dentons.com

DENTONS

Insights and Commentary from Dentons

On March 31, 2013, three pre-eminent law firms—Salans, Fraser Milner Casgrain, and SNR Denton—combined to form Dentons, a Top 10 global law firm with more than 2,500 lawyers and professionals worldwide.

This document was authored by representatives of one of the founding firms prior to our combination launch, and it continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

TECHNOLOGY ISSUES IN THE WORKPLACE

BY CATHERINE COULTER & JEEVYN DHALIWAL
FRASER MILNER CASGRAIN LLP

FRASER MILNER CASGRAIN LLP

YOUR FUTURE IS OUR BUSINESS

I INTRODUCTION

Recent years have seen an explosion of technology in the workplace, including both the proprietary technological developments created by companies and the means to improperly disseminate those developments and other confidential information through technology such as email and the internet. With this technology has come a great deal of law addressing items such as the protection of technology and confidential information and permitted uses of technology within the workplace. This paper is intended to provide an overview summary of some of those issues and to look at where the law might be headed in the future.

II NON-COMPETITION, NON-SOLICITATION AND CONFIDENTIALITY AGREEMENTS

INTRODUCTION:

Generally speaking, an employee who has left his or her employment with a former employer is free to compete with that employer, subject to three exceptions:

1. The employee has signed a valid restrictive covenant which limits his or her post-employment conduct;

2. The employee owes a fiduciary duty to the employer; or

3. The employee misappropriates or misuses the employer's proprietary trade secrets or confidential information.

In other words, an employee who is not a fiduciary may, in his or her new job, make use of any skills, information and knowledge acquired during employment, as long as the employee is not subject to a valid restrictive covenant and does not use any proprietary trade secrets or confidential information of the former employer.

There are essentially three different kinds of restrictive covenants:

1. Confidentiality Agreements - Those that require an employee to keep confidential an employer's proprietary trade secrets and confidential information;

2. Non-Competition Agreements - Those that prohibit competition with a former employer; and

3. Non-Solicitation Agreements - Those that prohibit an employee from soliciting a former employer's customers and/or employees.

DUTY OF CONFIDENTIALITY AND CONFIDENTIALITY AGREEMENTS:

The duty of confidentiality is an implied term of employment for all employees. In the leading case of *Lac Minerals Ltd. v. International Corona Resources Ltd.*[1], the Supreme Court of Canada determined that there are three required elements for the duty of confidentiality to be imposed. First, the information must have a quality of confidence to it. Second, the information must be imparted in circumstances that import an obligation of confidence. Third, the unauthorized use of the confidential information must be detrimental to the owner of the confidential information.

Because the duty of confidentiality is implied in all employment agreements, it may not be worth worrying about a written confidentiality agreement for one's employees, unless the information sought to be protected is:

1 *Lac Minerals Ltd. v. International Corona Resources Ltd.* [1987] S.C.C.A. No. 372.

(i) information from which a competitor can benefit;

(ii) information which is particular to the operation of the company; or

(iii) information which is otherwise vital to the corporation.

In any of those instances, a written confidentiality agreement will likely be of assistance. Because of the proprietary nature of the work product generated by virtually all technology companies, written confidentiality agreements are a necessary requirement in that industry.

When drafting a confidentiality agreement, the confidential information to be protected must be clearly defined. A well written agreement will also include a promise by the employee to return to the employer all confidential and proprietary information at the time of termination or resignation. Additionally, a well written agreement will contain a provision in which the employee confirms that he or she is not breaching any confidentiality agreement or obligation with a former employer by virtue of undertaking employment your company.

While there is a reasonable amount of case law in Canada in relation to the misuse of confidential information, for the most part it is extremely fact specific and the facts clearly demonstrate a misappropriation of confidential information. But what about the case where an employee leaves and the employer has only suspicions that he or she is using its confidential information to compete? In the United States, several jurisdictions have coined the phrase "inevitable disclosure" to refer to a still-developing concept where former employees go to a competitor and, by virtue of the fact that the product which the competitor is known to be developing is identical to that developed by the prior employer, the ex-employee is assumed to have misused the prior employer's confidential information in the development of that product, whether the disclosure of confidential information was intentional or not. While Canada does not have an "inevitable disclosure" doctrine, there are several cases which refer to the "spring-board doctrine", which is similar to the inevitable disclosure doctrine in many ways. In the cases of *Metrox Electronic Systems Ltd. v. Godrow*[2] and *Omega Digital Data Inc. v. Airos Technology Inc.*[3], the courts found that there were features in common between the products of the old employer and the new employer which were so striking, that the new employer's product could not have been prepared independently in circumstances where it was developed, at least in part, with the assistance of the former employees of the prior employer. In the words of Justice Guthrie in the Metrox case, he stated that:

