ARTICLE

Employement Laws and Data Protection: A Global Perspective

S. Ravishankar, FCS
Company Secretary in Practice
ASR & Co., Bengaluru
rslegaleagle@gmail.com

Social Media is gaining popularity and immense significance in India for conducting business and as a main platform for socialising with friends, family and also plays a major role in the promotion of business. Use of social Media for personal and business is so much entangled with each other that it is difficult to identify which laws would be applicable for these use of social media and how and what would be an unlawful use of the same.

On account of wide spread use of the Social Media by the employer-employee community in India, it becomes important to understand how social media could be used in a manner serving the best interest of the employers and at the same time not attract any legal consequences. The primary focus of this article would be to understand the attitudes of the global employers towards the use of employee Data collected through the social media and otherwise, legal pitfalls in their use and the international practices.

While presently there is no specific statute which governs DATA privacy in India, the protection in this regard is largely based on the Constitutionally guaranteed "Right to privacy". Although the concepts of "privacy", "sensitivity", "personnel information" and "anti-discrimination" are recognised in India, the laws pertaining to social media is still in its infancy and emerging phase. Therefore, we have to be guided by the international development in this regard.

Right to life and personnel liberty are fundamental rights guaranteed by Article 21 of the Indian Constitution as decided by the Supreme Court in the case of *Kharak Singh v. State of UP* (AIR, 1963 SC 1295). However the jurisprudence of this revolves around rights of citizens against illegal invasion of privacy by the government agencies and not by private organizations and hence the invasion of privacy on social media sites, and the risk associated with accessing publically available information is tricky and risky.

According to statistics the total number of social networks users in India is expected to be around 145.6 Million by the end of the year and about 224.2 Million by the end of 2018. Facebook is estimated to have around 100 million monthly active users out of which 80% use it through their mobile phones. Twitter is estimated to have around 33 million monthly users, Linkedin around 26 million users and finally Pinterest around 5.5 million users.

The use of social media by employers in India therefore raises questions as to what laws and rules will apply for workplace confidentiality and loyalty, and how they are balanced against the "freedom of expression" guaranteed by the Constitution.

Articles 19 (1) (a) and 21 of the Constitution do not patently grant right of privacy, but courts in India on many occasions have held that the right to privacy is a part of the fundamental rights of every citizen along with freedom of speech and expression, but this right is enforceable only against government agencies and bodies and not against private violations and invasions. Non-state invasions have to be necessarily governed by the general law of torts such as defamation, breach of confidentiality and so on and so forth. Currently the only relevant laws in India concerning DATA Protection are the Information Technology Law (IT Act 2000) read with the "Reasonable Practise and Procedures and Sensitive Personal Data or information Rules, 2011 (Data Protection Rules), the Indian Contract Act, 1872 and the general principals of Law of Torts. The IT Act is the only Act which addresses the Data

> The use of social media by employers in India therefore raises questions as to what laws and rules will apply for workplace confidentiality and loyalty, and how they are balanced against the "freedom of expression" guaranteed by the Constitution.

Protection & privacy. Section 43A of the IT Act, states that "*when a corporate body is negligent in implementing and maintaining reasonable security practises and procedures in relation to any sensitive personnel data information that it possesses and such negligence causes wrongful loss or wrongful gain to any person, the entity will be liable to pay damages by way of compensation to such affected person".*

Similarly, an employer who fails to properly implement security practises, resulting in wrongful loss or wrongful gains to any person could be liable to pay compensation to the aggrieved person. The adjudicating office appointed under the IT Act is empowered to award compensation up to INR 5 crores. Under the circumstances let us now examine the Employer- Employee relationships & DATA Protection in India when compared with Singapore, US & the UK through the following Table.

