

# Attitudes to Use of Social Networks in the Workplace and Protection of Personal Data

---

*David Haynes, City University, School of Informatics, Department of Information Science*

*August 2011*

## **Background**

Two surveys conducted during April and May 2011 identified some of the issues that arise when social network services are used in the workplace. A survey of managers responsible for data protection in the workplace explored concerns of employers and the ways in which these concerns might be addressed. The other survey looked at individual attitudes to protection of personal data and risk associated with use of social network services.

This survey report is part of the preliminary stage of a research degree at City University London to explore the range of issues associated with personal data on social networks so that areas for further study could be identified.

## **Methodology**

The two qualitative surveys were supplemented by interviews with academics, regulators and researchers. The surveys were delivered as online questionnaires designed and delivered using an academic licence for SurveyGizmo ([www.surveygizmo.com](http://www.surveygizmo.com)). SurveyGizmo was selected for its ability to formulate different question types, its analysis features and its ability to export results to other applications. The two surveys were:

1. A workplace survey of UK-based professionals responsible for information governance and data protection, and
2. A survey of a small sample of individual users and potential users to discover personal attitudes to protecting personal data on social networks.

The workplace survey was distributed via the following British Computer Society (BCS) special interest groups and other group lists:

- BCS Information Risk Management and Assurance LinkedIn Group
- BCS Information Security Specialist Group on LinkedIn
- BCS Law LinkedIn Group
- BCS Internet LinkedIn Group
- BCS Doctoral Consortium LinkedIn Group
- Data Protection and Security LinkedIn Group
- Information and Records Management Society LinkedIn Group

## Social Networks in the Workplace

- JISCMail Data-Protection
- JISCMail Records-Management-UK

Respondents were a self-selecting group. The principal concern was to keep the survey within the bounds of professionals responsible for information governance and data protection in UK-based organisations. The other survey was of individuals known to the researcher.

The results of the two surveys were exported to Excel for coding, sorting and filtering during the analysis stage. The responses to the survey were not attributable to any organisation or individual. This was to allow respondents to be open about their views on social networks and protection of personal data.

## Survey results

### Respondents and their organisations

Twenty-eight people responded to the personal survey and a total of 52 completed responses were received from LinkedIn and JISCMail discussion lists for the workplace survey. In the workplace survey the largest single group was members of the Information and Records Management Society (52%), the British Computer Society Information Security Specialist Group (15%), then CILIP and the Archives and Records Association (both 13.5%). Only two members of the National Association of Data Protection Officers responded. The preponderance of records managers, archivists and library / information professionals was reflected in the job titles with 13 Archivists or Records Managers. Nine respondents had 'Governance' and five had 'Data Protection' in their job titles. A further four were IT professionals and two were legal professionals.

The majority of workplace respondents worked in the public sector (including health and education) which accounted for 80% of responses. The remainder worked in the private sector (10%) or in consultancy (8%) and one person worked in the voluntary sector. The majority represented organisations that had 1,000 or more employees (67%). None worked in organisations of fewer than 10 people.

Most of the workplace respondents (58%) were employed by organisations that allowed the use of social networks in the workplace. Of these the majority did not have a written policy on use of social networks.

### Use of social networks in the workplace

Where organisations allowed staff to use social networks at work, most staff used Twitter (96%), Facebook (93%) and LinkedIn (71%). This selection was based on the top ranked English-language social network service, each with more than 80 million registered users. They were used for personal, professional, advertising and public information purposes – with considerable overlap between the categories.

## Social Networks in the Workplace

### Benefits

Workplace respondents identified the following benefits of using social networks in their organisations:

- Advertising and promotion
- Professional networking, sharing and collaboration
- Staff awareness and training
- Access to information

Advertising promotion, dissemination and sharing of knowledge were seen as benefits of social networks. Examples cited included: reaching younger audiences, marketing and promoting services, advertising events. It is seen as a rapid way of disseminating information to target audiences. One respondent suggested that they could help to break down information silos. Professional networking was the other major benefit identified by nearly half of the respondents. This included networking with clients, keeping up to date and forming communities of practice/interest.

Among those that do not use social networks at work, staff convenience, keeping staff happy and access to information were seen as potential benefits.

In the individual user survey respondents cited the following benefits:

- Keeping in touch with friends and family
- Easy communication with groups of friends or colleagues
- Professional networking and maintaining a professional profile
- Organising events
- Finding out what friends, family and colleagues are up to

### Risks

The following risks were associated with the use of social networks in the workplace:

- Reputation risk to the organisation if, for instance employees publish defamatory or damaging information on a social networking site.
- Liability for the actions of people posting on the site, especially if *“helping to promote (or failing to stop) an environment that is discriminatory/bullying”*.
- Accidental disclosure of information that could lead to loss of intellectual property. Confidential information could be disclosed with data protection of commercial consequences. Once disclosed, the data can be used inappropriately.
- Security breaches by exposing the organisation to malware for instance. Lack of awareness of security issues on the part of users was of particular concern. There are also capacity and service disruption issues related to use of social networks at work.
- Non-compliance with the Data Protection Act and other regulations. This particularly applies if the service provider is outside the UK and consequently personal data is transferred overseas.
- Time wasting during work was another concern. Staff members could be distracted by social networking during working hours.