> "... if an ex-employee is able, by information provided by or developed for the previous employer, to gain an advantage that the ex-employee would not have had if he or she had to check only public sources, such employee would still be liable for a breach of confidence despite public disclosure. This reflects an obligation to pay for the advantage gained from "convenient" confidential source, or the head start that the disclosure had given such employee over other members of the public. What is really being protected in situations of this nature is the original process of mind. The protection is enforced against persons who wish to use the confidential information without spending time, trouble and expense of going through the same process. One can reconcile the spring board principle with the overriding principle denying confidence and information in the public domain, by describing the "spring board" as a measure of the scope and duration of the obligation enforcing good faith upon an ex-employee while the rest of the world catches up."

It should be remembered that the test in an spring-board doctrine type of action is whether the employee would have been able to get to the developmental point it reached, within the same time frame, without access to confidential information. Former employees are, however, free to use reverse engineering and

2 *Metrox Electronic Systems Ltd. v. Godrow*, [1993] R.J.Q. 2249 (S.C.).
3 *Omega Digital Data Inc. v. Airos Technology Inc.* et. al. (1996) 32 O.R. (3d) 21 (Ont. Ct. (Gen. Div.)).

imitation in order to make developments based on prior non-confidential knowledge. The key to these claims seems to be:

(i) whether or not genuinely confidential information was used; and/or

(ii) the time frame for the development (ie. was the development created so quickly that it must be inferred that confidential information was used?).[4]

Notwithstanding the apparent willingness of courts in Ontario to accept the spring-board doctrine, where employers wish to seek an interlocutory injunction to keep their former employees from using confidential information, they will still have to successfully pass the legal test for an interlocutory injunction. In the leading case of *R.J.R. MacDonald*[5] the Supreme Court of Canada held that a party must meet the following test in order to be granted an interlocutory injunction:

1. The moving party must prove that there is a serious issue to be tried (in certain defined cases, the test is higher and the moving party must show that it has a strong *prima facie* case);

2. The moving party must show that if the relief sought is not granted, it will suffer irreparable harm which cannot be compensated for with an award of damages; and

3. The moving party must show that the balance of convenience is in its favour.

Of those three tests, the most difficult to satisfy is that of demonstrating irreparable harm. There are a number of good arguments that parties can make both for and against irreparable harm in misappropriation of confidential information cases and ultimately, findings of irreparable harm often seem to follow the strength of the first part of the test.

NON-COMPETITION AGREEMENTS:

Non-competition agreements are often difficult to uphold in Canada. In general, Canadian courts do not like to uphold any non-competition agreement which appears to be a restraint of trade. Additionally, non-competition agreements must be reasonable on their terms. The onus is always on the employer to prove that the terms of the non-competition agreement are reasonable.

In particular, the courts will look to three different facets of the agreement to determine whether or not it is reasonable:

(1) the geographic area of restraint;

(2) the duration of restraint; and

(3) the type of restraint.

With respect to geographic area of restraint, the restriction set out in the agreement should be limited, precise and no larger than absolutely necessary in order to protect legitimate business interests. Although some companies have restrictive covenants which provide for declining protection (eg. "The employee covenants that she shall not be employed by any entity engaged in: (a) North America; or (b) Canada; or (c) the provinces of Ontario or Quebec; or (d) a 50 mile radius of Parliament Hill, Ottawa…"), these clauses are an American import. While there seems to have been no firm pronouncement on their enforceability by the Canadian courts, there has been discussion in passing in a British Columbia case which suggests that the

4 *Cadbury Schweppes Inc. v. FBI Foods Ltd.* (1999), 167 D.L.R. (4th) 577 (S.C.C.)
5 *RJR MacDonald Inc.* v. Canada (Attorney General), [1994] 1 S.C.R. 311.

courts in Canada are not inclined to enforce these agreements, on the basis they are not prepared to assist in the drafting of something which should have been drafted properly in the first place. The view seems to be that if the parties do not determine for themselves what the legitimate geographical scope is, the courts will not assist them.

