City Research Online

City, University of London Institutional Repository

Citation: Haynes, D. (2011). Social Networks in the workplace - some data protection issues. Free Pint,

This is the published version of the paper.

This version of the publication may differ from the final published version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/5914/

Link to published version:

Copyright: City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

Reuse: Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

City Research Online: http://openaccess.city.ac.uk/ publications@city.ac.uk

FreePint
Supporting the value of information in your enterprise

Social Networks in the workplace - some data protection issues

Thursday, 1st December 2011

By **David Haynes**

Employers are under pressure to realise the benefits of social networks in the workplace. Recent discussion on one of my LinkedIn groups highlighted this and emphasised many of the positive aspects. Consumer-focused marketing organisations and information-intensive industries are obvious beneficiaries of social networks. Increasingly public authorities and charities are using them for campaigning and informing the public. Previous FUMSI articles have described some of the benefits of social networks in the workplace. These include use for:

- Providing information
- Keeping track of emerging trends
- Establishing relationships with customers
- Educating or informing the public
- Researching the market
- Building communities (of users or customers).

Risks associated with social networks

However there are risks. My own research identified some real concerns about the lack of protection of personal data. In a survey conducted in April 2011, users were typically concerned about loss of privacy and misuse of personal data. For instance, searches or messages posted in a private capacity may be exposed inadvertently to scrutiny by workplace colleagues and employers. One respondent was concerned about ads for menopause remedies that popped up on her screen every time she logged onto her social network during her lunch hour at work. In 2010 the Wall Street Journal started publishing a series of articles about the way in which social networking services use personal data to generate advertising revenue. This has already led to changes in the practice by some service providers.

Employers were concerned about potential damage to their organisations. In the survey the following three areas where highlighted:

- Reputational damage can occur if members of staff use social networks to make derogatory comments about customers, colleagues or rivals.
- Time-wasting by staff and distractions caused by using social networks during working hours.
- Security and the vulnerability to malware imported via social networks.

Regulating access to personal data

The survey went on to explore ways of managing use of social networks at work. Many respondents felt that enforcing the Data Protection Act was not an effective means of protecting personal data in this context. Section 36 of the Act exempts domestic use of personal data and one interpretation is that social networks fall into this category. However it was also argued that use of social networking services in the workplace is not exempt under Section 36. Another concern about the Data Protection Act is that the social network service provider may not have a UK presence, making it difficult to enforce the Act.

An alternative to legislation is to educate users. This was seen as one of the most effective ways of protecting individuals and organisations:

"Employers should ensure that staff receive adequate training in the use of SNS and there is

clear guidance on acceptable personal and business use."

Service providers can also be encouraged to set defaults to higher levels of privacy when users join a service. Users then have to opt in to sharing their personal data more widely than their immediate circle of contacts. This is in line with the recently implemented ePrivacy Directive, where informed consent is an important principle. One commentator has already suggested that there should be standard policies for privacy settings along the lines used for intellectual property with the Creative Commons.

One argument is that it is impossible to regulate the internet, so why not leave it to the market to evolve a way of working? Lawrence Lessig suggests four regulatory modes: law, market, architecture and norms. He suggests that building privacy protection into the architecture of information system will provide some protection, an idea taken up by the UK Information Commissioner's "Privacy by Design" initiative. Lessig also discusses norms which are evolving for the web environment. There will be different norms which apply to workplace and to personal use of social networks. Some of the norms that have already emerged for social networking include: no flaming, no spamming, no stalking ... Lessig goes on to say that a combination of regulatory modes will be needed and suggests that depending on legislation alone is not sufficient because of the territorial limits of law enforcement and lack of international coordination.

A manager's response

How does this affect information managers' work? In developing policies for use of social networks in the workplace, the following should be considered:

1. Protecting the privacy of your staff
2. Protecting the privacy of your customers
3. Managing reputational risk
4. Managing risk to your infrastructure
5. Protecting against data loss.

Some organisations have made considerable progress in developing policies for use of social networking services in the workplace. This is often as part of a wider information governance infrastructure, or organisational information policy. Examples of the measures included in these policies include:

- Educating the staff about safe behaviour on the internet – by means of briefing sessions, training and staff induction sessions.
- Ensuring safety of targeted users / customers.
- Ensuring that the IT system is secure and that encryption and other technologies are used where appropriate – particularly important where laptops are used outside the office.
- Guidelines on acceptable use with appropriate checks and restraints to ensure accountability and to discourage abuse of the service.

Further research will look at ways in which social network policies are implemented in the workplace.

Conclusion

Social network services are increasingly important tools for marketing and promotion. The focus of this research has been on external social network services, but many of the same principles could be extended to collaborative working environments such as SharePoint and cloud-based systems such as Huddle. Further research is also needed to look at ways in which social networks are used in the workplace.

Organisations cannot afford to wait for emerging social norms to regulate access to, and use of, personal data on social networks. Some of the measures described in this article provide a starting point for an organisational policy on use of social networking services.

Item URL: http://web.freepint.com/go/blog/65510
Printed: Friday, 17th April 2015

© 1997-2015 FreePint Limited