INDIA	SINGAPORE	US	UK
DATA Protection: An employer is required to obtain employee consent prior to collection of SPDI (Sensitive Personnel Data and information). Employees have the right to withdraw such consent at any point in time and require that the SPDI be returned or destroyed. Employees shall also have the right to review the information provided and ensure that any personal information, SPDI or other information found to be inaccurate or deficient is corrected.	The PDPA (Personal Data Protection Act) requires organisations to notify the employee of the purposes for which it intends to collect, use or disclose personal data and obtain the consent of the employee for the same. However, some exceptions to this requirement are available, for example, where the collection, use or disclosure of an individual's personal data is: (i) necessary for 'evaluative purposes' (i.e. determining the suitability, eligibility or qualifications of the individual for employment; promotion or continuance in employment; or removal from employment); or (ii) reasonable for managing or terminating the employment relationship. An employer who has sufficiently provided a general notification to employees on the purposes for which their personal data may be collected, used and disclosed need not notify employees of the same purpose prior to each time that it engages in such activities. Employees may request access to their personal data that is under the employer's possession or control ("access request"). An employer need not provide the requested personal data if it is in respect of one of the exceptions in the Fifth Schedule of the PDPA (e.g. it is opinion data kept solely for an evaluative purpose). In addition, an employer shall not provide access where the provision of such data could reasonably be expected, amongst others, to threaten the safety or health of another individual, cause harm to the safety or health of the requestor, or to reveal personal data about another individual	Employee data protection laws in other countries are often much more restrictive, though the U.S. is trending toward more data protection obligations with an assortment of data protection laws that regulate the collection, use and transfer of employees' personally identifiable information ("PII") and personal health information ("PHI"). These laws are not limited to protecting active employee information, so employers' obligations extend to former employees, job applicants, independent contractors and other non-employee groups whose personal information they may obtain (such as customers). There are five primary federal data protection laws that impact the employment relationship: the Health Insurance Portability and Accountability Act ("HIPAA"), which dictates under what circumstances and to whom PHI may be released; the Genetic Information Nondiscrimination Act ("GINA"), which covers genetic information; the Americans with Disabilities Act ("ADA"), which limits when an employer may obtain medical information, how such information may be used, and disclosure of such information; the National Labor Relations Act ("NLRA"), which prohibits employers from interfering with workers' rights to engage in concerted activity, including such activity through social media, and the Fair Credit Reporting Act ("FCRA"), which applies to those who use consumer reports, including background checks conducted on applicants and employees. Another federal law, the Privacy Act, limits the type of information that federal government employers may keep on their employees. Additionally, most U.S. states have enacted some form of data protection legislation that often impacts the employment relationship, though these states impose a wide range of requirements. Almost all states have enacted laws requiring notification of security breaches	Employers must comply with the Data Protection Act 1998 (DPA) when processing employee data. In particular, data must be processed fairly and lawfully, for specified and lawful purposes, and adequate security measures must be in place. There are restrictions on transferring data outside the EEA. The Information Commissioner can impose fines of up to £500,000 for serious breaches of the DPA. Employees are entitled to make a subject access request (subject to payment of a £10 fee). Employers then have 40 days to tell the employee whether their personal data is being processed, the purposes for which data is processed and to whom it is disclosed, and to provide a copy of all personal data that is held unless this would involve "disproportionate effort".