With respect to duration, a period of non-competition of greater than one year in length will generally be struck by the courts. Again, the onus is on the employer to prove that the length or duration of non-competition is reasonable in the particular circumstances. Often, in determining what a reasonable duration is, the courts will want to know what duration of time is required by the employer in order to replace the employee or to compete effectively with the departed employee or the company to whom the departed employee has moved. The exception to this rule is that the courts will often permit the enforcement of longer periods of non-competition in the context of an acquisition agreement. In other words, while it is seen as unacceptable for an employer to prevent a former employee from competing for a considerable period of time post-resignation or termination, it may well be acceptable where the former employee entered into the non-competition covenant in consideration for selling his or her stake in a company.

Sometimes, employers will offer their departed employees pay in lieu of notice for the time period during which they are bound by a non-competition agreement, as that is one way of showing the court that the employer is not trying to prohibit the departed employee from earning a living. However, in the Ontario case in *Medtronic of Canada Ltd. v. Armstrong*[6] the court would not enforce a one year non-competition agreement (which had been voluntarily entered into) in a case where the former employee was to be compensated for that one year period. In that case, the court took issue with the open-ended geographic agreement. Because the employer conducted business in more than 100 countries around the world, enforcing the agreement would have meant that the employee would had to have taken a one-year break from the industry in which he had worked for almost his entire career. The court determined that to do so was unreasonable, even though he would have been paid for that year, particularly given the fact that: (i) he would be unable to work in the field for a year; and (ii) he would lose all of the hands-on time and resources necessary to maintain adequate knowledge and competency, which he testified would have a detrimental effect on his career. Although the facts of this case suggest that it is an anomaly, it is important to bear it in mind when drafting restrictive covenants.

In the United States, the case of *EarthWeb Inc. v. Schalck*, suggested that it may be difficult for internet companies to enforce non-competition agreements. In the EarthWeb case, the Court cited the 1997 New York State case of *DoubleClick, Inc. v. Henderson*, which stated, "Given the speed with which the internet advertising area apparently changes, the employees' knowledge of DoubleClick's operation will likely lose value to such a degree that the purpose of a preliminary injunction will have evaporated before the year is up." In the *EarthWeb* case, *EarthWeb* sought to enforce a 12-month non-competition agreement, but the court determined that "measured against the IT industry in the internet environment, a one year hiatus from the work force is several generations, if not an eternity". While it is not believed that there have been any similar cases in Canada, the rationale applied by the courts appears to be sound and, given the fact that Canadian courts are inclined to not enforce non-competition agreements in the first place, fast-changing internet and other technology companies should be wary of the concerns enunciated in the New York State Courts when it comes to drafting duration clauses within non-competition agreements.

NON-SOLICITATION AGREEMENTS:

The above-noted difficulties which are inherent in enforcing non-competition agreements were discussed in the cases of *Semiconductor Insights Inc. v. Kurjanowicz*[7] and *Lyons v. Multari*[8]. In both cases, the Ontario court took the view that a non-competition agreement was sought where a non-solicitation agreement would have been more appropriate and in both cases, the non-competition agreement was therefore struck. In the

6 *Medtronic of Canada Ltd. v. Armstrong*, [1999] O.J. No. 4860 (Ont. Sup. Ct. Justice).
7 *Semiconductor Insights v. Kurjanowicz*, [1995] O.J. No. 3280 (Ont. Ct. (Gen. Div.)).
8 *Lyons v. Multari* (2000), 50 O.R. (3d) 526 (Ont. C.A.).

case of Semiconductor Insights, the court concluded that a "non-solicitation clause for specified duration would have protected the company's interests and would have been enforceable". As a result, it rejected the non-competition agreement as being overly broad and an attempt to restrain trade. The Ontario Court of Appeal's decision in Lyons was based on similar reasons. In that case, both the Plaintiff and Defendant were dental surgeons who had practiced together for 17 months with a non-competition provision for three years over a five mile radius. At the Court of Appeal, the court held that the non-competition agreement was too broad and could not be enforced. In short, where a non-solicitation agreement will do, a non-competition agreement should not be used. Moreover, only in exceptional cases will the employment relationship justify a non-competition agreement. It is also important to remember that even with non-solicitation agreements, the duration, geographic scope and intent must be narrowly drafted so that no more is sought by the employer than is reasonable for the former employee to give.

