolverton, 2006).

Commercial social networking companies making efforts to react to the problems of a number of underage children online using fake profiles. MySpace has reported to be working with the National Center for Missing and Exploited Children and the Advertising Council to create the largest–ever online safety program using nationwide public service advertisements (Auchard, 2006). MySpace is posting a number of safety first ads to avoid privacy loss issues. Computer users can see these advertisements on MySpace in the form of banner ads which were also viewed on a host of News Corp. outlets, including Fox Interactive Media Web sites, the 28 Fox Networks Group broadcast networks and other Fox All Access Radio and the New York Post. (Barnes, 2007).

Social networking sites are exploring technological solutions to better protect their users in addition to social awareness. There have been indications of a few cases of online friendships that turned violent or even homicidal which have led to tremendous pressure on social–network sites to provide better security for their members. Facebook recently improved its privacy setting to give members tighter controls over who sees what (Duffy, 2006). MySpace had begun utilizing software to try and identify children under the age of 14 and thus avoid fake profiles. Massachusetts Attorney General Tom Reilly has asked MySpace to install an age and identity verification system which will equip Web pages with a 'Report Inappropriate Content' link. This will respond to all reports of inappropriate content within 24 hours and will raise the number of staff who reviews images and content (Mitrano, 2006).

Legal solutions to privacy issues involve both technological solutions and the human monitoring of social networking sites. On 10 May 2006 Representative Michael Fitzpatrick, a Pennsylvania Republican, introduced a new bill into Congress called the Deleting Online Predators Act (DOPA). This proposed law would extend current regulations that require all federally funded schools and libraries to deploy Internet filters in their online and offline computer networks. The law is so broadly defined that it would completely limit access to any commercial social networking site that allows users to create a profile and communicate with strangers (Jenkins and Boyd, 2006). This bill is primarily aimed at protecting teens that access social networking sites through libraries and schools. However this does not protect students using computers in their own homes. Protection of students is a parental responsibility. But the education of students and their parents to the growing privacy problem on online privacy issues and hazards of social networking sites will require an educational effort that involves schools, social networking organizations, and government agencies (Barnes, 2007).

2.18 Conclusion

The protection of privacy is the primary responsibility of the user and as the number of cyber crimes associated with the lethargic use of privacy settings are increasing day by day, a deeper probe into the issues relating to the protection of privacy assumes great significance in the present scenario. This study would also throw light on the specific concerns that require immediate attention and prompt intervention. Chapter three explains in detail the research methodology undertaken in the study. It explains the data collection, data review and data analysis procedures.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter aims to provide an overview of the design of research that the researcher plans to implement in order to assess the usage of privacy settings in the sites Orkut, Facebook and MySpace by the users. The study also sets out to investigate the extent of the privacy settings in these sites by the users and also makes an attempt to assess the threats on the settings of privacy of these sites. The details of the process of research adopted and the methods of collection of data and analysis of data employed by the researcher are also explained in the chapter. Also the sources of data collection are explained in the chapter.

Interpretivism and positivism

Positivism has its roots in the "ontological basis of realism, meaning that reality exists independent of the Observer" (Landry and Banville, 1992; Myers and Avison, 2002). This claim is criticized by the concept of Interpretivism and this concept claims that the idea of reality is a "social construct" in itself or in other words what we assume or take for granted as reality is constructed socially or obtained by means of social constructions (Walsham, 1995) Interpretivism be formulated as "looking at the features of positivism that it rejects and the alternatives it suggests. This definition is not conclusive as it would include other non-positivist approaches that are not interpretivist".

Research approach

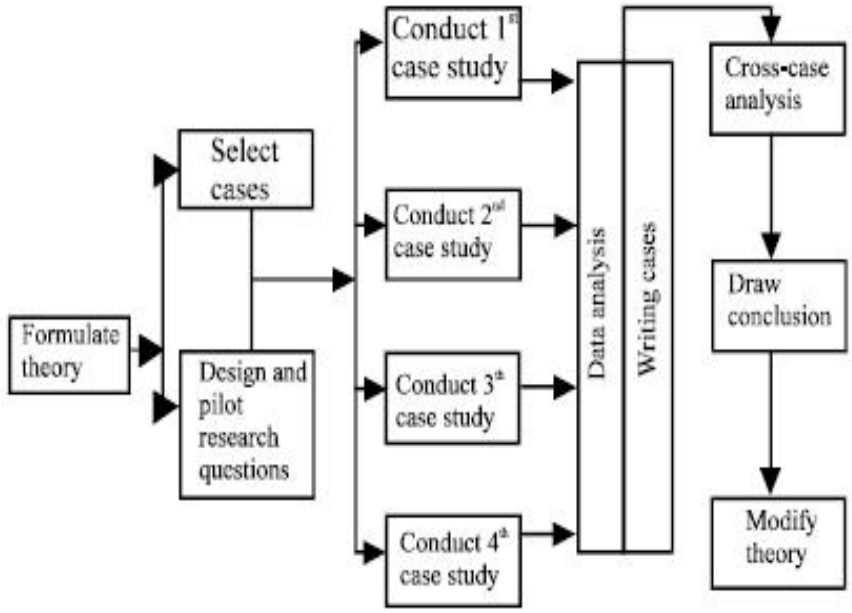
There are different research approaches used to study a particular research problem. The inductive approach would be used in case of a qualitative study and in this case a hypothesis should be developed with the help of the already available information by a thorough review of the literature (Bryman and Bell 2007). Hence this approach would not be suitable for the present study. This approach would not lead to the formation of any deeper insights or theories, but only empirical summaries could be formulated with this approach (Alvesson and Skoldberg 1994). The deductive approach is used for a quantitative study and in this case, the background knowledge is mostly a guess and thus this approach would not be useful for our study. In abductive approach the available empirical facts are used and for this study, this method is used as the conclusions obtained in this case would be helpful to confirm the findings of the previous research.

Research technique

Depending on the research problem, the method of undertaking the study varies. Morgan and Smircich (1980) are of the opinion that it is on the type of the social phenomenon being studied, the suitability of the method of research is derived. A case study approach was used to study the usage of privacy settings

Case studies

Yin (1989) suggests that a case is defined as "an event, an entity, an individual or even a unit of analysis". A case study is also defined as an "empirical inquiry that investigates a contemporary phenomenon within its real life context using multiple sources of evidence" (Anderson, 1993). The case is also concerned on the reasoning of why and how the events happen so that the contextual realities could be captured and the variations in what was initially planned and what actually occurred could be perceived. The case study does not deal with the organization as a whole. But the study pays attention to a specific issue, attribute or a unit of analysis. Hence in this study in order to gain insight into the privacy issues of social networking sites like Orkut, Facebook and MySpace case study method was chosen. The intricacies of these real life activities could be perceived by means of the evidence gained from multiple sources. According to the opinion of Patton (1987), case study is an appropriate method to gain deeper insight into the problem under investigation. Case studies are particularly important and useful in cases which are rich in information and help to gain an in-depth view.



Steps involved in a case study (Noor, 2008)

Data collection Methods

The method of data collection is a crucial aspect in any research because imprecision in the methods of data collections would adversely affect the results of the study and hence gives results that are invalid. There are many types of data the major types being Primary and secondary data.

Primary data

This type of data is obtained by the direct responses that are got from the people who are being interviewed. The personal experiences of these individuals, their feelings, attitudes are gathered by means of primary data. This type of data is obtained from the surveys, measurements made in the laboratory, observations in the field etc.

Secondary data

By reviewing the existing literature in the academics, the evidence obtained from the already available studies out there could be examined and a definite patterns and trends could be derived from such studies. The advantages of the secondary data are that it does not involve costs, saves times and efforts of the researcher and is unobtrusive. The problems associated with the collection of data could be avoided by the secondary data analysis and provides a basis for comparison. There are also some disadvantages associated with the secondary data collection. The credibility of the source that has published the data at hand is not in the control of the researcher and the researcher would not be able to capture the small nuances of the research objectives of this study. This is because the already available studies would have been designed to capture data that pertain to some other objectives. The next disadvantage of this method of data collection is that the data may be outdated. The authenticity of the techniques and measures used for the collection of data is not known to the researcher. The collection of secondary data involves many sources like Magazines, journals, published reports, books, research articles, films, TV, newspapers, Radio and websites.

Handling of the secondary data

The credibility of the data could be greatly increased if the data is obtained from multiple sources and this is a conventional and trade mark approach used in the collection of secondary data. Many potential sources could be used in the collection of secondary data. One of the advantages of this method is that all

the data that is obtained can be integrated or viewed in a collective and overall perception. Hence a holistic view on the issue of the use of privacy settings in Orkut, Facebook and MySpace and the potential threats and the extent of use could also be analyzed. There would be an aggregation of the data from the sources and every set of data would be considered as the piece of the puzzle and then a final understanding on the issue of privacy settings in the above mentioned social networking sites would be arrived. This would enhance the strength of the study and every strand of the data could be conceived better (Yin, 2003).

The fit between the research question and the data chosen for analysis

The process by which the secondary data is located is not straightforward at all circumstances. Hence there should be an achievement of a proper fit between the research problem at hand and also the data that is chosen to analyze the same. As it is most often an iterative process where a research problem is proposed, there should be a consideration of the potential data sets and a subsequent refining and revision of the research question with reference to the data that is available. There can be further revisions based on the other available data sources and a then the research question can be finalized. The most archetypal manner in which secondary data is used for research is to start with a question and then search the data sets that would help in the analysis of the question. Another method would be to start from looking at the secondary data sets that is available and then proceed with the formulation of a question that could be analyzed by means of the chosen data. Though the former method agrees with the conventional way of doing a research, the latter is useful in case of class room instructions. However both the methods would produce quality results. The following sequence could be followed in the conduction of research using secondary data (Boslaugh)

- Definition of the question
- Specification of the population and the variables
- Specification of the data to be collected (Boslaugh).