		involving PII and many have enacted laws requiring companies to destroy, dispose, or otherwise make PII unreadable or undecipherable. Some states have laws providing expanded protections to PHI. More recently, a significant number of states have enacted employee social media privacy laws.	
Pre-Employment Checks: There is no restriction upon the employer to carry out pre-employment checks. In case the employer collects employee's SPDI, (SENSITIVE PERSONNEL DATA & INFORMATION) the requirements of the Data Protection Rules need to be complied with which is clear that unless such information is required for a lawful purpose connected with a function or activity it cannot be collected. While dealing with the SPDI it becomes necessary for the employer to obtain prior written consent of the employee, allow the employee to review and correct the information and maintain reasonable.	An employer may collect, use or disclose the personal data of a prospective employee for the purposes of carrying out pre-employment checks, if the prospective employee is notified of such a purpose on or before such collection, use or disclosure, and gives his consent for the employer to do so. Alternatively, if the collection, use or disclosure of personal data for the purpose of conducting pre-employment checks falls within any of the exceptions under the Second, Third or Fourth Schedule to the PDPA (as applicable), or if the information is publicly available, the prospective employee's consent need not be obtained. In particular, the collection, use or disclosure of such personal data may be regarded as necessary for evaluative purposes.	There is no Federal law requiring current or former employees' access to their personnel records. There are, however, Federal laws regulating employee access to medical records, records of exposure to hazardous substances, and consumer reports. The Occupational Safety & Health Act ("OSHA") authorizes employees who may have experienced workplace exposure to a toxic substance or harmful physical agent access to their medical records and records of such exposure. The Fair Credit Reporting Act ("FCRA") grants applicants and employees access to their consumer reports, which is defined to include background check reports. Employee access rights to their personnel and medical records are guided by State law, and vary widely from State to State. In some States, employees have no legal right to these records. Many States, however, have some type of law authorizing access to personnel and/or medical records and outlining the terms of such access, though various Federal and State laws regulate the process for conducting such checks and how they may be used. A federal law, the Fair Credit Reporting Act ("FCRA"), requires employers to obtain written consent from applicants or employees before obtaining background reports from any company in the business of compiling background information. If an employer thinks it might take an adverse action against an applicant or employee because of something in a background report, it must give the applicant or employee a copy of the report and a notice of FCRA rights. Some States and even localities have their own laws that offer protections for screening applicants and employees similar to, or even greater than, those afforded by the FCRA. Various Federal and State anti-discrimination laws prohibit checking the background of applicants or employees or using background report information when that decision is based on a person's protected status, such as race, national origin, color, sex, religion, disability, genetic information, age, or other characteristics protected under state law. An employer's neutral practice of disqualifying applicants or employees based on criminal or credit history may disproportionately impact minorities, and therefore violate these anti-discrimination laws if not job	Employers can carry out pre-employment checks, but it is good practice to limit this to checking information provided by the candidate. More detailed vetting may be appropriate where the role entails risks to the employer, clients, customers or others. Criminal records checks can be made through the Criminal Records Bureau. Different levels of disclosure are available depending on the nature of the job applied for, with more detailed disclosures available where candidates will be working with children or vulnerable adults.

		related and consistent with business necessity. Beyond this general anti-discrimination rule, the law varies by State on whether, and to what extent, employers may consider background check information — especially criminal or credit histories — in making employment decisions. Some states impose very few restrictions on inquiries into and use of an applicant's criminal or credit history, while others take a much more restrictive position. For example, in some states, employers are prohibited from checking applicant credit reports altogether or may be allowed to do so only for certain types of jobs. Some States prohibit employers from asking about arrests, convictions that occurred beyond a certain time period, juvenile crimes, or sealed records. Some States permit employers to consider convictions only if the crime is job related, and others allow employers to consider criminal history only for certain types of jobs.	
Privacy During Employment: Indian law does not envisage any restriction on the employer's right to monitor employee emails, telephone calls or use of computer systems. As a best practice, surveillance rights and procedures are ordinarily built into the employee handbook/policy manual, to mitigate any privacy claims. While use of social media provides many benefits to employers, employers must be cautious of certain risk associated with this approach. Employers may have to think more strategically about the entire recruitment process & the DATA Collection and the employee's private life. Information that is feely available and acceeable in public domain or furnished under the Right to Information Act, 2005 is excluded from the ambit of SPDI. To that extent the employer is free to collect & use the information during and post-employment. As per Article 14 of the Indian Constitution, a citizen shall not be ineligible for or discriminated against in respect of employment on any grounds like religion, caste, race, sex etc... In addition to this Article the "Equal Remuneration At", 1976 (ERA) prohibits discrimination on the basis of sex in matters relating to employment and hence care should be taken to ensure that use of information during employment obtained from social media for the purpose of hiring does not lead to violation of ERA.	Generally, an employer is entitled to monitor an employee's emails, telephone calls or use of the employer's computer system, insofar as the employee is notified of and consents to the purpose(s) of such collection of his personal data. Further, it may not be necessary to obtain the employee's consent before such monitoring, if this is for the purpose of managing or terminating an employment relationship, or necessary for any investigation or proceedings. The PDPA does not specifically allow or restrict the ability of an employer to control an employee's use of social media in or outside the workplace. However, the employer may control an employee's use of social media contractually, such as by providing for a social media policy which the employee is bound to abide by under the contract of employment Moreover, an employee would remain bound by a number of Singapore laws and regulations in relation to his use of social media, whether in or outside the workplace. These could include, amongst others: the laws of intellectual property and/or confidentiality; defamation; harassment; and internet content regulation.	Generally, employer are allowed to monitor e mails of the employees, with some exceptions. An employer is usually entitled to monitor employees' use of its email and computer system if it owns the devices and runs the network. Employee monitoring has, however, become more complicated by the surge of employees utilizing personal devices for work activities. Various Federal and State laws prohibit unauthorised access to employees' personal electronic devices and personal email even when accessed on the employer's device and network. Generally speaking, a broad workplace usage policy (particularly one that speaks specifically to these "Bring Your Own Device" and personal email issues) serves to protect an employer's right to monitor activity on its network. An employer planning to monitor should maintain such a policy and obtain employee acknowledgments that they do not have a reasonable expectation of privacy when using the employer's devices and network. Some employees may have additional protection from email and computer monitoring, such as those in the public sector who may have constitutional privacy rights and those subject to union contracts that may restrict the employer's right to monitor. An employer's right to monitor employee telephone calls is more limited. Under federal law, employers may monitor employee calls made "in the ordinary course of business," but cannot listen to or record calls it knows are of a personal nature. Some States have additional	Monitoring may be permissible if there is a good reason for it and it is a proportionate response to the problem it seeks to address. An employer will normally need to conduct an impact assessment, weighing up the purpose of monitoring against the adverse impact for employees or others, to judge whether monitoring is justified. If electronic communications are being intercepted the employer will also need to make sure that it complies with the Regulation of Investigatory Powers Act. Misuse of social media in or outside the workplace may amount to misconduct, which an employer can deal with in the normal way through its disciplinary procedure. Whether a dismissal is fair will depend on the damage or potential damage to the employer's reputation, whether the employer has a clear policy on the issue, and whether dismissal is proportionate (as well as whether a fair procedure has been followed).