III FIDUCIARY DUTIES

INTRODUCTION:

As discussed above, fiduciaries also owe certain duties to their employers and former employers. Although all employees, whether fiduciaries or not, owe a duty to their employers and former employers to not misuse or misappropriate clearly confidential information, the duties of fiduciaries are heightened. Among other things, and even without the implementation of restrictive covenants as set out in the sections immediately preceding, fiduciaries owe a duty to not do anything which would conflict with the interests of their employers' business, including to not directly solicit customers of their current employers or former employers for a reasonable period of time. In other words, simply by virtue of being a fiduciary, an employee can find him or herself subject to at least some non-competition and non-solicitation obligations, even if restrictive covenants have not been signed.

The question then arises as to what triggers fiduciary obligations amongst employees. In the leading Supreme Court of Canada case of *Lac Minerals Ltd. v. International Corona Resources Ltd.*[9], the court found that "relationships in which a fiduciary obligation have been imposed seem to possess three general characteristics:

1. The fiduciary has scope for the exercise of some discretion or power;

2. The fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interests;

3. The beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the discretion or power."

The court went on to find that not all three elements need to be present in order for a fiduciary relationship to exist. The key feature of a fiduciary relationship however, upon which a case will rise or fall, is the existence of dependency or vulnerability on the part of the beneficiary.

WHO IS A FIDUCIARY?:

Directors, officers and other senior management are generally held to be fiduciaries. Difficulty arises most often in determining whether or not an employee truly is a member of senior management. While job titles may be of assistance, they are not determinative. Rather, what is most important is looking at the duties of the employee at issue. A fiduciary generally has authority to bind the employer and authority to make important decisions without requiring further levels of approval.

9 *Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574 (S.C.C.)

The test of determining whether or not an individual is a fiduciary becomes even more complicated when one looks at lower level employees who may be deemed 'key personnel' within an organization, as those individuals can also be held to owe fiduciary duties to their employers. There are a number of factors which the Canadian courts have looked at in determining whether or not an employee is a fiduciary, including the following:

1. The employee's knowledge and/or expertise make the employer extremely dependant upon them;

2. The employee is a valuable and trusted key employee;

3. The employee has virtually single-handedly developed the customer market and goodwill of the company by personal efforts;

4. The employee can make key decisions independently;

5. The employee has authority to bind the employer with respect to contracts and the like;

6. The employee maintains control over the employer's operations or a significant portions of those operations;

7. The length of service, compensation and/or job title of the employee are significant;

8. The employee has significant influence over key clients of the employer; and

9. The employee has agreed in an employment contract that he or she a fiduciary.

Even salespersons have been found to be fiduciaries in cases where their territory, business and/or responsibility account for a majority of the employer's business.[10] However, the courts will not lightly make a finding that an employee is a fiduciary. In the circumstances, if an employer contemplates giving significant authority to an employee or knows that it is going to be vulnerable to or dependant upon an employee, it should consider spelling out the fiduciary relationship in an employment contract, as well as having the employee enter into restrictive covenants, as appropriate.

WHAT OBLIGATIONS DOES A FIDUCIARY HAVE?:

The concept of fiduciary obligations carries with it the obligation of loyalty, faithfulness and honesty. Fiduciaries are precluded from placing themselves in a conflict of interest position with their employer, which conflict might include accepting kickbacks, diverting corporate opportunities and failing to disclose material conflicts of interest.

In the recent Ontario appeal case of *Felker v. Cunningham*[11], a fiduciary commenced employment discussions with his ultimate new employer several months before changing employment. The court's decision, that Mr. Felker did not act in a loyal or faithful manner, made it clear that fiduciaries, unlike regular employees, have a duty to advise their employers if they are pursuing other job opportunities, particularly where those other job opportunities may place them in conflict with their current employer. This principle, of course, does not apply to non-fiduciaries, who are free to pursue other job opportunities without telling their current employer.

What happens after the employment relationship comes to an end? If an employee has fiduciary obligations towards an employer, those obligations will continue post-termination or resignation. The leading case in this area is the decision of the Supreme Court of Canada in the case of *Canadian Aero Service Ltd. v. O'Malley*

10 *Demarco Agencies Ltd. v. Merlo* (1984), 48 Nfld. & P.E.I.R. 227 (Nfld. Dist. Ct.)
11 *Felker v. Cunningham*, Aug. 29, 2000, File No. C30591 (Ont. C.A.)

