Privacy Issues of Social Networking Sites at Workplace

By Jaideep Saxena
Assistant Professor
School of Computer and Electronics
IPS Academy Indore(M.P)

Abstract

Given the boom in the Internet and mobile devices industry, people across the world are more connected than ever before. Social networking is the in thing.

Social networking is all about developing connections or ties between friends and associates. While people have always networked with one another, the Internet has allowed user to do this in a global manner. Some great examples of popular social networks are Digg, LinkedIn, Facebook, and Twitter. Most people have heard of these services and many use them on a daily basis. These communities are able to generate income from advertising and additional paid services.

This paper mainly shows types of Social Networking Sites i.e. Public Social Network Site and Internal Social Network Site, Use of social networking sites at workplace, describe the effect of public social network site at workplace, Potential privacy issues in Social Network Sites at work and describe needs of internal or private social network site at workplace.

Introduction

A social network is an online service, platform, or site that focuses on building and reflecting of social relations among people, who, for example, share interests and/or activities. A social network service essentially consists of a representation of each user (often a profile), social links, and a variety of additional services. Most social network services are web based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, activities, events, and interests within their individual networks. Social networking sites share some conventional features. Most often, individual users are encouraged to create profiles containing various information about them. Users can often upload pictures of themselves to their profiles, post blog entries for others to read, search for other users with similar interests. To protect user privacy, social networks usually have controls that allow users to choose who can view their profile, contact them, add them to their list of contacts, and so on. In recent years, it has also become common for a wide variety of organizations to create profiles to advertise products and services.
Types of Social Network

There are two types of social network:

1. **Public Social Network Site**
   Social network sites are predominantly run by commercial providers, with the software and data residing on the providers’ own servers. They are often free, but sometimes subscription based. Well known examples include Facebook, LinkedIn and Twitter.

2. **Internal Social Network Site**
   Some large organisations run their own social network site on their own servers, this will refer to as an “internal social network site”. Examples Beehive at IBM, and Watercooler at HP. In some cases organisations will contract an external provider to provide a private social network site for them. In this case the servers may not be physically located in an organisation, but this paper will also treat this as being an internal social network site.

The Use of Public Social Network Sites for Work

This project significantly describes the fact that how public social network sites get used for work. “For work” means the ways in which people form ties and communicate with others on a professional or semi-professional basis. The use of public social networks at work is a useful place to start for two reasons: public social network sites are widely used at work, and there are several published studies making helpful data available. Some public social network sites, such as LinkedIn, are specifically designed for professional use but in reality, social network sites, be they professional or leisure oriented, are used by many people for a mix of work-related and leisure-related activities. [1]

**Facebook and LinkedIn at Work**

This paper has found two research teams that are exploring what happens when social network sites span professional and social boundaries. Skeels and Grudin [2] have conducted research within Microsoft, and DiMicco and Millen [3] have conducted research within IBM. Skeels and Grudin found that at Microsoft, in early 2008, around 37% of employees were using Facebook, with around 17% using it daily. More employees, around 50%, were found to have LinkedIn accounts, but far fewer of them, around 4%, were using it daily. Skeels and Grudin found a number of positive benefits come from using these technologies. LinkedIn was useful for building and maintaining professional networks. Facebook was useful in the workplace for creating and strengthening ties. But Skeels and Grudin also found worries amongst many staff using LinkedIn and Facebook about the legitimacy of this activity. In particular, there were questions over time wasting, and over security and the possibility of disclosing confidential information. There were also more practical problems for staff in mixing professional and social life, and there were related issues in whether connections should cross hierarchy, status and power boundaries.

DiMicco and Millen on the other hand looked at the use of Facebook by graduate recruits to IBM. They noticed that recruits would present themselves in one of three ways. Some were, as DiMicco and Millen put it, “reliving college days”, some were “dressed to impress” and others were “living in the business world”. All of these people had joined the IBM network on Facebook, therefore making themselves visible to anyone within the organisation. But the ways they chose to present
themselves differed markedly. What becomes clear from these studies is that the benefits and drawbacks of allowing public social network sites in the workplace are extremely difficult to evaluate. People use these sites in different ways, and the benefits people find in them, such as the creation and strengthening of ties, are difficult to measure. Because of this situation, both research teams have used qualitative methods to unpick the nuanced and contested values to be found in social networking.