## Social Networks in the Workplace

Respondents from organisations that do not allow use of social networks in the workplace were also concerned about the temptation for staff to waste time on social networks during working hours. Security and the risk of exposure to malware were also mentioned by several respondents, as was the impact of social networks on the bandwidth or other aspects of system capacity. Inappropriate use and compromised privacy or confidentiality were also mentioned, as was reputational risk. Higher organisational or government policy were also quoted as reasons for not allowing use of social networks.

Some respondents in non-user organisations said that they could be persuaded to allow use of social networks, provided there were guidelines in place to prevent abuse and time-limited access to prevent time-wasting. Several respondents felt that if there was a good business case for use of social networks e.g. to advertise events or as a public information service, they would be allowed.

There was a final point about risk from one workplace respondent:

*“Like all issues involving the internet, there are risks that are being run now that have not got proper mitigation in place to minimise those risks. Each facilitator and their employees have to assess those risks and put reasonable steps in place to protect the interests of firstly the employer and secondly to retain the convenience of the employee.”*

Respondents to the individual user survey were principally concerned about personal risks:

- Harassment (e.g. stalking)
- Identity theft and fraud
- Abuse of personal data by advertisers (e.g. spamming)
- Loss of privacy (where personal data is shared beyond the original intended audience)

### Protecting personal data

Among workplace respondents a variety of measures was considered for protecting personal data on social networks. When asked what precautions should be in place most workplace respondents envisaged several methods being used in concert.

Educating users or providing guidelines on use of social networks were the most frequently mentioned precaution. This ties in with ensuring that individuals are aware of their responsibilities for appropriate use of social networks:

*Employers should ensure that staff receive adequate training in the use of SNS [Social Network Services] and there is clear guidance on acceptable personal and business use*

*Staff need to be briefed clearly about the implications of sharing their personal information*

*...if access is to be allowed, then a full policy statement on who is responsible for what needs to be in place and agreed*

Monitoring and moderation of social network sites were mentioned as possibilities, although there may be some privacy issues attendant on this approach.

## Social Networks in the Workplace

Technical measures such as software filters, time-limited access and other security measures were also suggested. Some felt that the service providers should take greater responsibility for data security:

*the providers of websites could do more to promote security, and make the most secure setting the default, rather than something you have to select*

Two respondents mentioned better regulation or enforcement of regulation, which is dealt with later on, in the context of the Data Protection Act.

When it actually came to implementing precautions, educating users and providing guidelines or policies on use of social networks were the most frequently-mentioned measures. Some organisations already restrict access according to specific sites that are approved for work purposes.

One person mentioned encryption as a way of controlling access to personal data and several respondents suggested that informed consent should be required for disclosure of personal data or for changes to privacy settings of social network systems. Others felt that personal responsibility was the issue: *“we need to rely on the individual’s common sense and basic awareness of privacy rights to create social networks that are self-governed and self-policed”* and *“individuals should take responsibility for their actions”*. This could tie in with: *“more awareness for users regarding the implications of entering personal and sometimes sensitive personal data”*, *“educating and enabling users to look after their information responsibly”*, and *“making staff aware of their responsibilities when using social networks.”*

Individual users suggestions fell into two main groups:

- Personal responsibility for what personal data they reveal on their social network profiles and secure passwords
- Social network providers should take responsibility by implementing better privacy options, segregating the different groups an individual may be a member of, and alerting users when someone accesses their profile.

### Data Protection Act

Many respondents felt that the UK’s Data Protection Act (DPA) was ineffective or only partially effective for protecting personal data on social networks. This reflects an earlier interview with an expert who suggested that the Section 30 (domestic use) and Section 36 (freedom of the press) exemptions excluded social networks from the provisions of the Act. Service providers outside the UK were seen as a barrier to effective implementation of the DPA: *“most social networks go way beyond UK/EU boundaries and the data flies all over the world”* and *“the issue is jurisdiction – why should American firms care about our laws when what they are doing is perfectly legal in their country?”* Another suggested that *“most service providers are based outside the EU, making assertion of rights under DPA ineffective”*.

Lack of enforcement was seen as another factor limiting the effectiveness of the DPA. *“Not effective unless enforced”*. As one respondent pithily said: *“show me the prosecutions”*. Others said *“[The DPA] isn’t really enforced strongly and the fines are relatively small”* and *“the penalties are a low threat compared to the benefits of stealing identities”*.

