ALEXANDER HOLBURN
ALEXANDER HOLBURN BEAUDIN + LANG LLP

YOUR **PERSPECTIVE** OUR **FOCUS**™

EMERGING ISSUES IN DISABILITY MANAGEMENT - PRIVACY: RIGHTS, OBLIGATIONS AND REMEDIES

(PREPARED FOR THE 2013 CANADIAN HEALTH AND WELLNESS INNOVATION CONFERENCE)

Article written by John Elwick

INTRODUCTION

An individual's right to privacy covers a broad range of activities. This paper will deal with the legal basis for the acquisition of such rights and will then focus on the application of maintaining those rights with reference to situations involving disability management.

SOURCES OF PRIVACY RIGHTS

The first of these rights are contractual and typically arise from collective agreements for both the public and private sector. Such agreements usually do not contain provisions that expressly address privacy and how it is to be protected. Instead, reliance is often placed on provisions in the collective agreement which require work rules to be reasonable and recognize the implied restrictions on management rights to protect the privacy of employees. In this context, the enforcement of the right to privacy is usually provided by an arbitrator in the course of an arbitration hearing. In a non-unionized context, privacy breaches by an employer could be dealt with on a common law basis by an employee commencing a constructive dismissal action after leaving employment.

The second source of privacy rights is statutory and is covered by both federal and provincial privacy legislation. At the federal level, there is the *Personal Information and Protection of Electronic Documents Act* ("PIPEDA"), which applies to federally regulated private sector organizations. Under this act "personal information" may only be collected, used or disclosed to an organization with the consent of the individual whose information is being requested or if such information falls within certain categories for which there are exceptions.

The *Access to Information Act* and the federal *Privacy Act* are statutes which restrict information collection, use and disclosure in the federal public sector.

On the provincial side, we have the *Freedom of Information & Protection of Privacy Act* ("FIPPA") governing public sector organizations in British Columbia which limit the collection, use and disclosure of personal information. Professional regulatory bodies are covered by FIPPA and the statute also applies to any private sector organization providing services to the public sector. Privacy statutes in each province also contain provisions protecting the privacy of individuals in the public sector.

As to the private sector in British Columbia, the applicable statute is the *Personal Information Protection Act* ("PIPA") which governs the collection, use and disclosure of personal information for individuals, companies, partnerships and various unincorporated businesses in the province such as professionals, non-profit organizations and trade unions. As well, provincial privacy statutes apply to the private sector in most provinces.

The last type of legislation applicable to an individual's right to privacy is human rights legislation. While this type of legislation seeks to prevent and addresses discrimination primarily with respect to employment on the basis of several prohibited grounds, including sex, race and mental and physical disability, the Act indirectly protects privacy. Employers

are prohibited from collecting or relying on various types of information including application forms, employee medical records and are prohibited from requesting medical information of an employee during employment.

COLLECTION OF PERSONAL INFORMATION

Those who collect personal information, such as employers collecting information on employees, should advise their employees what personal information will be collected, used and disclosed. Information used for one purpose with the consent of the employee should not be used for unrelated purposes. Employers should consider giving employees access to personal information held about them to verify its accuracy. Employees can request access and request that inaccurate information be changed.

Employers should only collect personal information which they consider necessary for a particular purpose and must do so by fair and lawful means. Collection must be done in a manner which could be considered reasonable and appropriate in the circumstances. Information obtained should also be used and disclosed only for the purposes for which it is collected and should be retained only for the time required to fulfil the intended purpose. Collection should only be from an employee and not from third parties (with some exceptions).

As mentioned previously, consent is an important element in the collection, use and disclosure of personal information. Consent can take two forms – informed consent and deemed consent.

Generally, informed consent is consent given by an individual after being informed what his personal information is to be collected for and how it may be used and disclosed. As to deemed consent, there are limited situations in collecting personal information where one may act without consent. Examples include information available from a public source, information being necessary for medical treatment when consent cannot be obtained in a timely fashion, or information needed for an investigation for which obtaining consent might compromise the investigation.

BREACH OF PRIVACY

How may such breaches arise? Unauthorized or inadvertent disclosure of personal information can constitute a breach of privacy. This can take place in a number of ways, including an unauthorized use of that information, the failure to ensure accuracy of personal information and the failure to provide adequate safeguards to protect that information.

The following are examples of how the Office of the Privacy Commissioner of Canada deals with complaints of privacy breaches in relation to medical issues in a disability management and insurance context:

- **Disclosure of medical information without consent** – in this case, a rehabilitation consultant advised an employer that the insured was ready to return to work. In doing so, disclosure of parts of a medical report prepared by the insured's specialist were made to the employer. The insured had expressed concerns to the consultant about disclosing any medical information to his employer. The Privacy Commissioner found that disclosure was inappropriate, that written consent ought to have been obtained and made recommendations to the employer on obtaining consent.

- **Disclosure of medical diagnosis** – in this case, the complainant was sitting in the office of the benefits administrator for her employer and learned that highly sensitive medical information about her had been left in a voice mail message to the benefits administrator by an employee of the insurance company providing benefits to the complainant's employer. The insurance company employee realized the mistake and wrote to apologize. The complainant felt that the matter should have been brought to the attention of the company's privacy officer. The Privacy Commissioner agreed the disclosure was inappropriate but approved the steps taken by the insurance company to address the issue.

She disagreed with the complainant that the insurance company was not being open about its privacy policies and practices.