("Canaero")[12] Generally speaking, even after the employment relationship has come to an end, a fiduciary will continue to owe his or her former employer a duty not to:

1. directly solicit customers or clients of the former employer;

2. directly solicit former co-workers; and

3. use confidential information of the former employer.

With respect to the issue of direct solicitation, it has been generally agreed by the courts that fiduciaries are permitted to advertise their change of employment broadly. Some courts have even permitted fiduciaries to solicit their former employer's customers, provided that there is no misuse of trade secrets or customer lists. Other courts have drawn the line there and permit only indirect solicitation that is part of a broad solicitation through the relevant marketplace. Generally speaking, fiduciaries are also entitled to accept work from the customers of their former employers in cases where the customers approach them rather than the other way around. As was stated in the case of *309924 Ontario Ltd. v. Tyrrell*[13]:

> "It must be kept in mind in looking at the factors present, in any case, that employers are, or should be aware, that customers of a business who have the benefit of good advice, skill and attention of an employee such as the defendant, tend to seek out his services as opposed to those of other employees. Where such an employee changes employment and becomes a competitor, it is not unusual to find former satisfied customers bringing their business to his new location."

Interestingly, there is no general prohibition to keep fiduciaries from competing with former employers. The Canadian courts have tended towards the view that fiduciaries are entitled to earn a living, even if it means joining a competitor. However, where aspects of that competition are genuinely unfair (ie. there is a misuse of confidential information or a solicitation of clients and customers of the former employer), then it will be prohibited.

CONCLUSION:

All in all, there are cases throughout Canada that fall on both sides of the fiduciary duty equation. Some judges permit indirect or even direct solicitation by a fiduciary post-termination; others do not. As is always the case, each dispute will be determined on its specific facts. Suffice it to say that in Canada's common law provinces, which are courts of equity as well as courts of law, decisions will be influenced based on whether or not a judge perceives a particular solicitation to be fair. If so, the facts and law will generally be interpreted such that there is a finding that there has been no breach of fiduciary duties. And of course, the opposite also holds true.

The same analysis also holds true when looking at whether the fiduciary was terminated, constructively dismissed or resigned. Terminations and constructive dismissals mean that the fiduciary has no choice but to seek new employment. As a result, those individuals are often held to a lower standard when the courts make a determination as to the scope of their post-employment fiduciary duties. However, employees who resigned in order to commence alternative employment are often held to a higher standard of non-solicitation for a reasonable period of time, which period of time is often calculated based on how long it will take the employer to reasonably compete against the fiduciary and/or its new employer.

12 *Canadian Aero Service Ltd. v. O'Malley*, [1974] S.C.R. 592
13 *309925 Ontario Ltd. v. Tyrrell* (1981), 127 D.L.R. (3d) 99 (Ont. H.C.J.)

IV ENSURING CORPORATE SECURITY IN THE INFORMATION TECHNOLOGY AGE

Computers have become indispensable to the modern corporation in the Information Technology Age. Computer networks, e-mail, and access to the Internet offer many advantages to corporations in terms of efficiency, ease of communication among employees and clients, and marketing opportunities. However, the increasing use of and dependence on computers in the workplace raise some serious concerns for corporations. As employee access to computers, e-mail and the Internet has become commonplace, corporations have had to contend with a host of new threats to their security.

THREATS TO CORPORATE SECURITY:

TIME THEFT

One concern that has arisen as a direct result of computers in the workplace is decreased productivity or "time theft" that occurs when employees use e-mail and the Internet at work for personal reasons. A 2000 survey indicates that many employees spend part of their work day reading the news on the Internet, making on-line purchases and travel arrangements, and planning social events.[14] Another recent study of employees indicates that 38% of Canadians with Internet access at work spend an average of 4.5 hours per week surfing the Internet for personal reasons.[15]

VIRUSES, WORMS, AND HACKING

Another concern for corporations is the spread of computer viruses and worms. Viruses and worms cause inconvenient and often irreparable damage to systems and data stored on systems. The destructive force of computer worms has been felt numerous times in recent years, including the occurrence in 2003 when the worm SoBig.F caused over $50 million of damage in the United States alone and halted Air Canada operations.[16] Given that the day-to-day functioning of many corporations is dependant on computer networks operating properly, viruses and worms pose a serious threat to corporations worldwide.

