INTERVIEW

SOCIAL NETWORKING & CONFIDENTIALITY

THE LEGAL ANGLE

By Vikram Shroff & Harshita Srivastava

In view of the phenomenal growth in social networking platforms over the past decade and the ability to provide one of the biggest questions employers are facing these days is whether employees should be allowed to use social networking websites. Sites such as Facebook, Orkut, MySpace, Linkedin, hi5, Twitter and YouTube have created new means of business networking - expanding from a few dozen connections to hundreds of friends, acquaintances and followers. Company branded Facebook pages, Twitter feeds and blogs have become popular. HR managers in the US rely heavily on these sites to source potential recruits and gain a better understanding of a candidate's personality. Social media is here to stay.

Only until about a few years ago, organizations were contemplating whether to allow their employees internet access or access to personal emails. The same now seems to be happening with social networking websites. It may soon be a norm for organizations to provide their employees access to social networking sites. Since lines between company and personal matters are getting blurred thanks to the technology revolution, employers and employees are advised to consider the following aspects to mitigate the risks.

Loss of confidentiality

Certain social networking sites aim at professional networking through the exchange of business related information, contacts etc. Although such networking offers potential benefits, users need to be mindful that information that they share on such sites become public knowledge. They need to ensure that they do not disclose their employer's proprietary information. While India is yet to have a codified law on confidentiality and non-disclosure, such disclosure by employees is likely to be in violation of the employment agreement or non-disclosure agreement signed by them.

Defamation

Employees may post messages (which may include offensive comments about their employer) without prior deliberation of the consequences. At times, such information may trigger a case of defamation, which is recognised as a criminal offence under section 500 the Indian Penal Code, 1860.

Violation of Right to Privacy

More and more employers feel the need to monitor the information that their employees post on social networking sites, especially during office hours. A recent survey in the US revealed that approximately 71% of companies monitor employees on social networking sites. Assuming an employer may not have a contractual right, this may lead to claims by employees for breach of personal privacy. In the case of Pietrylo vs. Hillstone Restaurant Group, (FDC, New Jersey), the issue of employee's privacy rights on social media sites has been elaborately discussed and it was held that the employer cannot access such sites by coercing an employee to share his password.

Liability / reputational risk

Employees may use such sites to view or upload objectionable, illicit or offensive contents. This may be in violation of the organization policy or may offend co-workers, or may lead to harassment claims. The employer could also be held liable for failing to provide a healthy working environment, resulting in a loss of reputation.

Data theft

Certain social networking sites convince the users to post individual details on the web such as personal/ official contact information, details of employment, profile, salary, etc., thereby exposing to a risk of data theft and potential targets to hackers to commit fraud and launch spam and malware attacks.

Loss of productivity

While permitting access, employers need to be conscious about possible reduction in efficiency and productivity. Not to mention that extended hours spent by employees in office may lead to overtime claims.

Certain best practices

Employers are well advised to be proactive and create a policy framework for use of social networking sites. The survey mentioned earlier also found that 59% of organizations maintain a social media policy. The policy may include allowing time-based access (including during and after business hours), imposing limits on its usage, employer's right to monitor, etc. The policy should also include guidelines to ensure that (i) visiting such sites does not interfere with work commitments (ii) personals blogs have disclaimers on the lines that that the views expressed do not belong to the employer, (iii) information published does not breach the provisions of any confidentiality or non-disclosure agreement, (iv) employees do not defame and remain respectful of the company, its employees, clients and competitors, and (v) an agreed process is followed for blogging for the company or operating certain accounts. Care must be taken as excessive restrictions may not go down very well with the employees.

On a tactical basis, some companies allow access to social networking sites only on select computers that are outside the organization's networking environment with limits on usage or time to check the indiscriminate abuse of access. It is also recommended that training programmes should be conducted regularly to create internet security awareness amongst employees. Employees may need to be reminded from time to time that their web activities are being monitored.

Conclusion

There is no doubt that companies who are able to make effective use of such sites to enhance the brand awareness, implement marketing strategies, increase promotion of goods/ services, etc. are likely to gain a better online presence. Employers, who are careful and are able to clearly define the use of such social networking sites, may reap its benefits in the long term. As its said, a stitch in time saves nine!

Vikram Shroff heads the HR (Employment & Labour) Law practice group at Nishith Desai Associates, a research-based law firm. Harshita Srivastava is part of this group. Their views are personal.