

PRIVACY ISSUES IN SOCIAL NETWORKING SITES: A STUDY OF USERS IN KOLHAPUR AND SANGLI DISTRICTS

A. A. Sattikar^{#1}, Dr. R. V. Kulkarni^{*2}

#Assistant Professor

V. P. Institute of Management Studies & Research, Sangli, Maharashtra, India

&

**Professor & Head*

Chh. Shahu Institute of Business Education & Research (CSIBER), Kolhapur, Maharashtra, India

Abstract—

Social networking software is still in its adolescence. Users are becoming sophisticated enough to realise that there is little point in bringing people together just for the sake of bringing people together and they are demanding more. Nevertheless, it is an appealing and engaging environment once users have found their tribe. But it has been observed that security and privacy issues have not been seriously handled by these social networking sites. For example some sites are allowing their third parties to access the personal information of their users without bothering of the privacy. The list of the privacy risks with undesired access to profile information is continuously growing from the identity theft, spam to cyber bullying. Users need to be careful with what and how they reveal details of themselves. The challenge for users is to learn to judge precisely the amount of information they should divulge to attract a similar person and the amount they should reveal to protect themselves from exploitation.

Keywords— *Social Networking, Privacy, Security, Awareness*

1. Introduction

Online Privacy is a very delicate issue and needs to be tackled with due care. It highlights the need for the public to have a better understanding of the scope of use of data on social networking sites and the potential risks of posting data on such sites. In an increasingly competitive and commercial market, there is a real incentive for social networking sites to address the privacy issues and take steps to reassure their users as to how the users' data will be protected and used. Past work revealed that users have high expectations for privacy on social networking web sites. There are a number of commercial, legal and government organizations always trying to get access to this huge amount of data shared by users. Hence users must be careful while disclosing their details online. To protect themselves from online threats, users must identify how much information they should share and who will access this information. Users should apply privacy settings to protect their personal information in social networking web sites as such information is easily accessible for others.

2. Privacy Awareness among Users

Users are usually unaware of different threats to their security and privacy and always get confused when their personal information falls in “privacy issues” those are totally unknown to them. Many researches have been carried out to investigate users' concern about their security and privacy but unfortunately there

is no thorough research on the security and privacy issues of social networking and how users are concerned about these issues and what technology they are using to protect themselves. Similarly all the facts of privacy violations have not been considered which can prove dangerous for users while sharing information online. With the above background in the mind, the study is carried out to investigate user's concerns about privacy in Social networking web sites. The objective is to make people to take privacy issues more importantly and try to protect themselves from falling victim to online and offline crimes and incidents.

The study was conducted by means of a survey of social networking users in Kolhapur and Sangli district. The sample size of 500 respondents was drawn from the users of social networking sites from the selected cities and towns of Kolhapur and Sangli districts.

Table 1 Total Sample Profile

Total Sample Profile		Male	Female	Total	
Student	UG Student	120	88	208	250
	PG Student	24	18	42	
Non-Student	Businessman/Self-employed	9	4	13	250
	Employee	97	61	158	
	House Wife	0	79	79	
Total		250	250	N=500	

The primary data necessary for the study has been collected through questionnaire method. The questionnaire was based on a combination of closed-ended, dichotomous and multichotomous questions, with single and multiple responses.

Based on users' behavior, concerns and actual risks to their privacy associated with Social Networking web sites, the following hypothesis has been stated.