A related threat to corporations is computer hacking. Hacking occurs when unauthorized users break into an organization's computer network to steal information or create damage. In addition to being open to attack from outside hackers, businesses are vulnerable to hacking by internal personnel. The proliferation of computers, e-mail, and the Internet in the workplace facilitates and increases the risk that employees may access and disseminate confidential information, such as client data, business strategies, and company trade secrets. In an age where information is an extremely valuable corporate asset, the fact that it can be viewed, transmitted, saved or deleted as quickly as a keystroke, has made protecting the security of information a top priority for many corporations.

LIABILITY

Corporate security is also threatened by the misuse of e-mail and the Internet in the workplace. Employers are responsible to ensure that the workplace is free from harassment and discrimination. Consequently, corporations may be liable when an employer's computers and networks are used to create and distribute offensive data, such as pornographic images or discriminatory material. In an extreme example, in the United States Chevron recently paid $2.2 million to settle a sexual harassment suit brought by a female employee protesting an e-mail that was circulated within the company.[17]

Corporations may also face liability if their employees use company computer systems to publish defamatory material or to download and distribute software programs contrary to licensing agreements. Similarly,

14 Vault.com survey of 1,004 American employees, May 2000; please see: http://www.vault.com.
15 Ipsos-Reid study of 2000 Canadians, April 2003; please see: http://www.ipsos-na.com.
16 Please see: http://edition.cnn.com/2003/TECH/internet/08/21/sobig.virus/index.html.
17 Please see: http://edition.cnn.com/2001/TECH/internet/10/18/e-mail.beast.idg/index.html.

employers could conceivably face criminal liability in cases where inappropriate e-mail or Internet use would give rise to charges under criminal obscenity laws, hate propaganda laws or where such use might amount to criminal harassment.

THEFT

Finally, the presence of valuable electronic equipment such as computers in the workplace significantly increases the risk of theft, both by persons inside and outside of the corporation.

V PROTECTIVE MEASURES

In the face of these threats, corporations are turning to various methods to safeguard their interests and property. Ironically, computers and technology are the most common and effective means by which corporations can protect themselves.

MONITORING E-MAIL AND INTERNET USE:

In an attempt to address some of the concerns raised by the widespread use of e-mail and the Internet in the workplace, increasing numbers of employers are monitoring the computer-related actions of their employees. A 2001 American survey indicates that 77.7% of major U.S. companies record and review their employees' workplace communications and activities.[18]

There are numerous software programs and other tools that enable employers to monitor their employees' e-mail and Internet activities. Using these tools, employers can examine the content of sent and received e-mails, keep track of the frequency of e-mail and Internet use, and look at what websites employees are visiting. In addition, software can scan attachments for inappropriate language, block dangerous attachments, stop intellectual property breaches, quarantine questionable messages, and notify systems managers when e-mail and computer use policies are violated.

LEGAL CONSIDERATIONS

Corporations that engage in such monitoring activities need to be aware of privacy issues that are raised by this practice. Privacy legislation, both federally and provincially, curtails the extent to which employers are able to monitor in this regard.

There does not appear to be a Canadian case specifically addressing an employer's legal right to monitor employee e-mail and Internet use in the workplace. However, there are a number of cases and arbitral decisions which would indicate that employees do not have a reasonable expectation of privacy over the content of their e-mails or their Internet use when they are using their employers' computer systems.

The following points are distilled from the case law and arbitral awards concerning employee privacy rights arising from e-mail and Internet use in the workplace:

(a) In a non-employment context, a person has a reasonable expectation of privacy in their personal e-mail, though the expectation of privacy is lower than in traditional mail.[19]

(b) An employer has the right to impose and enforce relatively strict rules regarding the use of its computer equipment and networks in pursuing its legitimate business interests.[20] These rules should be set out and consistently enforced in a comprehensive and clear computer policy.

---

18 Please see: http://www.amanet.org/research/pdfs/ems_short2001.pdf.
19 *R. v. Weir,* [1998] A.J. No. 155 (Alta. Q.B.).
20 *Krain v. Toronto-Dominion Bank*, [2002] C.L.A.D. No. 406.