Modes of data collection

In a case study approach, the data collection involves the choosing of some of the examples and illustrations on the research problem in hand and then moving on to eventual intense investigation of the attributes of these cases or examples. Hence by the analysis of a less number of big cases, and also by comparing and contrasting the cases, the characteristics of the phenomenon can be perceived and the circumstances where they vary could also be arrived. Hence the concept of privacy issues in the social networking sites could be researched well with the help of the case study approach.

A desk based approach would be used for the secondary data collection. As the value and authenticity of research is dependent on the methods of data collection, as observed by Jackson (1994), this method is an unobtrusive method as it handles the literature that has been published already. But there should be an critical evaluation of the literature that has been collected should be done in terms of its reliability and verifiability by making comparisons with other sources that are authentic (Creswell 2003). Thus, considering the background of the present study, data would be obtained from previously published reports, case studies, documents, academic journals etc.

Analysis of the data

After the cases are being presented, the researcher would try to give an overall picture of the whole concept taken for the analysis to present the situation on the use of privacy settings in the networking sites. Based on the facts derived from the cases of the sites Orkut, Facebook and MySpace, the researcher would present his conclusions. Also the study cases would be compared and contrasted in the light of the facts that are collected for the present study. In the section on summary and conclusions, the implications of the interpretations and findings would be provided on the basis of the existing facts rather than

providing new facts. Hence the process of sifting and sorting and the interpretation of the available information is the essence of the case study.

CHAPTER 4: CASE STUDY ANALYSIS

This chapter deals with the collective analysis of the usage of the privacy settings of the sites Face book, MySpace and Orkut by the users and investigates the nature of potential threats on various aspects of privacy of the users. It also makes an attempt to identify the extent of users who actually use or give importance to the limiting privacy preferences and the factors driving the users to provide generous personal information and limited usage of privacy preferences. Hence the trends existing in the above mentioned social networking sites are comparatively assessed and the conclusions and recommendations would be provided.

CASE 1: Face book

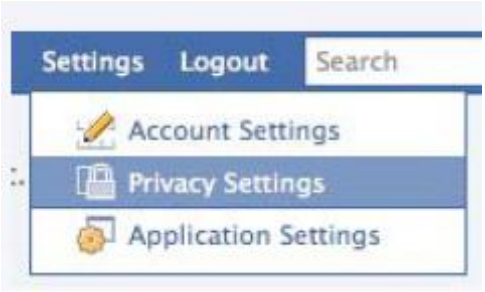
Privacy settings in Face book:

The Face book is an online networking site provided for the high school as well as college communities. It is highly successful among the college goers. But there is a huge amount of personal information that is available on the site and there is also a personal identification of the information for the young people. Hence being a mass phenomenon, the Facebook provides a window for a keen observation of the attitudes and patterns followed by the young individuals with reference to the privacy settings.

Level of access

- There are five levels of access provided by the Facebook
  - Everyone
  - All people in the network and also friends
  - Friends of friends
  - Exclusively friends
- The customized settings could be used so that some people can be excluded. Settings like “only friends” would help to keep in touch with friends and also stay protected from unknown people. The setting “Photos Tagged of You” allows for more tighter controls on the privacy issues so that only certain friends can see the photos tagged
- The sensitive photos could be kept in separate albums and made available only for family members
- To stay away from the random searchers of the web, the facility of”public search listing can be turned off
- The options like newsfeed and wall can be turned off if the actions done on the Facebook need to be kept confidential. This can be used for rejecting the unwanted friends, to hide the news read etc. this is also useful in staying away from advertising (CIPR, 2009)

  Figure1: Setting page



Source: (CIPR, 2009)

- The applications present in the Facebook have their own settings and they are to respect the privacy of the users. Though some of the applications appear simple, there is a risk of the creators stealing the information and selling them to the markets.

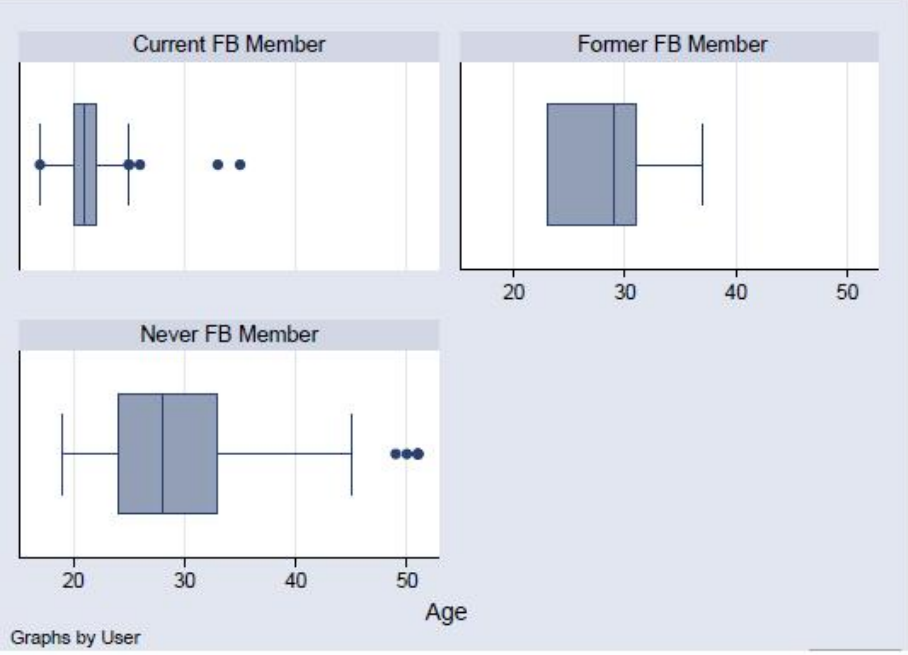
Trends and threats in the use of privacy settings

Acquisti and Gross (2006) conducted a comprehensive survey on a large sample of 7000 participant profiles by means of an electronic bill board. The profiles were accessed by means of PERL scripts. The data mining was done before the administration of the survey. Rigorous statistical tools and software were used for the data analysis.

Age and gender distribution

Majority of the members (64.29%) belonged to the undergraduate category and over 25 % were graduate students and 9.1 % belonged to the category of staff. As expected, age showed a strong relationship with the membership but the age distribution was broad. (sd 8.840476 vs. sd 2.08514).

Figure 2



.. Box-plots of age distribution for different membership status

Source: (Acquisti and Gross, 2006)

Figure 3

User	Are you... Undergrad	Graduate	Faculty	Staff	Total
Current FB Member	176	30	0	3	209
	84.21	14.35	0.00	1.44	100.00
	93.12	40.54	0.00	11.11	71.09
Former FB Member	2	4	0	1	7
	28.57	57.14	0.00	14.29	100.00
	1.06	5.41	0.00	3.70	2.38
Never FB Member	11	40	4	23	78
	14.10	51.28	5.13	29.49	100.00
	5.82	54.05	100.00	85.19	26.53
Total	189	74	4	27	294
	64.29	25.17	1.36	9.18	100.00
	100.00	100.00	100.00	100.00	100.00

. Distribution of survey participant status for FB members, non-members and
who never had a FB account.

Source: (Acquisti and Gross, 2006)

Age, the status of the students and the concerns on privacy

The hypothesis that was obvious is that there is an inverse correlation with individual concerns for privacy and the possibility of joining the face book. The members who were not in Facebook had higher concerns for privacy than that of the members. The levels of distribution of concerns of privacy threats for both the members as well as the non-members are provided in figure 4. There are the older and the senior members in college who do not opt for face book due to the privacy concerns. The non-members also have higher concerns on privacy than that of the members. But the youngsters show a shocking trend that apart from being not concerned about the issues of privacy, the youngsters want their privacy to be explored by the others.