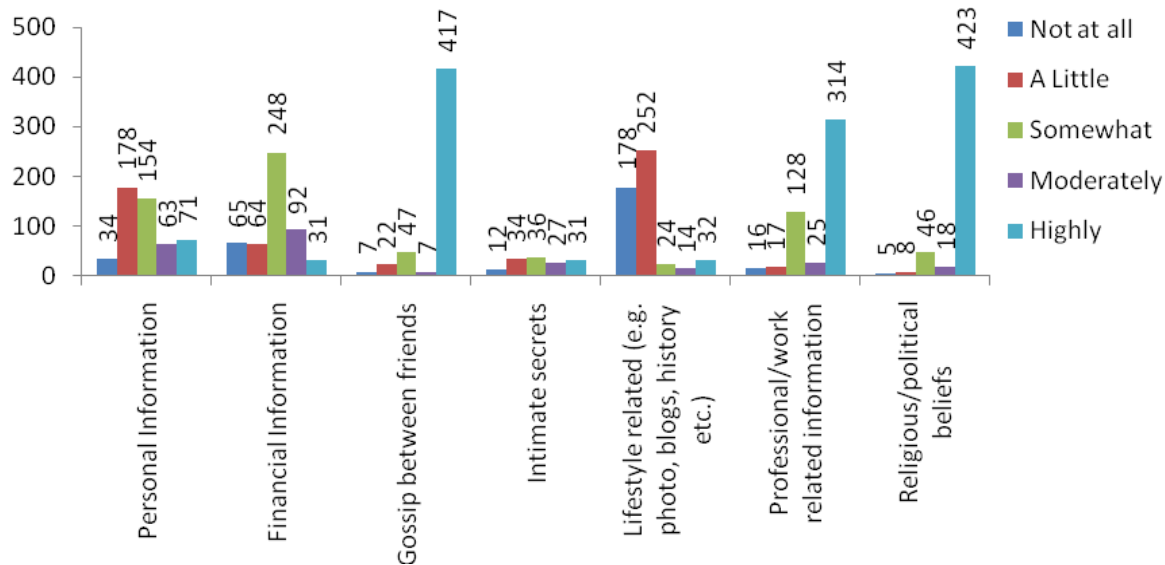
H0: There is no significant relationship between concern about privacy and disclosure of information.

Despite the fact that there is some level of online danger today, respondents who participated in the survey are confident in their ability to stay safe online, the below table shows the concern of users about their privacy on social networking sites.

Table 2 Concern about Privacy of information submitted on Social Networking Sites

Sr.	Particulars	Not at all	A Little	Somewhat	Moderately	Highly	Total
		1	2	3	4	5	
1	Personal Information	34	178	154	63	71	500
2	Financial Information	65	64	248	92	31	500
3	Gossip between friends	7	22	47	7	417	500
4	Intimate secrets	12	34	36	27	391	500
5	Lifestyle related (e.g. photo, blogs, history etc.)	178	252	24	14	32	500
6	Professional/work related information	16	17	128	25	314	500
7	Religious/political beliefs	5	8	46	18	423	500

Fig. 1 Concern about Privacy of information submitted on Social Networking Sites



When asked if respondents had ever decided not to submit personal information online, they were somewhat concerned (67%) about the privacy of their personal information and had made a similar decision about their financial information (63%). Among the respondents, most were highly concerned not to post gossip between friends (83%) and intimate secrets because of its impact on their privacy (78%). Although students are heavy social media users, it’s still surprising that they are less concerned about