- **Individual's medical information disclosed to a third party** – in retaining a third party medical consultant for an opinion, an insurer shared with that consultant the insured's medical brief and her two previous medical assessments without the insured's consent. The two previous medical assessments of the insured's condition were the subject of ongoing dispute resolution hearings. Here the Privacy Commissioner found that disclosure without express consent could take place as the insured had put her medical information in issue. As a result, she had given her implied consent to the collection, use and disclosure of her personal information by the insurer for the limited purpose of defending itself in the particular proceedings.

SURVEILLANCE AND EMPLOYEE PRIVACY

One of the tools resorted to by employers and insurers in the employment and disability context is surveillance.

Video surveillance has been used over the years in monitoring employees, particularly if there have been unsuccessful attempts to accommodate an employee who has had a disability claim, yet a concern that the employee should be able to return to work. This type of surveillance is usually used when other methods to obtain information are not sufficient.

Is it reasonable to conduct video surveillance, particularly when doing so outside the workplace? Certain PIPEDA case summaries on the subject suggest that the use of video surveillance should be limited and that the employer must have evidence of a substantial nature to show its suspicions are warranted, that it has exhausted other means of obtaining information that could not be considered to be an invasion of privacy and the collection of video evidence is for a specific and limited purpose.

Social media and off duty conduct surveillance is a relatively new type of surveillance brought about by the type of information that is often readily available on the internet. For example, when a person commences a lawsuit for disability benefits, there is an implied consent that the opposing party can collect the plaintiff's personal information in order to defend itself, but only information that is relevant to conduct a defence.

There have been several decisions over the past five years from both the courts and arbitration boards as to accessing social media postings, such as those on Facebook, and the use and disclosure of information obtained through such access. In a number of cases, disclosure has been ordered, although limits have been placed on what can be obtained from a posting. Other decisions have refused to order disclosure, in some situations where the applicant has overreached by seeking hard drives, Facebook and Twitter account profiles, iPhone and digital camera records relating to an individual's health and employability.

Caution should be used when conducting surveillance or using social media to monitor an employee's activities. If done unreasonably, it could expose an employer to complaints to privacy commissioners under various privacy statutes, complaints under the *Human Rights Act* and in a collective agreement setting, a grievance for a breach of privacy. To assist parties in determining the risks of using personal information published in social media, the British Columbia Privacy Commissioner has published **"Guidelines for Social Media Background Checks" found at www.oipc.bc.ca/guidance-documents/1454.**

REMEDIES FOR BREACH OF PRIVACY

Pecuniary losses are recoverable under PIPA and under the *BC Privacy Act*. Types of loss include financial losses if inaccurate financial information results in a loss of a business opportunity. Another type of loss could be the cost incurred for the need to monitor credit history where unauthorized access to personal information might possibly result in potential identity thefts.

As to non-pecuniary loss, there have been minimal awards under PIPEDA and also under PIPA. However, there have been more substantial awards under the BC *Privacy Act.* Examples of such awards include one against Walmart for misappropriating a former employee's photo for commercial purposes and an award against an individual for intercepting and recording a neighbour's telephone conversation. These awards resulted from actions for negligence, breach of conduct or breach of fiduciary duty resulting from a breach of privacy.

There is now an emerging cause of action for breach of privacy in tort. British Columbia's *Privacy Act i*ncludes a provision that "it is a tort …for a person wilfully and without claim of right, to violate the privacy of another". A similar type of provision is found in the privacy legislation of other provinces.

A decision by the Ontario Court of Appeal in 2012, *Jones v. Tsige* 2012 ONCA 32, found that there could be a cause of action in tort. This has come to be labelled an action for "intrusion upon seclusion". In this case, an employee had been surreptitiously reviewing another employee's bank account for several years. Upon discovering this, the owner of the records sued her fellow employee. The lower court dismissed the action on the basis that Ontario law did not recognize a tort of breach of privacy.

The Court of Appeal disagreed, it found the defendant's conduct intentional and reckless and the plaintiff's private concerns had been invaded without justification. The court held that no proof of harm to an economic interest need be made to obtain damages, however damages from a finding of a breach of privacy interest would generally result in modest damages. In this case, the damages awarded were $10,000.

It will be interesting to see whether other jurisdictions will follow the decision. Prior to this decision, the British Columbia Court of Appeal had held in another case that there was no common law tort of invasion of privacy in that province.

CONCLUSION

The scope of privacy legislation has expanded since its introduction approximately 20 years ago, sparking a growth in the body of law on privacy, as organizations and individuals become increasingly knowledgeable about rights to privacy and how to guard and enforce those rights. This area of the law will only expand as new methods of disseminating information, such as Facebook, appear.

ALEXANDER HOLBURN
ALEXANDER HOLBURN BEAUDIN + LANG LLP

ABOUT THE AUTHOR

JOHN W. ELWICK
PARTNER

John Elwick is a partner at Alexander Holburn Beaudin + Lang LLP in Vancouver, British Columbia. His practice focuses on employment, pension and benefits law and insurance law. His insurance practice is primarily directed to acting for local and national insurance companies in life and disability claims as well as undertaking regulatory work for insurance companies, including appearances as counsel before administrative tribunals dealing with insurance regulatory issues. John has appeared as counsel at all levels of courts in British Columbia and at the Supreme Court of Canada. He has also presented at seminars sponsored by various organizations including the Law Society of British Columbia's Continuing Legal Education program. John's most recent presentation was at inSight Information's Disability Claims Management and Litigation Conference in October, 2012. His topic was "ASO Agreements and the Duties of Employers in Disability Claims". John can be contacted by phone at 604-484-1707 or by email at jelwick@ahbl.ca.