Figure 4

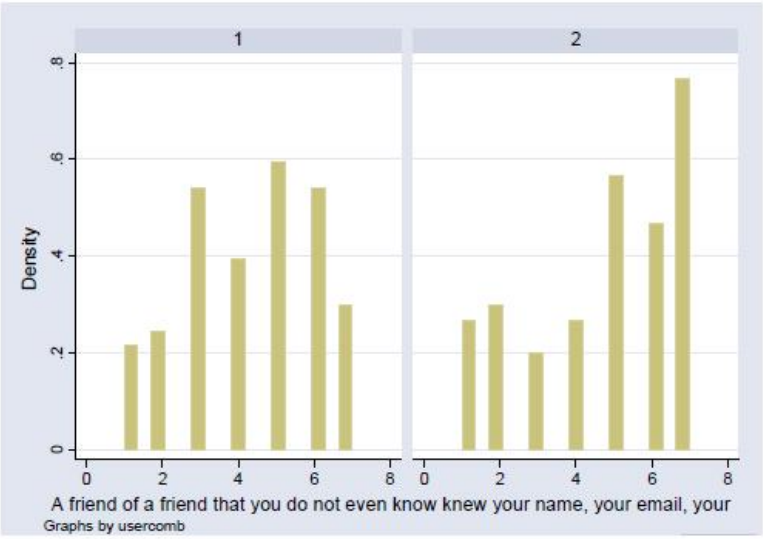


Figure 5

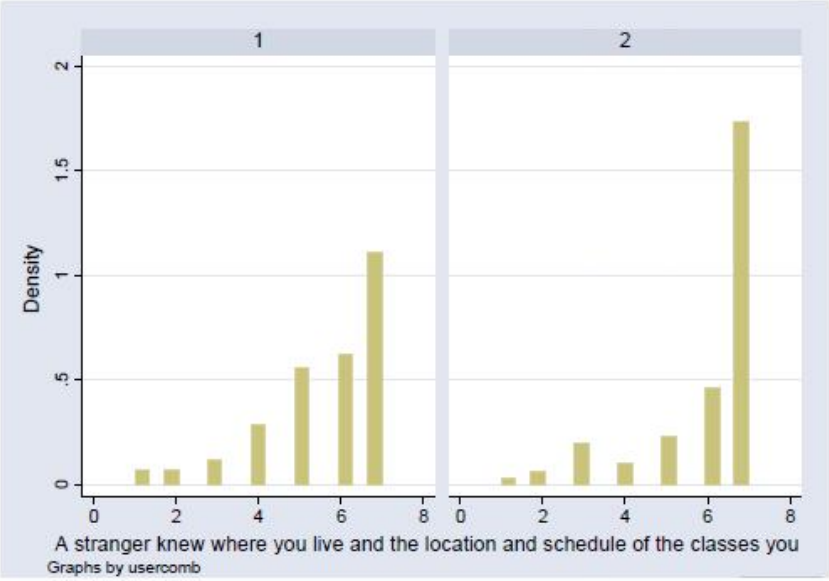


Figure 4 and 5: The privacy attitude distribution between the members(1) and the non-members(2) who dint have facebook profiles or were members but deactivated now.
Source: (Acquisti and Gross, 2006)

Figure 6

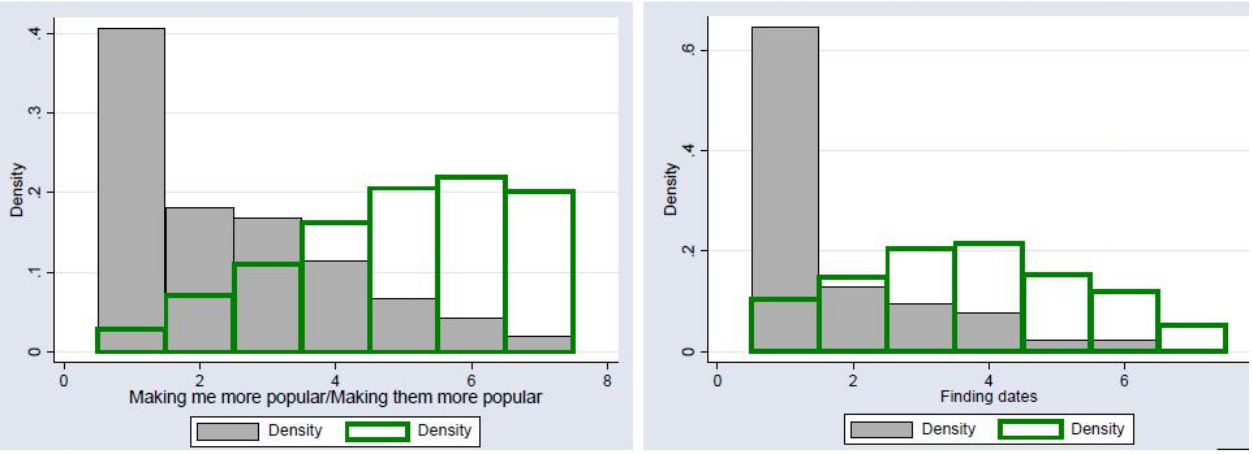
usercomb	Threats to your personal privacy 1	2	3	4	5	6	7
Current member	6	15	20	28	46	52	42
	2.87	7.18	9.57	13.40	22.01	24.88	20.10
	100.00	71.43	80.00	68.29	71.88	76.47	60.87
Current non member	0	6	5	13	18	16	27
	0.00	7.06	5.88	15.29	21.18	18.82	31.76
	0.00	28.57	20.00	31.71	28.13	23.53	39.13
Total	6	21	25	41	64	68	69
	2.04	7.14	8.50	13.95	21.77	23.13	23.47
	100.00	100.00	100.00	100.00	100.00	100.00	100.00

The distribution of the survey participants who had concerns about the threats for their personal privacy between the members and non members Source: (Acquisti and Gross, 2006)

Reported usage of Facebook and the information provided

To gain an understanding of the factors that motivate the individuals concerned on privacy the primary objective of the participant to use the facebook was sought out. The intention of dating stood out as one of the primary motives. Other motives like, getting to know their class mates, being able to stay in contact were also in the list. But at present, "Showing information about themselves/advertising themselves," "Making them more popular," and "Finding dates" are identified as the most sought out actions.

Figure 7.

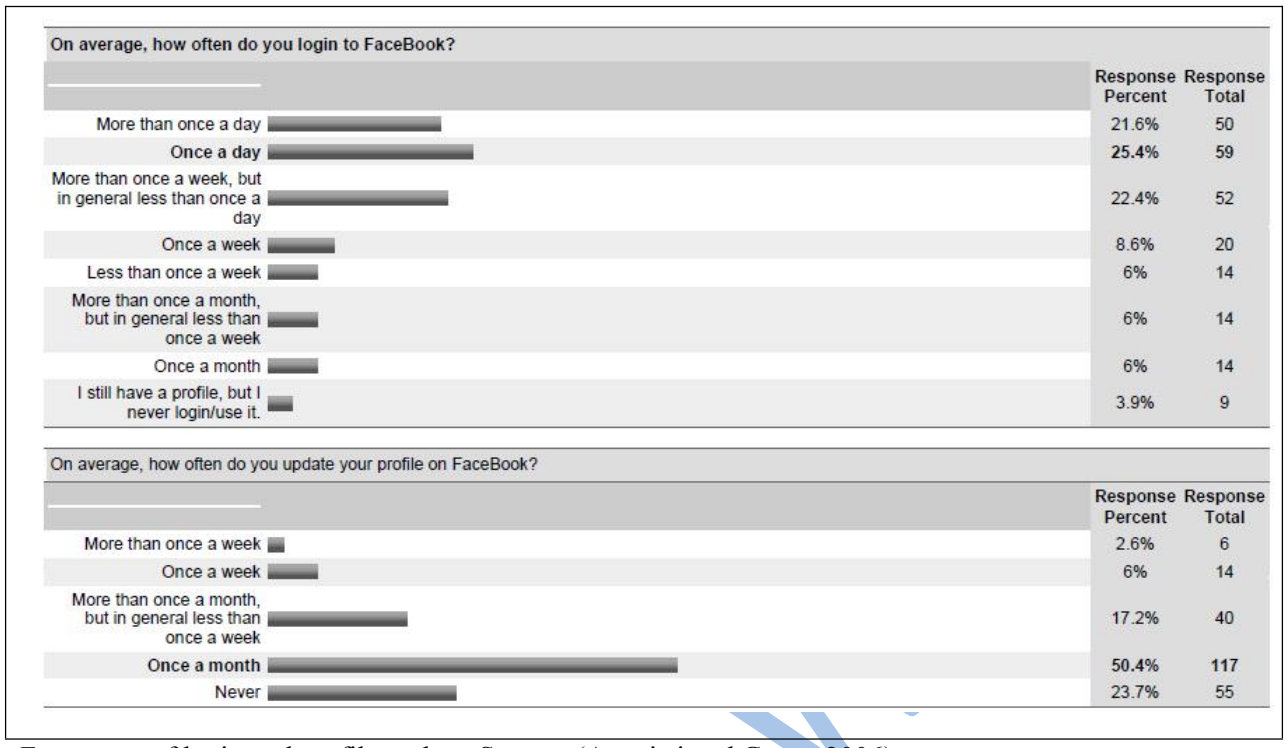


"Do as I preach, not as I do - How useful is FB for you" (indicated in grey boxes) vs. Other member use FB, how often do you believe that are illustrated in boxes which are transparent?
Source: (Acquisti and Gross, 2006)
Figure 8: Information provided by the facebook users

What personal information do you provide on the FaceBook and how accurate is that information?

	I don't provide this information	I provide this information and it is complete and accurate	I provide this information but it is intentionally not complete or not accurate
Birthday	12% (29)	84% (195)	3% (8)
Cell phone number	59% (138)	39% (90)	2% (4)
Home phone number	89% (207)	10% (24)	0% (1)
Personal address	73% (169)	24% (55)	3% (8)
Schedule of classes	54% (126)	42% (97)	4% (9)
AIM	24% (56)	75% (173)	1% (3)
Political views	42% (97)	53% (122)	6% (13)
Sexual orientation	38% (88)	59% (138)	3% (6)
Partner's name	71% (164)	28% (65)	1% (3)

Source: (Acquisti and Gross, 2006)
Among the people who participated in the survey, the members of Facebook provided more than that of the nonmembers but the difference between the members and nonmembers did not show any statistical significance. But the members of Facebook provided more information on their personal and contact addresses and political views than that of the nonmembers.
Figure 9



On average, how often do you login to FaceBook?

	Response Percent	Response Total
More than once a day	21.6%	50
Once a day	25.4%	59
More than once a week, but in general less than once a day	22.4%	52
Once a week	8.6%	20
Less than once a week	6%	14
More than once a month, but in general less than once a week	6%	14
Once a month	6%	14
I still have a profile, but I never login/use it.	3.9%	9

On average, how often do you update your profile on FaceBook?