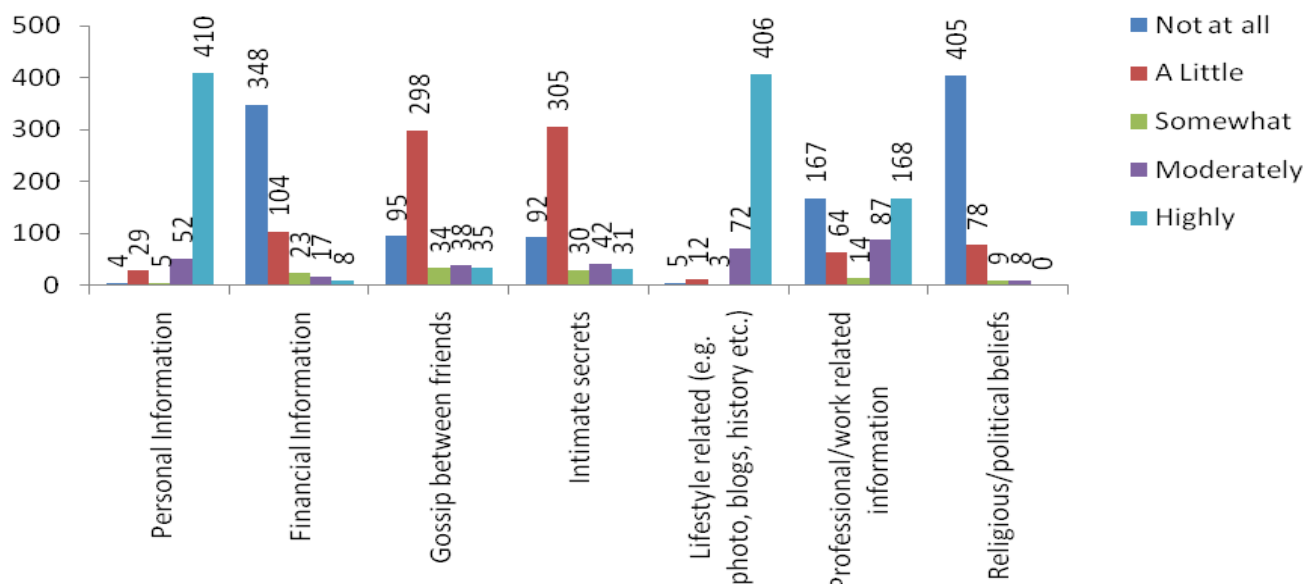
privacy while disclosing lifestyle related information (86%) while employees, businessman/self-employed users are highly concerned about the privacy of their professional/work related information and sharing it with friends and strangers (63%).

As a follow-up to concern for privacy while sharing religious/and political beliefs, users wanted to determine high concern about sharing such information (85%) primarily due to heightened awareness of the issue in news and media.

Table 3 Activeness in disclosing information submitted on Social Networking Sites

Sr.	Particulars	Not at all	A Little	Somewhat	Moderately	Highly	Total
		1	2	3	4	5	
1	Personal Information	4	29	52	410		500
2	Financial Information	348	104	23	17	8	500
3	Gossip between friends	95	298	34	38	35	500
4	Intimate secrets	92	305	30	42	31	500
5	Lifestyle related (e.g. photo, blogs, history)	5	12	3	72	406	500
6	Professional/work related information	167	64	14	87	168	500
7	Religious/political beliefs	405	78	9	8	0	500