**Banning the Use of Public Social Network Sites at Work**

The view of many employers in the UK on the use of public social network sites at work is not favourable. Many have gone so far as to ban the use of sites such as Facebook. A report by the TUC in 2007 [4] recognised and sought to nullify concerns, arguing that the media exaggerates the problems and consequently employers have been overreacting. The TUC report recognises that employers’ concerns tend to be about time wasting, about the posting of inappropriate content; about the slandering of co-workers or customers, and the possibility of exposing the organisation to a higher risk of phishing attacks (e.g. Pet names mentioned on Facebook might be used as passwords at work). The TUC claim that when handled properly, allowing internet access for staff during breaks can be beneficial for staff and can help them develop IT skills. They recommend a clear and well thought out policy on social networking, this being the best way to ensure employees do not waste time. The TUC also point out that employees are entitled to a private life.

The TUC report assumes social networking to be exclusively a leisure activity. However, as people’s private and work lives are blurred, so too is the use of social network sites. Many people will connect on a social network site to people they know through work, perhaps to colleagues, perhaps to their boss, or perhaps to clients. [2][3]

**Privacy in online social networks**

1. Privacy Risks

Internet users “lack any realistic sense of how public or how permanent the record of their posts online is. This paper has already seen incidents that contents on SNS have been used by employers and law enforcement to assess users. Once contents have been put up on SNS, even if they got deleted by the users, the SNS operators or even external web archive can still save copies of the contents which may be taken out of context and can have negative impact on the users in the future.

The fact that users can use pseudonymous user names on SNS further magnify the illusion that they will not be accountable for what they say or act on SNS. However, Liu and Maes [5] showed that pseudonymous users may be identified through face re-identification, in which the same user uses the same or very similar picture on different social network sites. Narayanan and Shmatikov [6] demonstrated an algorithm purely based on network topology that can de-anonymize users on social networks with very low error rate (in one study of Twitter users, the error rate was 12%). Gross and Acquisti [7] pointed out that other risks range “from identity theft to online and physical stalking, from embarrassment to price discrimination to blackmailing”. Chew et al. [8] raised three privacy-sensitive areas in social networks: lack of control over activity streams, unwelcome linkage, and deanonymization through merging of social graphs.
2. Users’ Behavior towards Information Sharing and Privacy

Gross and Acquisti[7] found that for the majority of CMU Facebook users, their personal data is generously provided and only a very small percentage of them change the default privacy settings on the site. Certainly, there are notable differences across social networks, genders, and socio-economic groups of users. Dwyer et al.[9] found that Facebook users have a greater sense of trust in Facebook and in other members on Facebook and thus reveal more information, however despite their lower trust MySpace users are more likely to extend online relationships beyond the confines of MySpace. Fogel and Nehmad [10] observed that in general men have less privacy concerns that their female counterparts and thus tend to disclose more personal information such as telephone number and physical address on SNS. In a study of MySpace users, Gilbert et al. [11] found that rural users have fewer friends and fewer comments than urban users. Besides, rural users, particularly women, have a higher level of privacy concern and use privacy setting more than urban users.

3. Legal Implications

From a legislative point of view, privacy in social networks poses unique challenges than online privacy in general. This is because users largely provide their information on social networks at their own initiatives (thus can be treated as their consent). Traditional privacy laws based “informed consent” protect users against unfair or disproportional data collection and usage by the websites would be ineffective in this new arena. Therefore, it is not clear how these privacy legislations would apply in Social Network Site.

Potential privacy issues in Social Network Sites at work

Most existing literature in SNS use at workplace either did not explicitly discuss privacy issues or commented that privacy is less of an issue. For example, DiMicco et al. [3] noted that they did not find privacy concerns from their study of Beehive. However, they only studied Beehive users and thus it is possible that the fact that some employees did not adopt Beehive was partly due to their privacy concerns. Therefore, it is also important to study employees who choose not to use SNS at work.

This paper believes the privacy landscape in the enterprise context is convoluted. From the employee’s perspective, there are three types of privacy threats. First, there is privacy among individual users. In the corporate context, they can be your superiors, subordinates and peers. Secondly, there is privacy between users (employees) and their employers. What if the company keeps track of employees’ computer usage at work? How would an employee’s interactions with contacts from her personal circle on SNS affect the impressions that their employers have on them and even the assessment of their work performance? Thirdly, there is privacy between users and SNS operators. From the privacy policies of popular general SNS, it is not clear if the operators can/will transfer or sell the contents on SNS to third parties, but our impression is that the operators still keep this option open.