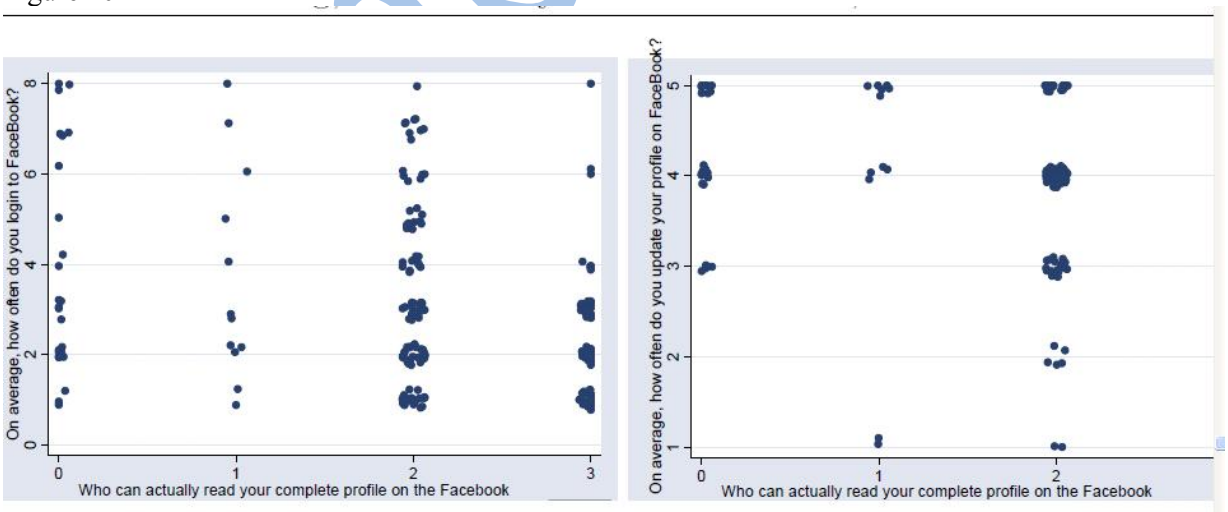
	Response Percent	Response Total
More than once a week	2.6%	6
Once a week	6%	14
More than once a month, but in general less than once a week	17.2%	40
Once a month	50.4%	117
Never	23.7%	55

Frequency of login and profile update. Source: (Acquisti and Gross, 2006)

Information available on attitudes and behavior

The finding to be highlighted here is that about 16 percent of the participants had high concerns on revealing information on their attitudes and behaviors in personal life like the name of the partner, political and sexual orientation. As the concerns for privacy increase there is less number providing such information. But still observing that 48 percent of the concerned people reveal their sexual orientation and 21 percent show the name of their partners and 47 percent are willing to expose their political orientation, the extent of their privacy concerns can be assessed.

Figure 10



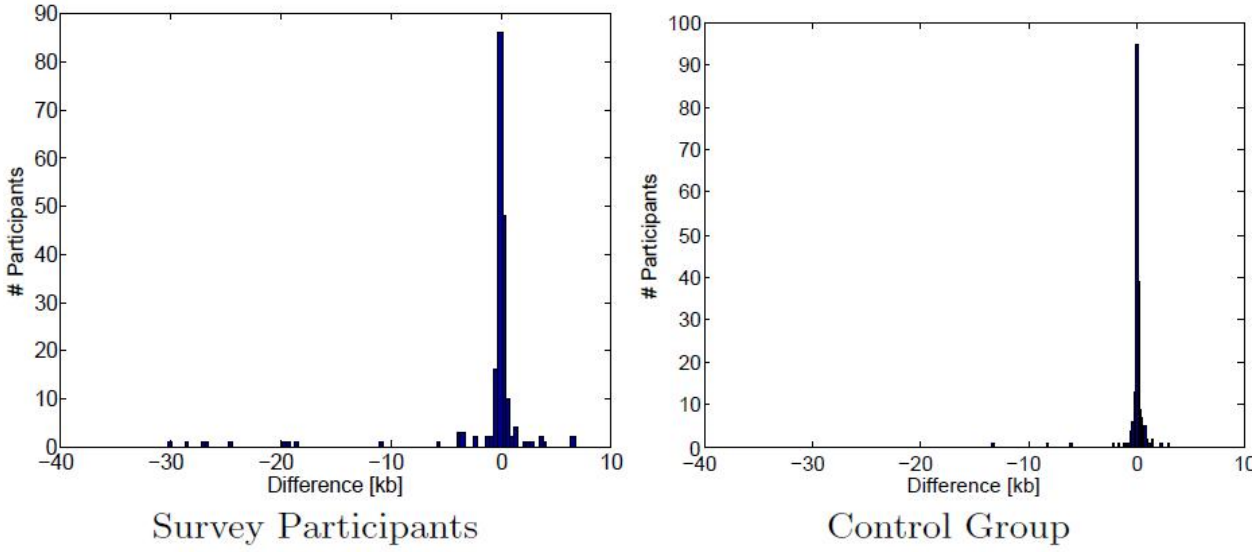
"Self-awareness of ability to control who can see one's profile, by frequency of login (left) and frequency of update (right). On the x-axis, the value 0 means "Do not know" if there is any way to control; 1 means "No control"; 2 means "Some control" and 3 means "Complete control." On the y-axis, higher values mean less frequent login or update".

Source: (Acquisti and Gross, 2006)

Impact of the survey

The profiles of the users were downloaded before and after the survey and the information was compared. There were only a small number of members who changed their behavior after the survey. This kind of change is possible to happen in the participants even if such a survey was not done. There are high concerns for privacy, but only a fraction of the participant had high concerns enough to deactivate their profiles just for the implications on their privacy.

Figure 11



"Changes in profile sizes for survey participants and a control group. The sizes for the survey participants changed significantly more".

Source: (Acquisti and Gross, 2006)

Factors that drive the provision of generous personal information

Routinization

A study conducted by Debatin et al (2009) showed that the concept social networking with special reference to Facebook has become an integral part of the life of the students and is ingrained deeply as a daily routine which exemplifies the nature of pervasive technology. The convenience and the ability to stay connected socially with a lot of ease is prompts the students and youngsters to provide information generously.

Ritualization

There are instances of ritualisation in Facebook that revealed that Facebook has grown tremendously and occupies a very important position in the daily lives of the college students. The Facebook had important functions in the social and emotional context as it provides ways of ritualisation and opportunities for consuming its content and also provides new definitions on friendship and safety net that enables one to fall out of touch with their contacts.

Rumor mill

The gossips as well as rumors are a central aspect of Facebook and they are blown in large proportions by the manner in which news is fed into the system. On the other hand it serves as the social glue that makes

the student society interesting and lively. One of the key determinants that makes the students use facebook is gossip and rumor even if the students are not ready to admit the same.

Invasion of privacy

The invasion of one's privacy is not just a possibility in hypothetical terms, but it is a part and parcel of facebook. The unwanted intrusions happening in the personal lives of the users lead to lack of control, anger, fear etc. there are some strategies used by the members to deal with the same. There are options in the Facebook to exert more control on the settings of privacy. Another strategy adopted psychologically is that the intrusions into privacy are interpreted in an unthreatening context. The users are reassured that these incidents are pranks by the creeps and immature individuals. One of the participants stated that ''it's just Facebook. . . There was a time before Facebook. You can do without it. It's ok.''

CASE 2: My Space

Privacy settings in MySpace

The social networking sites have become a common and increasingly popular phenomenon in the recent years and among the sites myspace.com has become an integral part of the adolescent culture in many countries.

Site traffic rank:

Bonneau and Preibusch, (2009) have done a comprehensive analysis of the privacy practices and policies of over 45 social networking sites. In their revisiting of the privacy policies of the sites among which MySpace was also included, the following trends appeared. MySpace is a popular networking site in nations like Australia, US, Ireland, UK etc and its main competitor is Facebook in US as well as Canada. The user base rounded off in millions is provided in the table.

Figure 18

Site	Traffic Rank	Users (M)	Country	Category
Windows Live Spaces	4	120	USA	General-purpose
Facebook	5	175	USA	General-purpose
MySpace	7	250	USA	General-purpose

The user count of MySpace highlighted in Millions rounded

Source: (Bonneau and Preibusch, 2009)

The terms of use and privacy policy

In the study conducted, which surveyed the users exposed to the terms of use as well as the privacy policies because signing up is significantly an agreement that is governed legally by the privacy policy documents. In the case of MySpace, a clear statement for the using of privacy policies is given. This feature is almost absent in many other networking sites.There is the provision of the disclaimer near the button for submission which is the link to access the terms of use. The privacy policy also would be given as a link near the sign up button.