Fig. 2 Activeness in disclosing information submitted on Social Networking Sites

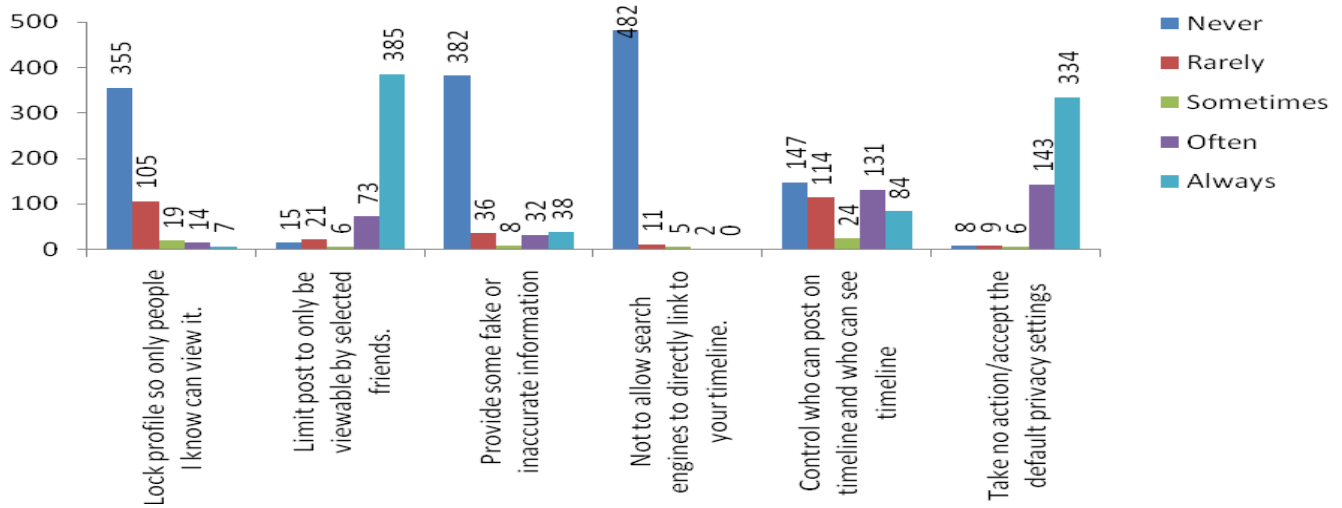


The table above is designed to find out what types of information are routinely posted on social media. The respondents indicated that their personal information could be highly found on their social media profile (82%). Very few respondents have their financial information listed on their profile (8%). Nearly 80% of those surveyed are highly active in listing the lifestyle related information on their profile and 34% of those surveyed have Professional/work related information on their Facebook profile. At a minimum, the respondents provide negligible information of Religious/political beliefs (8%). It is evident from the survey that nearly 2/3rd of those surveyed are little active to provide Gossip between friends and Intimate secrets (60%).

Table 4 Privacy controls settings used in Social Networking Sites

Sr.	Particulars	Never	Rarely	Sometimes	Often	Always	Total
		1	2	3	4	5	
1	Lock profile so only people I know can view it.	355	105	19	14	7	500
2	Limit post to only be viewable by selected friends.	15	21	6	73	385	500
3	Provide some fake or inaccurate information	382	36	8	32	38	500
4	Not to allow search engines to directly link to your timeline.	482	11	5	2	0	500
5	Control who can post on timeline and who can see timeline	147	114	24	131	84	500
6	Take no action/accept the default privacy settings	8	9	6	143	334	500

Fig. 3 Privacy controls settings used in Social Networking Sites



The survey found that 71% of the respondents did not know what the privacy settings were on their profile and did not have locked their profile to be viewed by only people they know. Females seem to be more active online than males, perhaps because communicating and sharing information are more typical behaviors for them. For instance, females (48%) are more likely than males (29%) to limit post to only be viewable by selected friends. Looking at the results in the above table in relation to the results for providing fake or inaccurate information, researchers found it likely that some percentage of these respondents (8%) provided such information (mostly the profile picture) to the general public. It is discouraging that most of the surveyed participants are completely unaware of linking of search engines to their timeline. 3% of those surveyed have rarely allowed search engines to directly link to their timeline. Unfortunately, it leaves 62% of the survey respondents vulnerable to having their personal information exposed due to incorrect privacy settings for controlling who can post on timeline and who can see timeline. Only 17% of the respondents recognized correctly to control who can post on timeline and who can see timeline, the majority of respondents did not recognize the potential risk of not controlling the timeline. It is evident from the survey that most respondents did not take any action for the privacy setting. Nearly 2/3rd of those surveyed got default privacy settings.

Hypothesis Testing

Null Hypothesis (H0): *There is no significant relationship between concern about privacy and disclosure of information.*

Test Used: Chi-squared test.

A chi-square test for independence compares two variables in a contingency table to see if they are related. The chi-square test is used to determine whether an association (or relationship) between 2 variables in a sample is likely to reflect a real association between these 2 variables in the population. In the case of 2 variables being compared, the test can also be interpreted as determining if there is a

difference between the two variables.

Table 5 Personal information details.

Sr.	Particulars (O)	Not at all	A Little	Somewhat	Moderately	Highly	Total
1	Concern about privacy	34	178	154	63	71	500
2	Activeness in disclosing	4	29	5	52	410	500
	Total	38	207	159	115	481	1000

Source: Table 4.20 and Table 4.21

Table 6 Observed frequency table for Personal information details.