		restrictions on monitoring employee telephone calls, such as requiring employers to inform the parties to the call that the conversation is being recorded or monitored. Generally speaking, an employer may limit employees' use of social media during working hours and how employees use social media regarding the employer's business. For example, an employer usually has the right to discipline an employee who violates company policy by harassing other employees on social media or disclosing company proprietary information on social media. But, an employer's control over an employee's use of social media is limited. Many State and local laws prohibit employers from disciplining employees based on lawful, off-duty activity on social networking sites unless the activity implicates the employer's legitimate business interest. Additionally, the National Labor Relations Act ("NLRA") protects employees' rights to engage in "concerted activity," which includes such activity on social media. The NLRA applies to union and non-union employers alike, so all U.S. employers must be mindful of their social media policies and practices so as to not infringe upon these NLRA rights. Employer access to private social media content is also limited. The Federal law prohibits employer access to private social media accounts without consent from the employee or applicant. Many States have password privacy laws that prohibit employers from even requesting social media user name and password information from employees and applicants. These laws usually provide exceptions for employers when investigating workplace misconduct or complying with applicable law.	
The laws are silent on the employer's ability to control an employee's use of social media in or outside the workplace. That said, social media policies are gaining popularity and are being included as a part of employee handbooks/policy manuals.			
DATA Protection Post-Employment As per the Data Protection Rules, any SPDI so collected can be retained & used no longer than it is required for the purpose for which it was collected or as may be prescribed under the Law. It is also a good practise to conduct an Audit of the employee data at the time of exit to determine what data would be legitimately required and what data needs to be expunged. In case the data is required after the employee's exit then the employer must justify its requirement and its usefulness and also take the employee's consent to retain and use such data.	Under Singapore law, restrictive covenants post-employment are *prima facie* void unless: (i) there is a legitimate interest that the employer seeks to protect; and (ii) they are reasonable in the interests of the parties and in the interests of the public. Restrictive covenants should be no wider than necessary to protect the legitimate interests of the employer and employee.	Most States follow the general rule that restrictive covenants are enforceable, provided they are necessary to protect a legitimate interest of the employer and are reasonably limited in duration, geographic scope, and the restrictions placed on the employee in pursuing his or her profession. The minority position — held most notably by California — prohibits the use of restrictive covenants in virtually all circumstances.	Employers will only be able to enforce covenants if they can show that they have a legitimate business interest to protect (such as confidential information or customer connections) and that the covenant goes no further than reasonably necessary to protect that interest. If the covenant is too wide in its scope or duration, it will not be enforceable. Restrictions usually last between three and twelve months, depending on the seniority of the employee and the nature of the interest to be protected.