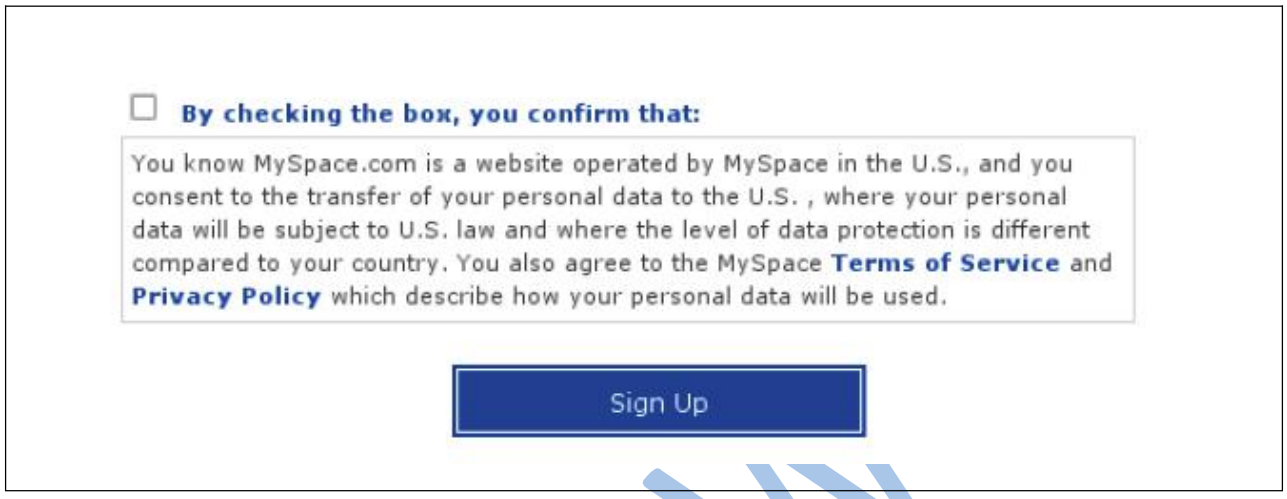
Privacy Policy Review

The users were not forced to acknowledge the privacy policy. There are only very few sites that actually encouraged the users to read the policies. Providing a condensed version of the privacy policy of the site is a good feature followed in MySpace. Myspace showed the paragraphs that were extracted from the detailed privacy policies.

Provision of a preset combination of buttons that could selectively enable the selection of the privacy policies with one click is a nice feature found only in few sites. These are called as "high privacy

options". In case of Myspace also there are a pre-set combination of such provisions but this option only controls which other user of the site can message the user

Figure 19



Terms of use and acknowledgement of privacy policy
Source: (Bonneau and Preibusch, 2009)

Prevention of Phishing

In the websites surveyed, only MySpace with the exception of BlackPlanet has incorporated an option on phishing and thereby warning the users for entering the passwords at their site. There is a danger of the Phishers to duplicate in a fraudulent manner and this should be made known to the users.

Privacy score:

Also reading of the issues on privacy can be moderated in a proactive manner in a way that trust is established with the users and without any mention of the issue of privacy. The professionalism exhibited by the site and the quality and ease of use of the site is more useful in gaining the trust and confidence of the users (Acquisti and Gross, 2006). The role of the contents of the privacy policy and the indications on the issues of privacy come next in winning the trust of the users. This might be the reason for the differences existing between Facebook and MySpace. Face book has a very appealing screen design and hence it is trusted most by the users more than that of MySpace. Hence the privacy score of 0.48 is slightly lesser than that obtained by Face book. The excess confidence on Facebook is due to the clarity in the layout of the site than that of the privacy policies of the site**.**

Figure 20
Privacy score of Myspsce, Source: (Bonneau and Preibusch, 2009)

Site	1 – Data Collection Score	Privacy Control Score	Privacy Policy Score	Privacy Score	Function-ality Score
Badoo	.33	.07	.33	.23	.40
Bahu	.24	.22	.43	.35	.50
Bebo	.62	.44	.57	.70	.60
BlackPlanet	.29	.26	.54	.46	.50
BuzzNet	.29	.22	.43	.37	.60
Classmates.com	.33	.22	.63	.51	.30
CouchSurfing	.14	.30	.26	.26	.30
CyWorld	.14	.47	.50	.51	.50
Eons	.24	.36	.48	.46	.50
Experience Project	.81	.19	.30	.44	.30
Facebook	.10	.61	.41	.53	.90
Flixster	.33	.26	.48	.44	.40
Friendster	.29	.30	.48	.44	.60
Gaia Online	.81	.44	.46	.69	.30
Habbo	.81	.37	.48	.66	.50
hi5	.43	.32	.43	.48	.70
Hyves	.29	.41	.41	.47	.70
Imbee	.05	.37	.57	.46	.30
Imeem	.71	.15	.57	.55	.50
Impulse	.43	.34	.13	.30	.30
Kaioo	.57	.15	.46	.43	.20
Last.fm	1.00	.22	.48	.64	.40
LinkedIn	.52	.39	.67	.70	.50
LiveJournal	.48	.60	.37	.62	.50
meinVZ	.38	.41	.65	.65	.40
MocoSpace	.52	.30	.43	.49	.30
Multiply	.05	.36	.39	.34	.40
MyLife	.29	.07	.43	.28	.30
MySpace	.29	.41	.43	.48	.80

Trends and Threats to privacy in MySpace:
Tufekci (2008) has done a study on a sample of 704 college students to assess the privacy concerns in leading social networking sites.

Threat of sexual exploitation and negative attention
In case of MySpace there is no division of networks and groups as is the case with Facebook. It is a general social network site which can be used by all the users. It is a site that has attracted a lot of negative attention in the media because it had some users who prompted the fears of sex predators who connect to the youngsters and then exploit them. There is no walled area in MySpace like in the case of Facebook. However in myspace there is an option for restricting the site to the friends only.

Levels of disclosure

The study also aimed to assess if the privacy concerns of people inclflueced their decisions to use the social networking sites. The levels of disclosures in the site was also analysed and the differenct expectations of the audience were also brought out. The disclosures are in different ranges starting from disclosing a favorite book to the disclosure of sensitive aspects like sexual orientation. The variables that were taken for the study were mostly associated with the use of the social networking sites by the students. More than half of the students had a profile on Myspace.

Figure 21

	As Percentage of SNS Users
Has profile on	
Facebook (FB)	91.2
Myspace (MS)	55.5
Choice of SNS (% of SNS users)	
Only FB	40.7
Only MS	4.8
Both FB and MS	50.5
Another SNS (neither FB nor MS)	3.3

Note: $N = 601$.

Percentage of people using Myspace Source: (Tufekci, 2008)

On further probing if the real names of the students were used on the websites, an overwhelming proportionon of 62.8 percent of the people were operating under their real names. There were also questions on the common settings like the visblity of the profiles to everyone or others and 59 percent of the Myspace users made their profiles visible to every one

Figure 22

	Percentage Using Real Name	Percentage With Profile Visible to Everyone
Facebook	94.9	42.2
Myspace	62.7	59.0

Source: (Tufekci, 2008)

Tufekci,(2008) states that "To probe students' choice to use a real name versus a made-up name, we ran a logistic regression with two predictor variables: the students' general level of concern about online privacy and specific audience concerns ("How concerned are you that people you do not want to see your profile will see it?"). We controlled for gender, age, and race (White or not). We report the results in two tables. On both sites, people were about 40% less likely to make their profile visible to everyone for each level of increase in their concern over the profile being found by unwanted others. Also, men were significantly more likely than women to make their profile visible to everyone on Myspace".

Figure 23

	Profile Visible to Everyone on Facebook	Profile Visible to Everyone on Myspace
General privacy	0.962	0.940
Unwanted profile gaze	0.640***	0.614**
Male	1.641†	2.504***
White	0.858	1.261
Age	1.210*	1.060
Baseline odds (constant)	0.076	1.790
N	287	187

†.05 < *p* < .10; *p < .05; **p < .01; ***p < .001.

Logistic Regression Results: Odds of Having Made Profile Visible to Everyone
Source: (Tufekci, 2008)

Bonneau and Preibusch,(2009) further state that "To assess the significance of perceived likelihood of specific future audiences on disclosure, we ran 12 logistic regressions with dependent variables of disclosure levels and profile visibility on Myspace. Perceived likelihoods of different future audiences (employer, romantic partner, government, and corporations) were predictor variables.Gender, race, and age remained our standard controls. The results are two other logistic regressions, measuring the association between using real name on Myspace and the perceived likelihood of these future audiences".

Figure 24

	Uses Real Name on Facebook	Uses Real Name on Myspace
Male	1.521	1.175
White	0.536	1.258
Age	0.918	0.953
Employer	1.681	1.002
Romantic partner	0.961	0.861
Government	1.421	1.149
Corporation	12.522	1.035
Baseline odds (constant)	1.521	2.683
N	173	104

"Logistic Regression (*e*B) of Using a Real Name on Myspace Modeled With Gender, Race, Age, and Perceived Likelihood of Employers, Romantic Partners, Government, and Corporations Viewing the Profile" Source: (Tufekci, 2008)

CASE 3: ORKUT

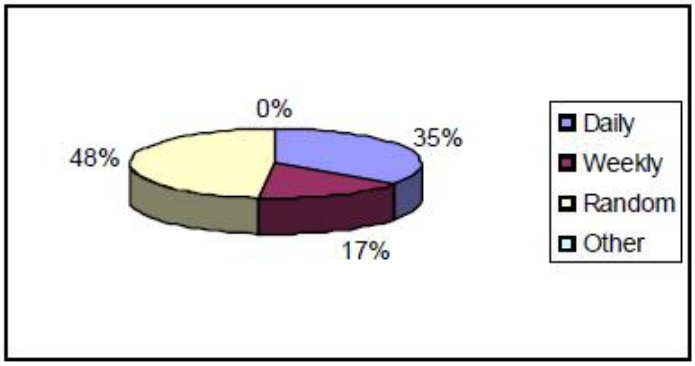
Privacy and safety settings in Orkut

- The settings of privacy are in such a way that the profiles of the users will not appear in the search results inside orkut even if they are searched with emil addresses,
- The contents in orkut are set to be shared by friends and friends of friends. The setting that is default is friends only
- The users would not be able to make public the information in the profile field
- The function of safety filter prevents the teenagers from the use of mature content and if one user is marked as unsafe by the team, then all friend links would be made unavailable automatically
- The email address of a person should be known by a user in order to send a friend request to the users. If a user is marked unsafe, friend requests cannot be sent by him to someone even if his/her email address is known. The unsafe users would not be shown as friend suggestions in any one's profile.
- The advertisement classified as "family ads" are shown by orkut.
- Orkut also provides some web links that have information on the safety issues
    - KeepSafe
    - Cyberbully411
    - ConnectSafely.org
    - National Crime Prevention Council (USA)
    - The Internet Keep Safe Coalition (googlesupport.com)