(c) In the absence of a company computer policy setting out acceptable and unacceptable use of e-mail, an employee has no reasonable expectation of privacy in relation to e-mails received and sent in the workplace on the employer's time and equipment.[21]

(d) Even where an e-mail policy is published within a workplace, and even where the published policy outlines some privacy rights for an employee, an employee may not have a reasonable expectation of privacy when the contents of the employee's e-mail are of an unprofessional nature, offensive, or where access by the employer is in furtherance of investigating illegal activity, in which case the employer's interests would outweigh any claimed privacy right.[22]

(e) There is no reasonable expectation of privacy in a message sent by an employee to a union chat group on the employer's network.[23]

(f) An employee who uses an employer's computer at home for business and personal use has a reasonable expectation of privacy in relation to personal files, despite the fact that they are created on the employer's computer.[24]

(g) Employees who use their employer's electronic network to send and receive pornographic and vulgar messages and images have no reasonable expectation of privacy when the employer has a clear policy against the use of e-mail for unacceptable purposes and a log-on warning that the system is monitored in accordance with the policy.[25]

(h) Employers are less likely to be found infringing an employee's right to privacy when the monitoring of e-mail and Internet use is done in response to a complaint or a legitimate suspicion of misuse, rather than as random or general surveillance.[26]

VIDEO SURVEILLANCE IN THE WORKPLACE:

In addition to monitoring the use of e-mail and the Internet to guard against various threats to corporate security, corporations are increasingly using video surveillance to monitor the workplace and the conduct of employees. Video surveillance has been present in the workplace for many years. However, as security concerns have become more prevalent, video surveillance has become both more sophisticated and more common.

LEGAL CONSIDERATIONS

As with surveillance of employee activities by use of e-mail and Internet monitoring, video surveillance in the workplace raises legal concerns about the potential violation of employee privacy rights. Historically, employees have looked to arbitration to deal with privacy issues related to video surveillance. The arbitral awards dealing with video surveillance indicate that an attempt is made to balance an employee's right to privacy within the workplace against an employer's right to protect its legitimate business interests. Over the years, several considerations have guided arbitrators in their attempts to balance the rights of employees and employers. Typically, arbitrators will examine the facts of a particular case and consider: [27]

(a) Is video surveillance and recording necessary to meet a specific need;

---

21 *Milsom v. Corporate Computers Inc.*, [2003] A.J. No. 516.
22 *Supra* note 8.
23 *Camosun College v. CUPE, Local 2081 (Metcalfe Grievance)*, [1999] B.C.C.A.A.A. No. 490.
24 *Pacific Northwest Herb Corp. v. Thompson*, [1999] B.C.J. No. 2772 (S.C.).
25 *Treasury Board (Solicitor General Canada – Correction Service)* (2003), 116 L.A.C. (4th) 418.
26 For example, see *supra* note 12.
27 *Eastmond v. Canadian Pacific Railway*, [2004] F.C.J. No. 1043 [Eastmond].

(b) Is video surveillance and recording likely to be effective in meeting that need;

(c) Is the loss of privacy proportional to the benefit gained; and

(d) Is there a less privacy-invasive way of achieving the same end?

It is important to note that in light of policy considerations specific to collective bargaining relationships, arbitral decisions may have limited applicability to the non-unionized workplace. However, the policy considerations that relate to balancing employees' privacy interests and employers' business interests are largely the same in both a union or non-union context. As a result, the principles established in arbitral decisions should be of interest to union and non-union employers alike.

While most of the legal authority on video surveillance comes from arbitral decisions, with the adoption of the *Personal Information Protection and Electronic Documents Act* (the "*PIPEDA*")[28], employees of federal works, undertakings, or businesses may now file a privacy complaint with the Office of the Privacy Commissioner of Canada.[29] Recently, one such complaint, based on video surveillance in the workplace, was adjudicated at the Federal Court level. In *Eastmond*[30], the Federal Court considered whether video surveillance violated the privacy rights of the employees of Canadian Pacific Railway. After canvassing the arbitral decisions on video surveillance and considering them in conjunction with the requirements set out in the *PIPEDA*, the Court held that video surveillance was permissible in the circumstances. The Court mentioned several factors that influenced its decision, including the fact that the surveillance was not continuous, surreptitious, or limited to employees. In addition, the cameras were not used to measure work productivity and the recorded images were locked up and accessed by responsible managers and the police only after an incident had been reported. In this case, the Court concluded that the loss of privacy was proportional to the benefit gained by the use of the cameras.