## Social Networks in the Workplace

Several respondents saw user awareness as a key issue, without which legislation is ineffective: *“what is lacking is education of people as to how their information may be used/stored”, “[The DPA is] not very effective as many users are ignorant of protection of their personal data” and “the public ends up in charge of their own protection rather than the site providers. As most people don’t have a knowledge of the DPA, this is a concern”*. Another saw it as an issue of personal responsibility: *“its effectiveness is limited by the fact that people putting up personal info might be construed to be consenting to the distribution of their information”*.

There was also a concern that the speed of technological change made it difficult for legislation to keep up: *“I think the DPA is lacking – it’s not being adapted or updated to cover emerging technologies”*.

Finally, one respondent pointed out that *“there is a mismatch between public concerns when personal data is lost by an organisation, and the degree of personal data that individuals are willing to post on SN [social networking] sites”*.

In contrast, some respondents felt that the Data Protection Act was an effective tool for protecting personal data on social networks or that the situation was improving because of *“increased enforcement powers of the ICO”*. In the words of one respondent: *“the ICO has the teeth to prosecute the employer for breaches by those it permits to use social networks on the employer’s website”*. A number of areas for improvement were identified:

*“The problem is understanding, application and enforcement – particularly of the individual as a data controller and the limits of the ‘domestic purposes’ exemption”*

*“I think it is effective, however [I] do think that consent should not be implied”*

*“I think it’s just about adequate, but public education on the subject is rather limited. The developers of the social networks need to make it clearer about who will see your personal details and easier for users to specify their own restrictions”*

*“The Act is fine, but there is some catching up to do in terms of its application”*

## Future developments

Some respondents felt that developments in the following areas might affect the use of personal data on social network sites in the next two years:

- Technical
- Managerial
- Legal and Political
- Social and Behavioural
- Economic and Market

The speed of technical change may influence other factors such as improved security measures, possibly applied by the service providers. Emerging technologies such as cloud-based services may continue to develop, because *“institutions are becoming more reliant on this technology”*. There may even be the *“development of a private cloud for the public sector”*. Another respondent suggested that the *“proliferation of smart phones and tablets will greatly increase the use of social*

## Social Networks in the Workplace

*networks*". There may also be developments in the exploitation and use of personal data: *"the need to accept cookies is one area where there may be a rethink on access in some organisations"*. Increased data mining is seen as a general threat or as a specific risk to firewall security.

On the management side, at least one organisation is currently reviewing its policy on new and emerging technologies. One respondent foresaw: *"an increased use of social networking sites as a means of corporate communication and data sharing"*.

Legal and political changes ranged from war (although it was not clear whether the respondent meant cyberwar, economic war, or direct physical combat) to regulatory issues. Some foresaw increased regulation (including new laws and regulation) or improved enforcement of regulations. For instance, the forthcoming changes to electronic commerce regulations, revision of the European Data Protection Directive, new Federal Communications Commission regulations in the United States, and more stringent data privacy laws might all be influences. Others thought that increased non-compliance would be the issue. One felt that *"court cases which may take place and provide legal precedents may help to shape future legislation in this area"*.

Social and behavioural influences such as *"more acceptance of it [social networking] as a business tool, but with social overtones"* and *"recognition by people that they have little control over the huge portfolio of data they may have shared and published over many years on these sites"* were also considered.

Social networking for marketing purposes may increase over the next two years. For instance *"social search and more blatant targeted marketing may change attitudes amongst users"*.

## Conclusion

While individual users and potential users of social network services were concerned about protection of personal data, the perception among some workplace respondents was that risk to the organisation was of primary concern. In other words protection of personal data was not the main issue in use of social networks in the workplace, nor was it thought to be the role of the average organisation to protect personal data on social networks. The following issues were highlighted by the two surveys:

- Mixed views about the efficacy of data protection legislation as a means of regulating access to personal data
- Concern about lack of enforcement or difficulty of enforcement of data protection legislation across national boundaries
- The need for social network service providers to be more open about what they do with personal data, and defaulting to more secure settings
- The need for greater education and awareness of the risks associated with posting personal data on social networks and the need for individuals to take responsibility for protecting their own personal data

## Social Networks in the Workplace

Possible next steps for this study are to:

1. Look at the privacy policies of social network service providers and to examine the degree to which they comply with the Data Protection Act
2. Examine the policies of UK employers on the use of social network services in the workplace. This might start with an initial review employers' policies gathered in the Online Database of Social Media Policies<sup>1</sup>.
3. Conduct case studies to investigate use of social networks services in the workplace and to study ways in which personal data is handled and protected
4. Investigate attitudes to social network service use in the workplace by means of a quantitative survey. This might be focused on a specific sector such as public sector organisation using these services for public information, or commercial organisations that use social networks for promoting their products and services.

### Acknowledgements

My thanks to David Bawden, Professor of Information Science at City University for his guidance, to friends and colleagues who completed the questionnaire survey, and to the chairs of the professional groups that allowed me to post a link to the workplace survey on their discussion lists.

---

<sup>1</sup> <http://socialmediagovernance.com/policies.php>