Trends and threats in the use of privacy settings

A plethora of the social networking sites exist in India, and among them Orkut is the most widely used social networking site that includes many features like profile creation, chatting, formation of communities and groups, facilities to share videos and music. In a survey conducted by Ashwini and Smitha (2009), on a sample of 478 participants in India, Orkut emerged as the leading social networking site. As per the Comscore report (2009), in December 2008, orkut is the most visited social networking site with more than 12 million visitors. There is an increase by 81 percent of the orkut users, and the audience for orkut is three times the audience base for Facebook, in India. Saad (2006) is of the opinion that "Orkut has become famous primarily as a relationship site, but it is undeniable that such goal has often been distorted. With the practice of preserving user anonymity, the Orkut site provides a fertile space for the practice of crimes, putting in risk the right of third parties, who for sure will have to be compensated." Also, Pasha (2007), states that "Orkut.com has been my breadwinner. Eighty per cent of Internet-savvy youth in the age group of 16 to 30 are members of Orkut.com. On an average, they access the site every alternative day. If I block access to the site, nobody will turn up at my Internet centres and it will affect my bread and butter. Blocking a site is not at all possible and reasonable (from the moral point of view). If someone is upset with the contents, they can take up their grievances directly with the (people who operate the) site."

Figure 12



Frequency of access of the site by the users

Source (Ashwini and Smitha, 2009)

Figure 13

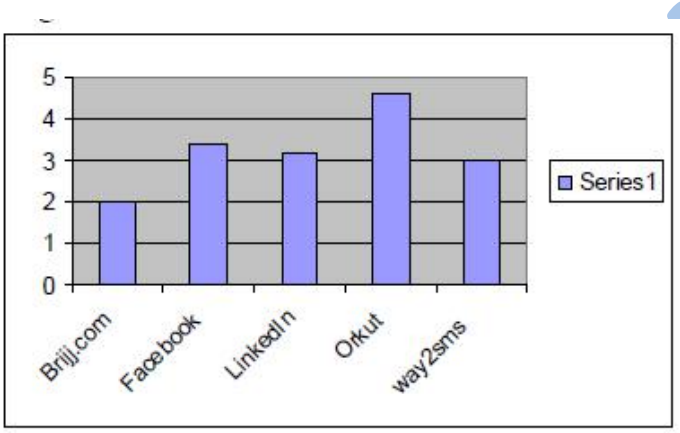
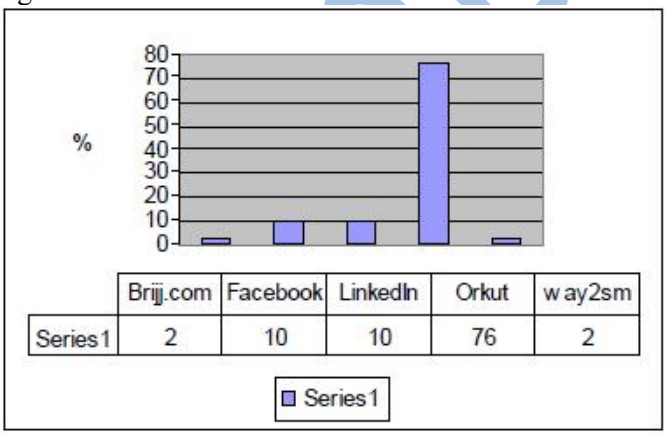
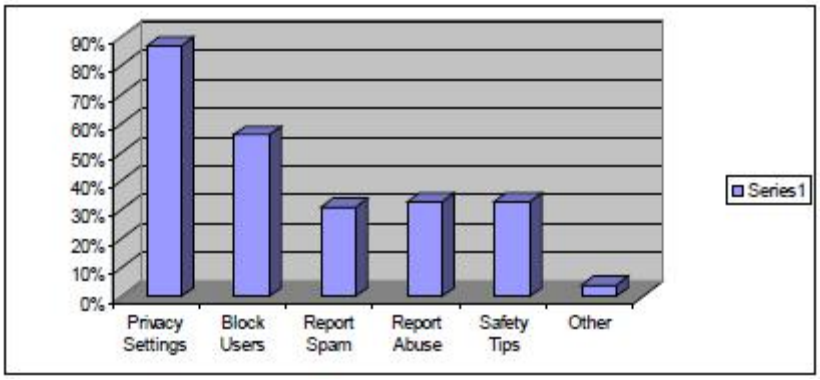


Figure 14



Cosmetic aspects (figure 4) Social networking site preferences of the respondents (Figure 5)
Figure15



Concerns on security of the users

The simple survey done by Ashwini and Smitha (2009) showed that among the security features, the users gave more importance for the in-built security features and least concern for safety tips.

Threats and privacy failures

A report by the privacy international (2007) based on a study done for a period of six months into the practices of privacy on the web based companies showed that Google is in the last place with numerous seatbacks and conflicts in its approach to privacy. Though other companies also found a place, Google emerged as the worst. These failures also apply to Orkut owned by the Goolge. Google was ranked the worst according to a full range of search on the social networking sites, email and e-commerce. The personal information of the users is accessible to Google which included the address, hobbies, employment, phone numbers etc which are contained in the profiles of the users. Google indeed, maintains all the above mentioned information, even after the profile has been deleted by the orkut user.

Ambiguous privacy settings

Though there are many complexities in the settings of privacy in orkut, there are also many confusing words and ambiguous settings that compounds the privacy issues in orkut. As pointed out in the illustration figure 16 shows a check box “enable photo tagging” that is associated with the others’ ability to tag the photos by the others and restricts the ability for viewing a set of user’s photos that are tagged, even if the photos have been tagged by the user. There is also one “confusing dangling modifier in the first sentence. Whether the word “with their friends “signifies the person being tagged or the person who is tagging the photo is also not clear. Also, there is an option to choose between “any users” and “only members” in case of the visibility of the profile. There is an assumption that “any users” includes members who are not registered and after the selection of “only members”, the setting became “any members”. There is also no written help in the managing of such privacy settings, confusing labeling and terminology (Bonneau and Preibusch, 2009).

Figure 16

"Coarse-grained privacy setting with potentially confusing wording and nonstandard input controls ("2yes")(Orkut)"
Source **:** (Bonneau and Preibusch, 2009).

Changing the Privacy Settings

In a comparative study done by Fox and Naidu (2009), among various social networking sites, orkut was found to the least user friendly site with reference to managing the privacy settings. Only 40 percent were successful in managing which was very low compared to that of the other sites. The difficulty was because the users had to make use of a drop down menu as against the use of a radio button in case of other sites that allowed privacy options.

Figure 17

Task	Facebook	MySpace	Orkut
Add information to profile.	90	90	88.9
Upload a profile picture.	90	**20**	**33.3**
Write on wall of friend.	100	100	66.7
Read & Reply to a message.	90	100	66.7
Change privacy settings for profile.	88.9	70	**40**

Orkut shown as least user friendly in managing privacy issues
Privacy intrusion due to data theft worms

The security labs (2006) identified a worm that propagated via orkut and steals the details on the passwords usernames and banking details. The lab announced that "The initial executable file that causes the infection installs two additional files on the user's computer. These then e-mail banking details and passwords to the worm's anonymous creator when infected users click on the "My Computer" icon. The infection spreads automatically by posting a URL in another user's Orkut Scrapbook, a guestbook where visitors can leave comments visible on the user's page. This link lures visitors with a message in Portuguese, falsely claiming to offer additional photos. The message text that carries an infection link can vary from case to case. Orkut is popular among Brazilian Internet users. In addition to stealing personal information, the malware can also enable a remote user to control the PC and make it part of a botnet, a network of infected PCs controlled by a hacker. The botnet in this case uses an infected PC's bandwidth to distribute large, pirated movie files, potentially slowing down an end-user's connection speed".

CHAPTER 5 – CONCLUSIONS & RECOMMENDATIONS
On analysing the settings of privacy, extent of use and the threats of privacy the following are the facts that are revealed from the studies presented above:

Summary of the findings

On the whole, the intention of dating stood out as one of the primary motives. Other motives like, getting to know their class mates, being able to stay in contact were also in the list. But at present, "Showing information about themselves/ advertising themselves," "Making them more popular," and "Finding dates" are identified as the most sought out actions. As the concerns for privacy increase there is less number providing such information. But still a high percent of the concerned people reveal their sexual orientation and relatively high percent show the name of their partners and are willing to expose their political orientation, show the extent of neglect of the privacy concerns. When, the profiles of the users were downloaded before and after the survey and the information was compared. There were only a small number of members who changed their behavior after the survey. This kind of change is possible to happen in the participants even if such a survey was not done. There are high concerns for privacy, but only a fraction of the participant had high concerns enough to deactivate their profiles just for the implications on their privacy. The members who were not in Facebook had higher concerns for privacy than that of the members. . But the youngsters show a shocking trend that apart from being not concerned about the issues of privacy, the youngsters want their privacy to be explored by the others.
Myspace has been shown to be a site with more information provided on the privacy policies that that of the other sites. But still when coming to the matter of trust, Myspace falls behind. . The professionalism exhibited by the site and the quality and ease of use of the site is more useful in gaining the trust and confidence of the users (Acquisti and Gross, 2006). The role of the contents of the privacy policy and the indications on the issues of privacy come next in winning the trust of the users. This might be the reason for the differences existing between Facebook and MySpace . Facebook has a very appealing screen design and hence it is trusted most by the users more than that of MySpace. Hence the privacy score of 0.48 is slightly lesser than that obtained by Facebook. The excess confidence on Facebook is due to the clarity in the layout of the site than that of the privacy policies of the site.