Based on the discussion of the two previous sections, this paper identifies the following privacy-related issues that need to be further investigated.
1. Impression Management

From existing literature, users know that impression management plays an important role in employees’ everyday work and also in SNS use at work. How do they manage their self-representations simultaneously at a SNS with regard to their personal contacts including family members, professional contacts including their peers, superiors, and subordinates, and SNS operators is an open research question.

2. Pressure to Reveal Personal/Working Information

Brzozowski et al. [12] suggested that in order to encourage adoption of internal social media in an enterprise context, managers should “lead by example”. This paper suspect this may put managerial and/or peer pressure on employees to contribute contents on enterprise SNS.

3. Unintentional Social Undermining in Workplace

Baron [13] argued that interpersonal relationship and interaction are a critical factor affecting the workplace performance. Duffy et al. [14] showed that social undermining in workplace can be quite dramatic. They defined social undermining as “behaviour *intended* to hinder, over time, the ability to establish and maintain positive interpersonal relationships, work-related success, and favourable reputation”. This paper defines *unintentional social undermining* as behaviour that is not intended but practically cause social undermining effect. While (intentional) social undermining may be rare on SNS use at work since adding people to one’s friend list are controlled by the users (they probably would not add people who they have negative relationships with), this paper suspect that unintentional social undermining on SNS can be more frequent. For example, tagging colleagues on photos may cause embarrassment. Besmer and Lipford [15] found that a common reason why people untagged photos is that they did not look good on these photos. Unintentional social undermining can seriously affect employees’ carefully crafted self-representations. SNS at work can be a double-edge sword: it can encourage social support among co-workers but it can also lead to unintentional social undermining in workplace.

**The Use of Internal Social Network Sites at Work**

Some organisations have developed or purchased their own social network sites for use internally.

1. Third Party Development of Internal Social Network Sites

Many organisations that use internal social network sites appear to be using systems developed by third parties. Proctor and Gamble use an online community application called People Connect, which is supplied by Telligent. Best Buy has an employee social network called Blue Shirt Nation, which has been built by third party developers using the open source framework Drupal. BearingPoint, Deloitte, Dow Chemical, and IBM are using a system called The Select Minds Corporate Social Networking Solution Suite, which is supplied by Select Minds. Very little information is available about these systems, although Kuhn [16] from Select Minds has published a general report about his experience in the area.

Kuhn explains that there is often enthusiasm for social networking sites amongst many staff of large organisations; many will desire an...
internal version of Facebook, and college graduates joining the workforce will be surprised employers do not already offer such services. Kuhn explains that there is often frustration with existing knowledge management and portal solutions, and unofficial, special-purpose social media offerings often flourish. However, he also says that managers and directors regularly have concerns about adopting internal social network sites. Concerns include: that social networks might not correspond to organisational charts and could undermine command and control prompts apprehension; that there may be inappropriate behaviour (this fear is driven in part by horror stories in the media, but also the real concern of legally actionable behaviour); and that social networks could be used to form or reinforce cliques. These fears can be mitigated with the provision of controls, for example preapproval of user-generated content, controls on abusive language, and controls on repetitive and potentially abusive behaviour. He has never encountered a client that is comfortable with the anything goes world of Facebook, but says that the interest in control lessens over time as internal social network sites mature. Kuhn explains that organisations that devote one or more people to driving usage (by submitting content, by seeding and encouraging forum discussions, by sending digest email updates) see far more traffic than those who devote fewer resources.

In Kuhn’s experience, the typical constituencies of internal social network sites are employees, alumni, retirees and VIPs (managing directors, retired partners etc.).

2. In-House Development of Internal Social Network Sites

Several large organisations, particularly those in the technology sector, have created their own social network site. SAP has developed an internal social network called Harmony. [17] Accenture have developed a social network site called People Pages. Microsoft has developed a site called Town Square. Deloitte (who use the Select Minds system mentioned above to power their external alumni social network) have created an internal social network site called D Street. IBM has developed two internal social networks: Bluepages (launched in 2001) and Beehive. HP (Hewlett Packard) has developed their own internal system called Watercooler. [1]

