Usage of Social Media by Employers to Collect Information on Employees

Canada has adopted a European-inspired non-fragmented approach to the collection of personal information in the private sector.

In 2000, the Federal *Personal Information Protection and Electronic Document Act* (PIPEDA) was enacted and intended to apply to every private sector employer that '*collects, uses and discloses personal information in the course of a commercial activity*'. PIPEDA applies to federal works and undertakings and to commercial transactions in every province, except those that have enacted 'substantially similar' privacy legislation. To date, of the thirteen provinces and territories in Canada, only Alberta, British Columbia, Manitoba and Quebec have enacted substantially similar privacy laws of general application. In 1994, Quebec had already introduced its *Act Respecting the Protection of Personal Information in the Private Sector* (the 'Quebec Act'), the first legislation of its kind in North America, as a direct response to the EU's directive on data protection. There is also the British Columbia Personal Information Protection Act (the 'BC Act') and the recently enacted Manitoba private sector privacy legislation, *The Personal Information Protection and Identity Theft Prevention Act* (the 'Manitoba Act'). The Alberta Personal Information Protection Act (the 'Alberta Act') is currently being revised after having been declared unconstitutional by the Supreme Court of Canada in the case of *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401.* In that case, the Court found that the privacy protection in the Alberta Act could not go so far as to prohibit a union from taking and publishing pictures of strike breakers, as this would violate the guarantee of freedom of expression under the *Canadian Charter of Rights and Freedoms*.

The phrase 'in the course of a commercial activity' is not precisely defined in PIPEDA. It is generally accepted that a commercial activity must have a transaction-based component, meaning it includes not only activities conducted in the normal course of business, but any particular transaction or conduct that has a commercial character.

Thus, PIPEDA has limited or no application to non-commercial organizations such as not-for-profit entities and charities. This creates a gap in Canadian law: non-commercial activities operating exclusively in a province that has not enacted privacy legislation are not regulated by PIPEDA (or any other privacy law for that matter). However, this void is largely filled by the common law applicable in each province and human rights legislation of general application.

PIPEDA defines ‘personal information’ broadly to mean any information about an ‘identifiable individual’, except for an individual’s name, title, business address or telephone number. Personal information also includes information that indirectly, through association of bits of information and through inferences, constitutes information about an identifiable individual. This definition is large enough to encompass a wide range of employment-related information, including the employee’s home address and phone number, social insurance number, identification number and security passwords, date of birth, income, personal interests and hobbies, prior work record, loan and credit information, criminal record, racial background, sexual orientation and medical record – clearly many of the things that one can find on a social media site.

PIPEDA essentially prohibits personal information from being collected, used or disclosed by an employer without the individual’s consent. Similarly, the Alberta, British Columbia, Manitoba and Quebec Acts require the obtaining of an individual’s consent for companies to use, collect or disclose personal information about that individual. Express consent is required where the information is likely to be considered sensitive, whereas implied consent is sufficient in all jurisdictions except Quebec, for information that is less sensitive. In Quebec, express consent is always required.

The Privacy Commissioner of Canada is the watchdog organism entrusted with ensuring compliance with PIPEDA. The Privacy Commissioner can investigate complaints of violation of PIPEDA, as well as audit the personal information management practices of an organization to ensure compliance with PIPEDA. However, the Privacy Commissioner cannot impose sanctions: it reports on violations or noncompliance, after which complainants or the commissioner may seek appropriate remedies before civil courts. In recent years, the Office of the Privacy Commissioner of Canada has argued in favour of stronger enforcement powers to allow it to properly fulfill its mandate.

Moreover, the purpose for which information is being collected must be clearly identified at the time that it is being collected and those who are responsible for collecting the information must be capable of explaining such purpose to the individuals whose information is being collected. Only information that is clearly linked to the identified purpose may be collected. A host of other requirements must also be met: the information must be accurate and individuals must be allowed access to this information and the opportunity to correct it, etc.

The question arises as to whether employers commit a privacy breach if they collect information that is posted voluntarily and publicly by potential or current employees. Canadian privacy law does not seem to distinguish between protecting personal information that has been made public versus information which has been collected, but kept private.

In fact, PIPEDA sets out ten general principles which organizations must follow when they collect, use or disclose data: Accountability, Identifying Purposes, Consent, Limiting Collection, Limiting Use, Disclosure and Retention, Accuracy, Safeguards, Openness; allowing Individual Access; giving individuals an opportunity for Challenging Compliance.

It can be argued that merely browsing through information on social media may constitute ‘collection’ of information. In British Columbia, the Information and Privacy Commissioner held that retailers who were viewing drivers’ licenses to verify for age or identity, were actually collecting personal information. Thus, an employer who browses through a potential employee’s Facebook profile on his phone during lunch, may similarly be ‘collecting’ this information just as would a human resources

department that created a file and downloaded all the candidate's social media information. However, under the Quebec Act, the mere act of viewing information does not violate privacy protection, unless the employer creates a file with the information obtained. Thus, inasmuch as information is consulted then discarded and not kept on file, pre-hiring screening of employees would not constitute collection of personal information under the Quebec Act but may do so in other Canadian jurisdictions.

The power of employers to monitor the use of social media by employees, or to use social media to gather information on employees, stems primarily from the management (and underlying property) rights of employers. For example, the *Civil Code of Quebec* defines a contract of employment as 'a contract by which a person, the employee, undertakes for a limited period to do work for remuneration, *according to the instructions and under the direction or control* of another person, the employer'.

Collection of information through social media may also be justified by the duties incumbent on employers to third-parties with respect to whom employers are vicariously liable for the acts of employees (breaches of confidentiality, damage to reputation, etc.) and also with respect to ensuring fair and safe working conditions pursuant to labour standards or human rights legislation.

Article by

Patrick L. Benaroche and Charif El-Khouri