Sr.	Particulars (O)	Personal Information Details		Total
		Less	Greater	
1	Concern about privacy	429	71	500
2	Activeness in disclosing	90	410	500
	Total	519	481	1000

Table 7 Expected frequency table for Personal information details.

Sr.	Particulars (O)	Personal Information Details		Total
		Less	Greater	
1	Concern about privacy	259.5	240.5	500
2	Activeness in disclosing	259.5	240.5	500
	Total	519	481	1000

<p>t-value</p> $\sum \frac{(O-E)^2}{E}$ <p>= 461.28</p>	<p>The p-value in the chi-square table for d.f = 1 at 5% significant level is 3.84. Since the calculated t-value (461.62) exceeds the p-value (3.84), reject the null hypothesis at 5% level. The conclusion is that <i>there is significant relationship between concern about privacy and disclosure of information and it is found that people who are highly concerned about their privacy disclose less information.</i></p>
---	--

3. Conclusion

There is significant difference between privacy settings used by male and female users while using Social Networking web sites. It is found that females are more likely to use privacy settings to protect themselves when using Social Networking web sites. It was predicted that females are more likely to be cautious over social networking sites and use the privacy settings to help them accomplish this. This was the case with the results showing that though females were more private when it came to types of profiles, management of privacy settings, the majority of males also kept watch on their privacy settings showing that there is no gap between the two genders when it comes to profile privacy. It was also revealed that people who have greater concern about privacy will disclose less information.

The way social networking sites and tools are evolving as a vital tool to communicate with current and new friends, security and privacy seems to be compromised in while protecting users against issues like identity theft. Forming a self-group on social networking sites and participating in online communication sets personal information in a danger of getting stolen and leaving only option to take responsibility for protecting ourselves. Users should always take care while sharing information. They should not reveal sensitive and personal information like home address, phone numbers or financial information. Their identity can be easily revealed if they share more information through posts.

The world of social media, mobile technology is constantly evolving around information security, users should protect themselves against cybercrime by staying alert with ongoing developments. At the end it's a concern amongst users that will help them to remain safe against threats.

4. References

- Avner Levin, Patricia Sanchez Avril; Two notion of Privacy online; Vanderbilt Journal of Entertainment and Technology Law, Summer 2009
- Helen Anderson; A privacy wake-up call for social networking sites; Entertainment Law Review, 2009
- Lior Jacob; A Social Networks Theory of privacy; University of Chicago Law Review, Summer 2009
- Nick Graham, Helen Anderson; Are individuals waking up to the privacy implications of social networking sites?; European Intellectual Property Review, 2010
- David Hector Mones; Living Our Lives Online: The Privacy Implications Of Online Social Networking; Journal of Law and Policy for the Information Society, Spring 2010.

- Brian Kane; Balancing Anonymity, Popularity, & Micro-Celebrity: The Crossroads Of Social Networking & Privacy; Albany Law Journal of Science and Technology, 2010.
- Jennifer Hendry; Facebook and the Commercialisation of Personal Information: Some Questions of Provider-to-User Privacy; University of Leeds Law Review, 2010.
- A.A. Sattikar, Dr. R.V. Kulkarni (2011), “A Review of Security and Privacy Issues in Social Networking”, International Journal of Computer Science and Information Technologies, Vol. 2 (6), 2011, 2784-2787
- A.A. Sattikar, Dr. R.V. Kulkarni (2012), “A Role of Artificial Intelligence in Security and Privacy Issues in Social Networking”, International Journal of Computer Science and Engineering Technologies, Vol. 2 (1), 2012, 792-795
- A.A. Sattikar, Dr. R.V. Kulkarni (2013), “A Research on Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking”, National conference on Innovative developments and Emerging research Avenues in Software technologies 11 October 2013