Orkut is the site popular only in India and Brazil. Google maintains the address, hobbies, employment, phone numbers etc which are contained in the profiles of the users. Google indeed, maintains all the above mentioned information, even after the profile has been deleted by the orkut user. Though there are many complexities in the settings of privacy in orkut, there are also many confusing words and ambiguous settings that compounds the privacy issues in orkut. orkut was found to the least user friendly site with reference to managing the privacy settings. Only 40 percent were successful in managing which was very low compared to that of the other sites.

Recommendations

Learning from others

As there is an increasing importance for screen design Myspace can take the example of Facebook in providing a more appealing screen design. Both Facebook and Myspace being the leadig social networking sites can incorporate more fool proof settings in their privacy settings by taking the example of some of the good features from other less popular social networking sites like Sonica and Netlog which possess a preset combination of buttons for the selection of privacy options. The warning on the prevention of phishing could be made as integral and important features of the sites. Orkut instead of displaying privacy settings in a drop down or pop up menu can make its settings more user friendly and follow the lead of the other more popular sites-Facebook and MySpace and propagate itself into nations other than India and Brazil as well.

Demystifying social stigma

David Brin (1998) is of the opinion that the increase in the level of exposure would make the society transparent where many of the behaviors that are stigmatized are common occurrences and they are not big deals. For example, the profiles indicating the orientation for same sex would help to remove the stigma existing around such minority people.

Negative consequences

There has been a lot of adverse influences from the social networking sites on the users that ranges from incidents like the blackmailing of a beauty queen and a college student who was denied a certificate as there was a picture of him in Facebook holding a drink. When we take the politicians, most of the embarrassing part of their lives came to light only after they were established as renowned national figures. But now, because of the increased levels of exposures so early in lives there may be a great constricting effect. There would be filtering out of many good talents before they make themselves good enough to be specifically exposed and embarrassed. In the context of the politicians and other national figures post hoc exposures would do great deal of harm to their lives, but the filtering of the younger age itself would lead to a dramatic shrinking of the pipe line or introduce drastic alterations in the charaters of people who make it through.

As rightly said by (Tufekci, 2008), "The problems engendered by the affordances of information technology are here with us to stay, and there are no simple solutions. Our conversation about this issue should include an understanding of the process of privacy optimization sought by students and a dialogue about how we, as a society, wish to draw the boundaries between public and private, disclosure and withdrawal, and past choices and future possibilities"- a persusive insistence on the importance and implications of the privacy policies by the sites, parents, teachers and the government would go a long way in the minimization of privacy related threats.

Fighting with technology

There are privacy services that are pervasive as well as easy to use available so that control can be exerted over the presence of private data online. Developing an online privacy life cycle from the perspective of the user and the use of the same perspective for categorizing of the services would lead to effective management of privacy issues. A solution in the form of a layered design for facilitating online privacy is also a feasible solution. There are also other sophisticated technological options like the advent of "the PeCAN (Personal Context Agent Networking) architecture to a platform for pervasively providing multiple contexts for user privacy preferences and online informational privacy services , and use of platform network effects for increasing wide-scale user adoption of privacy services. Platform-mediated networks, are reportedly the vehicles for most of the revenue earned by 60 of the world's largest companies, and other platforms that commonly host millions of users, will not have to individually reinvent and manage sophisticated user services for privacy protection since universal privacy platforms can be layered on them in future". (Dawn, 2010)

REFERENCES

- Acquisti, A., and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. In Privacy-Enhancing Technologies, LNCS vol. 4258, 6th Workshop on Privacy Enhancing Technologies (pp. 36–58), Berlin/Heidelberg: Springer.
- Adams (1999).The implications of users' multimedia privacy perceptions on communication and information privacy policies, in: Proceedings of Telecommunications Policy Research Conference,
- Albrechtslund,A. (2008). Online social networking as participatory surveillance. First Monday, 13(3).
- Amanda, L (2005)"Protecting teens online," Pew Internet and American Life Project, at http://www.pewinternet.org/pdfs/PIP_Filters_Report.pdf,

- Anderson, G., (1993). Fundamentals of Educational Research. Falmer Press, London, pp: 152-160.
- Anderson, K. J. (2001). Internet use among college students: An exploratory study. Journal of American College Health, 50, 21−26.
- Antón, A. I., Earp, J. B., Bolchini, D., He, Q., Jensen, C., and Stufflebeam, W., (2004). The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. IEEE Security and Privacy, 2(2), pp. 36-45.
- Antone R (2006). "Another isle man allegedly baits teen victim on MySpace," Honolulu Star Bulletin (9 March), at http://starbulletin.com/2006/03/09/news/story05.html,
- Ashley, P. Hada, S. Karjoth, G.. Powers and Schunter M. (2003). Enterprise Privacy Authorization Language (EPAL 1.1). IBM Research Report, October 1,
- Ashley, P. Hada, SKarjoth, . G. Powers, C. Schunter, M. (2003). Enterprise Privacy Authorization Language (EPAL 1.1), Research Report 3485, IBM Research Available from: <http://www.zurich.ibm.com/security/enterpriseprivacy/e pal/>.

- Ashwini, R. and Smitha, L (2009). Empirical study of factors affecting success of SNS (Social Networking Sites)
- Auchard, E . 2006. "MySpace.com hires child safety czar from Microsoft," Reuters (10 April), at http://today.reuters.com/news/articlebusiness.aspx?type=mediaandstoryID=nN101347andfrom=business, accessed 12 April 2006.
- Bahrampour,T and Aratani,L (2006). "Teens' bold blogs alarm area schools," Washington Post (17 January), http://www.washingtonpost.com/wp-dyn/content/article/2006/01/16/AR2006011601489.html,
- Barnes B., Susan. (2007). A Privacy Paradox, Social networking in United States, First Monday Volume 11, Number 9 — 4 September.
- Barth, J.C. Mitchell, J. Rosenstein, (2004). Conflict and combination in privacy policy languages, in: Proceedings of WPES'04, ACM Press, , pp. 45–46
- Berkovsky, S., Aroyo, L., Heckmann, D., Houben, G., Kröner, A., Kuflik, T., et al. (2007).
- Blakely, R. (2007). Facebook prodded into privacy U-turn. in The Times. http:// business.timesonline.co.uk/tol/business/industry sectors/media/article2966861.ece
- Bonneau, J and Preibusch,S (2009). The Privacy Jungle: On the Market for Data Protection in Social Networks. The Eighth Workshop on the Economics of Information Security
- Boslaugh, S. Secondary Data Sources for Public Health: A Practical Guide. Cambridge niversity Press. Cambridge.
- Boyd, D., and Ellison, N. B. (2007). Social network sites: Definition, history and scholarship.Journal of Computer-Mediated Communication, 13 article 11.
- Brin, D. (1998). The transparent society. New York: Addison- Wesley.
- Bryman, A and Bell, E (2003) Business Research Methods Oxford University Press
- Bygrave, L.A. (2002), Data protection law: approaching its rationale, logic, and limits, Information Law Series, 10, Kluwer Law International, The Hague,

- Carminati, E. Ferrari, A. Perego, Private relationships in social networks, Private Data Management, IEEE Press, 2007.
- Carminati, E. Ferrari, A. Perego, Rule-based access control for social networks, OTM Workshops, LNCS 4278, Springer-Verlag, 2006. pp. 1734–1744.
- Comscore ,"Top Social Networking Sites in India February", 18th, Comscore report, 2009
- Cranor, L. Langheinrich, M. Marchiori, M. Reagle, J. (April 2002).The Platform fo Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation Available from: <http://www.w3.org/TR/P3P/>.
- Cranor L. F. (2002). Web Privacy with P3P. O'Reilly
- Creswell, J. W., Shope, R., Plano Clark, V. L., andGreen, D. O. (2003). How interpretive qualitative research extends mixed methods research.
- Dawn N.J, (2010)Layering privacy on operating systems, social networks, and other platforms by design. Identity in the Information Society
- Debatin, B., Lovejoy, J,P., Horn, A,K., and Hughes, B,N. (2009)Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication 15: 83–108
- Duffy,M., 2006. "A dad's encounter with the vortex of Facebook," Time (19 March), at http://www.time.com/time/magazine/article/0,9171,1174704,00.html, accessed 21 March 2006.
- Dumortier, J. Goemans C. (2004), Legal challenges for privacy protection and identity management, Security and Privacy in Advanced Networking Technologies, vol. 193, IOS press.
- Ellison, N. B., Steinfield, C., and Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), article 1.
- Fitzpatrick M G., (2006). "Deleting Online Predators Act of 2006 (DOPA), A bill introduced into the United States Congress, 9 May 2006," at http://thomas.loc.gov/, accessed 20 August 2006.
- Flinn, S., and Lumsden, J. (2005). User perceptions of privacy and security on the Web. http://www.lib.unb.ca/Texts/PST/2005/pdf/flinn.pdf.
- Feigenbaum, J. Freedman, M.J. Sander, T. A. Shostack (2002). Privacy engineering for digital rights management systems, in: Proceedings of DRM'01, Springer- Verlag, 2002, pp. 76–105.
- Fox,D and Naidu,S **(2009)**, Usability Evaluation of Three Social Networking SitesUsability news. Vol. 11 Issue 1
- Google support (2010) Retrieved online on June 28 2009 from http://www.google.com/support/orkut/bin/answer.py?answer=177575
- Gross.R. Re-identifying facial images (2005) Technical report, Carnegie Mellon University, Institute for Software Research International. In preparation.
- Gross, R., Acquisti, A., and Heinz, H. J. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM Workshop on Privacy the Electronic Society.
- Harris Interactive, (2001). Why some companies are trusted and others are not: personal experience and knowledge of company more important than glitz, , http://www.harrisinteractive.com/ harris_poll/index.asp?PID ¼ 237.
- Hilty, M. Basin, D.A. Pretschner, A. (2005). On obligations, in: Proceedings of ESORICS'05, LNCS, vol. 3679, Springer-Verlag, pp. 98–117.