All three systems were implemented in large, distributed organisations in which employees are scattered across a myriad of sites, business units and countries, making it virtually impossible for them to know everything going on inside the company. Employees’ at all three companies had already been finding value in the use of Web 2.0 technologies including social network sites, but these mainly public sites were not always an appropriate place for company information. Beehive was launched in May 2007 and, within a year, supported 30,000 employees (around 7.5% of IBM staff). Around one third of these however did not connect to another user or contribute any content. Uptake was globally distributed, and tended to reflect the structure of IBM and the mix of roles rather than any one group. Watercooler was launched in June 2007. The go-live of Watercooler coincided with a major emergency (a forest fire near one of the locations), and the technology was quickly found useful as a way of getting up to date information. However the number of active users of Watercooler is 3000, 0.9% of employees. D Street was launched for 1500 Deloitte staff in June 2007. In June 2008 it was rolled out to 46000 staff, and around 25% of these had edited their (automatically generated) profile within eight weeks.
There are useful lessons to learn from Watercooler, D Street and Beehive, but all three proved hard to track and evaluate. Users do not have to be logged in to use these technologies, click rates do not correlate with reading rates, and content production rates do not necessarily correlate with quality. In order to understand the effectiveness of Watercooler, HP carried out a survey, and supplemented this with an analysis of clicks on blog posts. To understand the effectiveness of Beehive, IBM carried out interviews, repeated over the course of a year. Watercooler was found to be popular for finding people with specific interests or expertise, and for more generally exploring the organisation and groups of people. A majority of users would check the Watercooler home page for new content regularly, and around one half of people that did so would sometimes or usually read new content. Around 20% of people who looked at the homepage would rarely click on links to new content, but some said they appreciated being able to see what is going on at a glance. Beehive was found useful for people to build relationships and make sense of other people. It was found that although users connected with local colleagues, they did not use the site to share content with them. Instead content was more likely to be shared with "weak ties". These weak ties would initially be people they had formally worked with, but would later include people they met through the system. Users liked Beehive because they were able to connect with people more personally, they saw it as helping their career advancement, and they could gather support for their projects. Deloitte clearly views D Street as valuable, although the patterns of use have not been reported. The Lessons learned reported by Deloitte concern governance and programme management. They realised they needed buy in across the organisation and legal guidance during the requirements definition. Senior stakeholders wanted moderators to be able to view and veto content.

Comparison of internal social network sites in three global organisations [1]

<table>
<thead>
<tr>
<th>Social Network Site</th>
<th>Beehive</th>
<th>D Street</th>
<th>Watercooler</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organisation</strong></td>
<td>IBM</td>
<td>Deloitte LLP</td>
<td>Hewlett-Packard (HP)</td>
</tr>
<tr>
<td><strong>Size of Organisation</strong></td>
<td>398000 staff, the largest technology company in the World in 08 by staff.</td>
<td>165000 staff in 140 Countries. 46000 consultants (professionals)</td>
<td>310000 staff, the largest technology company in the World in 08 by turnover.</td>
</tr>
<tr>
<td><strong>Industry</strong></td>
<td>Technology.</td>
<td>Professional services.</td>
<td>Technology.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Profile Creation</td>
<td>Manual.</td>
<td>Automatic for every professional (consultant) In company directory.</td>
<td>Bloggers cross referenced With company directory.</td>
</tr>
<tr>
<td>Uptake in first year</td>
<td>30000 registrations (7.5% of staff). 2/3 of which contributed content or made connections.</td>
<td>11500 profile edits in first 8 weeks (25% of Professionals).</td>
<td>3000 active users (0.9% of Staff).</td>
</tr>
<tr>
<td>Who uses it</td>
<td>? Uptake reflects workforce. 40% of users in USA, 55 countries represented in total. 27% of users are engineers, 15% vice presidents or directors 32% are mobile workers.</td>
<td></td>
<td>Users in every business group, and 55 different countries. Highest usage from Engineering and marketing staff, lowest from operations.</td>
</tr>
<tr>
<td>Control and moderation</td>
<td>Access controls, users can choose who they wish to share content with.</td>
<td>Moderated content.</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

Finally this paper shows the various facts of social networking sites i.e. advantage and disadvantage of social networking sites, effect of these sites at workplace, various privacy issues at workplace, needs of internal social networking sites and shows comparatively study of existing internal social networking sites.

My next paper will shows how we can develop internal social networking sites, what necessary features must be added and explain security model of this.

References

1. Dr John Rooksby Social Networking and the Workplace. In proceeding of Group 2009, School of Computer Science, North Haugh, University of St Andrews, KY16 9SX. UK.


