Social media now part of the workplace environment

Notwithstanding the above, many employers have embraced social media as a medium for communicating with employees and encouraging employee engagement, including establishing private Facebook groups for their employees or creating internet chat sites where employees and customers can interact. Facebook and Twitter and, to some extent, Wikipedia, present valuable advertising tools, providing a free and instantaneous method of communication with a national and international online audience, and sites such as LinkedIn enable employees and employers to network with existing and potential customers.

In a relatively short period of time, social media have changed the way people interact and communicate as well as how they work and from where. Whether it be a simple vent of frustration on Facebook or a seemingly humorous prank posted on YouTube, an understanding of social media and work practices is key to ensuring that employees and employers are informed and mindful of the ramifications of inappropriate use of online social forums. Employers today must understand the potential uses and abuses of social media.

Note

1 The authors would also like to acknowledge the assistance of Ryan Zahrai in preparing this article.

Rakhi Jindal
Nishith Desai Associates, Mumbai
rakhi@nishithdesai.com

Gowree Gokhale
Nishith Desai Associates, Mumbai
gowree@nishithdesai.com

Vikram Shroff
Nishith Desai Associates, Mumbai
vikram@nishithdesai.com

The Indian legal position on employee data protection and employee privacy

Historically, the concept of data protection and privacy has not been addressed in any Indian legislation. In the absence of specific legislation, the Supreme Court of India in the cases of *Kharak Singh v State of UP*, AIR 1963 SC 1295 and *People's Union of Civil Liberties v the Union of India* (1997) 1 SCC 318 recognised the 'right to privacy' as a subset of the larger 'right to life and personal liberty' under Article 21 of the Constitution of India. However, a right under the Constitution can be exercised only against any government action. Non-state initiated violations of privacy may be dealt with under principles of torts such as defamation, trespass and breach of confidence, as applicable.

There are certain statutes and regulations in India which indirectly recognise the right of privacy in special categories, such as the prohibition on the publication of names of children involved in proceedings under The Children Act, 1860 and the requirement to maintain the confidentiality of human subjects of medical research under the guidelines published by the Central Drugs Standard Control Organisation. The labour specific legislations of India do not contain any provision with respect to protection of employee data or privacy of employees.

Law on data privacy and its effect upon employers

The Information Technology Act, 2000 ('IT Act') is the only legislation which has attempted to address the issue of data protection and privacy. Section 43A provides for the protection of sensitive personal data or information ('SPDI') and section 72A protects personal information from unlawful disclosure in breach of contract. The government has recently introduced certain rules ('Rules') under the IT Act which, read along with section 43A, set out the compliances which need to be observed by an entity which collects or stores or otherwise deals with SPDI (such as passwords, financial information, health conditions, sexual orientation, medical records and biometric records).

Employers collect SPDI of their employees for various reasons such as for selection processes, record retention purposes, employee evaluations or other legitimate business purposes. As such, employers need to be mindful of the compliances relating to SPDI and the related liability.

In case an employer is negligent in implementing and maintaining 'reasonable security practices and procedures' for the protection of the employee's SPDI, it may result in 'wrongful loss or wrongful gain' to any person. In that case, the employer is liable to pay compensation to the relevant employee. The aggrieved employee could approach an adjudicating officer appointed under the IT Act where the compensation claimed is up to INR 5 crores (approximately US$100,000) or the appropriate civil courts where the compensation claimed is above INR 5 crore.

Compliances in relation to SPDI

The IT Act sets out various parameters and compliances for an employer while dealing with employee SPDI.

- *Nexus* – SPDI should only be collected where there is a need to collect such information. For example, a company which is involved in disposing of hazardous wastes may need to collect very detailed medical records of its employees to be used in case of mishaps – it is easy to see why such records are needed by the company. The question that next arises is how long the data may be retained post cessation of employment. The Rules state that SPDI may not be retained longer than is required for the purposes for which it was collected or as may be prescribed under law.
- *Opt in and opt out* – Specific written consent (including via electronic modes) should be taken from the employees prior to collection of the SPDI whereby the employees are made aware of the requirement to collect the information, the specific items of SPDI being collected, the intended recipients of the SPDI and whether the SPDI would be onward transferred. There should also be an opt out option available to the employees.
- *Privacy Policy* – Employers should have a well documented privacy policy as per the requirements of the IT Act which should also be available on the employer's website.
- *Access* – The employees should be allowed to revise and correct deficiencies in the information.
- *Transfer* – SPDI can only be onward transferred (within or outside India) where specific employee consent has been taken (unless such transfer is mandated by law) and provided the transferee adheres to similar levels of data protection as mandated under the IT Act. The data collector may transfer SPDI outside India provided the transferee adheres to similar levels of data protection under the IT Act.
- *Reasonable security practices and procedures* – The employer should maintain 'reasonable security practices and procedures' to protect the SPDI. Such reasonable security procedures may either be agreed to upfront between parties (such as by way of appropriate disclosures in the employee manual) or may be as mandated by law or in the absence of both, as is recommended in the Rules. The Rules have the International Standard IS/ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management Systems – Requirements'.