- Hoffman, D., Novak, T.P., Peralta, M., 1999. Building consumer trust online. Communications of the ACM 42 (4), 80–85.
- James E. Katz and Ronald E. Rice, (2002). Social consequences of Internet use: Access, involvement, and interaction. Cambridge, Mass.: MIT Press.
- Jenkins, H and Boyd, D2006. "Discussion: MySpace and Deleting Online Predators Act (DOPA)," (24 May), at http://www.danah.org/papers/MySpaceDOPA.html, accessed 26 May 2006
- Jessi, H and Paula,L (2005). "The MySpace generation," BusinessWeek (12 December), at http://www.businessweek.com/, accessed 8 December 2005.
- Jiang, X., Hong, J. I., and Landay, J. A. (2002). Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing. Paper presented at the Fourth International Conference on Ubiquitous Computing, Goteberg, Sweden.
- Johnson,C III. (2007). Safeguarding against and responding to the breach of personally identifiable information. Office of Management and Budget Memorandum.
- Karjoth,G M. Schunter, M, E,. Van Herreweghe (2003). Translating Privacy Practices into Privacy Promises - How to Promise What You Can Keep. In Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), pp. 135-146.
- Kaveri,S, StephanieRM. , Natalia, W., Espinoza ,G Online and offline social networks: Use of social networking sites by emerging adults, Journal of Applied Developmental Psychology 29 (2008) 420–433
- Kavakli, C. Kalloniatis, P. Loucopoulos, S. Gritzalis (2003) Incorporating privacy requirements into the system design process: the pris conceptual framework, Internet Research 16 (2).
- Kenny, S, Borking. J. (2002).The value of privacy engineering, Journal of Information, Law and Technology 4 (1)
- Kolbitsch, J., and Maurer, H. (2006). The transformation of the Web: How emerging communities shape the information we consume. Journal of Universal Computer Science, 12(2), 187–213.
- Lampe, C., Ellison, N., and Steinfield, C. (2007). A Face(book) in the crowd: Social searching vs. social browsing. Proceedings of the SIGCHI conference on human factors in computing systems (pp. 434−444). New York: ACM Press.
- Landry, M. and Banville, C. (1992). A Disciplined Methodological Pluralism for MIS Research. Accounting, Management and Information Technology (2:2), 77 – 92
- Langheinrich, M. (2001). Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. In Ubicomp 2001: Ubiquitous Computing, 2001 (vol. 2201/2001, pp. 273–291). LNCS: Springer.
- Langheinrich, M. (2002). A Privacy Awareness System for Ubiquitous Computing Environments. Paper presented at the 4th International Conference on Ubiquitous Computing (Ubicomp 2002), 237-245.
- Lederer, S. (2004, April 1, 2004). Background Readings
- Li, N. T. Yu and Antón A. I. (2003) A semantics-based approach to privacy languages. CERIAS Technical Report TR 2003-28, Purdue University.

- Liu H. and Maes. P. (2005). Interestmap: Harvesting social network profiles for recommendations. In Beyond Personalization - IUI 2005, January 9, San Diego, California, USA.
- Matthew, F; Dutta,S (2008). Throwing Sheep in the Boardroom: How Online Social Networking Will Transform Your Life, Work and World. Wiley
- Mcmillan, S. J., and Morrison, M. (2008). Coming of age with the Internet: A qualitative exploration of how the Internet has become an integral part of young people's lives. New Media Society, 8, 73−95.
- Mitrano, T. 2006. "Thoughts on Facebook," at http://www.cit.cornell.edu/oit/policy/memos/facebook.html, accessed 26 July 2006.
- Morgan, G., and L. Smircich, 1980. The Case for Qualitative Research. Acad. Manag. Rev., 5 (4): 491-500.
- Morgan, C., and Cotten, S. R. (2003). The relationship between Internet activities and depressive symptoms in a sample of college freshman. CyberPsychology and Behavior, 6, 133−142.
- Myers, M., D and Avison, D. (2002). An Introduction to Qualitative Research in Information Systems. Qualitative Research in Information Systems: a Reader. (eds. Myers, M. D. and Avison, D.), pp. 3 - 12, London et al.: Sage
- Newitz (2003). Defenses lacking at social network sites. SecurityFocus.
- PashaM. K, (2007)Sify.com.
- Paolo,G. Nicola, Z Information (2009) Towards the development of privacy-aware systems and Software Technology 51 337–350
- Patton, M., 1987. How to Use Qualitative Methods in Evaluation. Sage Publication, California, pp: 18-20.
- Parameswaran, M., and Whinston, A. B. (2007). Research issues in social computing.Journal of the Association of Information Systems, 8(6), 336–350.
- Paul, P., (2001).. Mixed signals. American Demographics 23, 44–49.
- Phillips, P. Flynn, P. Scruggs, T, Bowyer, (1997) . K. J. et al Classification of research efforts in requirements engineering, CSUR 29 (4) 315–321.
- Preibusch, S., Hoser, B., Gürses, S., and Berendt, B. (2007). Ubiquitous social networks—opportunities and challenges for privacy-aware user modelling. In Proceedings of the Data Mining for User Modelling Workshop (DM.UM'07) at UM 2007 Corfu, June,
- Privacy international (2007). A consultation report. A Race to the Bottom - Privacy Ranking of Internet Service Companies. Retrieved online on June 28 2009 from http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961
- Providing context-aware personalization through cross-context reasoning of user modeling data. In Proceedings of the International Workshop on Ubiquitous and Decentralized User Modeling (UBIDEUM) at 11th International Conference on User Modeling User Modeling Inc., 26 June, (pp. 2–7).
- Ratnasingham, P., Kumar, K.,(2000). Trading Partner Trust in Electronic
- Reina ,S.J.,and Curtis,T (1995). Tendencies and tensions of the information age: The production and distribution of information in the United States. New Brunswick, N.J.: Transaction Publishers.
- Room, S. (2007), Data Protection and Compliance in Context, BCS,.
- Saad, H.E.D., (2006), Brazil.

- Savona E, U. and Mignone, M(2004,) ‘‘The Fox and The Hunters: How IC Technologies Change the Crime Race’’, European Journal on Criminal Policy and Research 10: 3–26, at pp. 7 11.
- Staab, S. Domingos, P. Mika, P. Golbeck, J. Ding, L. et al., Social networks applied, IEEE Intelligent Systems 20 (1) (2005) 80–93.
- Stefan ,W Privacy threat model for data portability in social network applications International Journal of Information Management 29 (2009) 249–254
- Sue,D(2006)“Teens who tell too much,” New York Times (15 January), at http://www.nytimes.com/,
- Sullivan,B (2005). “Kids, blogs and too much information: Children reveal more online than parents know,” MSNBC.com,
- The security labs (2006).Data-theft worm targeting google's orkut. SpywareGuide Database.
- Topping, A. (2009).Warning to criminals: police may be watching you on Facebook. in The Guardian. http://www.guardian.co.uk/news/blog/2009/jan/14/facebookarrest-new-zealand
- Tufekci, Z (2008) Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology and Society Vol. 28, No. 1, 20-36
- Verini, J.,2006. Will success spoil MySpace? Vanity Fair (March), pp. 238–249, and at http://www.vanityfair.com/commentary/content/articles/060308roco01
- Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. European Journal of Information Systems 4, 74 – 81
- Warren, S.D,Brandeis. L.D. (1890). The right to privacy, Harvard Law Review 4 (5) 193–220.
- Wang, H., Lee, M.K.O., Wang, C., (1998). Consumer privacy concerns about internet marketing. Communications of the ACM 41 (3), 63–70.
- Wang, D.-W.. Liau, C.-J Sheng T. H, Privacy protection in social network data disclosure based on granular computing, IEEE International Conference on Fuzzy Systems, IEEE Computer Society, 2006.
- Ways To Adjust Privacy Settings In Facebook. (2009). Center for information policy research (CIPR)
- Weiss, S. (2007). The need for a paradigm shift in addressing privacy risks in social networking applications. In: Post-Proceedings: The Future of Identity in the Information Society; Third International Summer School organized by IFIP WG 9.2, 9.6/11.7, 11.6 in cooperation with FIDIS Network of Excellence (pp. 161–171), Sweden: Karlstad.
- Wellman, B., Salaff, J., Dimitrova, D., Garton, L., Gulia, M., and Haythornthwaite, C. (1996). Computer networks as social networks: Collaborative work, telework, and virtual community. Annual Review of Sociology, 22, 213-238.
- Worek J. (2005). Overview of the face recognition grand challenge. In IEEE Conference on Computer Vision and Pattern Recognition, June 20-25, San Diego, California, USA.
- Yin, R., 1989. Case Study Research. Sage Publication, California, pp: 22-26.