In light of these requirements, it is extremely important for organisations to have well documented policies on employee data protection and employee privacy. Appropriate audit mechanisms should also be enforced. The documentation to be executed by new recruits should be analysed to ensure compliance with these requirements. With respect to existing employees, it is important to obtain necessary consent for future use and transfer of SPDI. It is common to see clauses on employee consent for collecting and sharing data being introduced in employment contracts and company policies. It is also good practice to conduct an audit of employee data at the time of exit to determine what data may be legitimately required such as for social security or pension purposes and what data needs to be expunged.

Impact on multinational companies

Several multinational companies process their employee data at a single location in the world and the data is made accessible to subsidiaries located across the world. Hence, when putting their data protection systems in place, they need to take into account data protection laws of all the relevant countries. The provisions of Indian laws as discussed above may pose some unique situations and requirements which have to be adhered to.

In some cases the foreign entity may not have a local presence in India but may merely

outsource certain activities (such as the payroll related activities) to India. In such cases, the Indian outsourcing vendor is not required to comply with the Rules with respect to the collection and transfer of information but will be required to comply with the other Rules with respect to the need to implement and maintain a privacy policy and reasonable security practices and procedures.

What if no SPDI is being collected?

The specific requirements under the IT Act as stated above are only triggered where SPDI is collected. However, employers need to be careful where any kind of sensitive information is being collected. For example, even if the specific requirements under the IT Act are not triggered, it is possible that the employer may face liability under common law. For example, though in a different context, the Supreme Court in 1999 (ie, before the Rules were introduced) in the case of *Mrs Neera Mathur v Life Insurance Corporation of India, and Anr* held that a requirement for female applicants to furnish details of pregnancies at the time of appointment, amounted to breach of privacy.

It is for this reason that some employers may choose to be compliant with the Rules as a matter of good practice, even if the Rules do not directly apply.

Employee surveillance

The number of outlets and the effectiveness of the media, along with the technology with which an employee is able to communicate and transfer information, is greater today than ever before. While employee surveillance has not been dealt with under the IT Act, these issues have assumed great importance particularly in light of the rapidly growing information technology and outsourcing industry in India.

Employers may face critical issues in terms of data leakage, intellectual property violations, defamation and a host of other issues in cases of misuse of such means of communication by an employee. For instance, if an employee downloads pornographic material on an office laptop and circulates such material to other employees, such action may be construed to be a case of sexual harassment and the employer may become liable for creating a hostile environment.

There are various ways and means in which employers monitor their employees, including the recording of telephone calls, monitoring of e-mails and surveillance cameras. However, the controversial and legal issues associated with employee monitoring cannot be ignored. The Supreme Court has held in the case of *People's Union For Civil Liberties v Union of India* that a telephonic conversation in private without interference would come under the purview of right to privacy as mandated in the Constitution and that unlawful means of phone tapping are invasions of privacy. While the constitutional right to privacy under Article 21 of the Constitution is only available against state action, in the absence of legislation in this matter, the same principle may be extended to the private sphere.

As such it is of critical importance that balance be maintained between the employer's legitimate requirement to obtain data and monitor employee activities to safeguard company interests, and the employee's genuine concern for respect of privacy.

Conclusion

While the Rules are fairly new in India, the issues relating to employee data protection and privacy will be thrust to the forefront in the coming years. It is essential for employers to understand the nuances of these issues and be prepared to be compliant with the regulations as well as to protect the interests of the company.

The Indian Government is proposing a comprehensive legislation on the 'Right to Privacy' ('Privacy Bill'). A working draft of the proposed Privacy Bill includes a provision whereby an employer does not need to obtain written consent of an employee where employee information is being collected for the purpose of and in connection with employment. It remains to be seen whether the Privacy Bill goes through. In the meantime, employers should gear towards compliance with the Rules.