What follows are some additionally salient points derived from the cases and arbitral decisions concerning video surveillance in the workplace:

(a) In the absence of express limitations in a Collective Agreement, there is no blanket prohibition of video surveillance in the workplace.[31]

(b) Generally, an employer does not have the right to intrude on an employee's privacy by videotaping his or her conduct. An employee's right to privacy, however, is not absolute and in certain circumstances the employer's interests may outweigh an employee's right to privacy. In order for an employer to establish that this is the case, it must demonstrate that it was reasonable for it to resort to surveillance and also that the surveillance was conducted in a reasonable manner.[32]

(c) In the unionized context, employers have the right to use video surveillance for security purposes, such as deterring theft and ensuring the safety of employees.[33]

(d) The use of periodic video surveillance to assist in the supervision of shift changes and allow monitoring of work is permissible.[34]

---

28 S.C. 2000, c. 5.

29 *PIPEDA* also applies to (1) organizations that collect, use or disclose information in one province and disclose it outside that province for a fee and (2) organizations that collect, use or disclose information in the course of commercial activities in a single province.

30 *Supra* note 14.

31 Michel G. Picher, "Truth Lies and Videotape: Employee Surveillance at Arbitration" (1998) 6 C.L.E.J. 345 at 351; *Unisource Canada Inc. v. Communications, Energy and Paperworkers' Union of Canada, (CEP) Local 433*, [2003] B.C.A.A.A. No. 309; [2004] B.C.J. No. 1261 [*Unisource*].

32 *Pope and Talbot Ltd. and Pulp, Paper and Woodworkers of Canada, Local No. 8*, [2003] B.C.C.A.A.A. No. 36 [Pope]; *Unisource, supra* note 18; *Vancouver General Hospital* (2002), 107 L.A.C. (4th) 392 [*Vancouver General*]; Toronto (City) (2002), 104 L.A.C. (4th) 193; *Eastmond*, *supra* note 14.

33 *Vancouver General, ibid.; Unisource, supra* note 18; Re *Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union* (1979), 23 L.A.C. (2d) 14.

34 *Pope, supra* note 19.

(e) Video surveillance in public places where there is no reasonable expectation of privacy is permissible.[35]

(f) The collection of personal information by surveillance video will not be reasonable when it is related only to an investigation of the breach of an employment agreement.[36]

(g) Surreptitious, as opposed to non-surreptitious surveillance will be harder for an employer to justify. Surreptitious surveillance is only justified where there is: a substantial problem; a strong possibility that surveillance will be effective in rectifying the problem; and no reasonable alternative to surreptitious surveillance.[37]

(h) Employers should ensure that their employees are informed of the purposes for which surveillance cameras are being used and should develop and distribute a policy document on the use of the cameras.[38]

(i) To justify the collection of personal information on an employee without knowledge and consent, an employer must have substantial evidence to support the suspicion that an employee is engaged in wrongdoing or that the relationship of trust has been broken. The employer must also be able to show that it has exhausted all other means of obtaining the information that it required in less privacy-invasive ways, and must limit the collection to the purposes as much as possible.[39]

BIOMETRIC DEVICES:

Biometric devices are the newest technological devices that are available to corporations to address security threats in the workplace. Biometrics is a type of personal identification that uses psychological or behavioural characteristics not shared by any other individual.There are several different types of biometric devices in use that include: fingerprint recognition; eye scan; facial recognition; hand geometry; and voice recognition.

Biometric devices have become significantly less expensive in recent years with the result that increasing numbers of corporations are looking at biometrics to secure their facilities. For instance, biometrics are being used for pre-employment screening, to control who has access to company facilities and computer networks, and to prevent "buddy punching" or fraudulent time and attendance entries.

The most commonly used biometric devices require an employee to type in a personal identification number or to swipe a card, at which time an encoded image of the employee's hand is retrieved. The device then compares the encoded image of the hand with the employee's handprint to determine whether or not the employee is in the company's system.

Recently, the Globe and Mail reported that several McDonald's restaurants in Winnipeg, Manitoba have begun to utilize biometric technology to keep track of their employees' work hours. Instead of punching in and out using traditional time clocks, employees at these McDonald's restaurants place their hand on a scanner that confirms their identity and records their arrival and departure times.[40]

At this point, there does not appear to be any judicial or arbitral consideration of the impact of biometric technology on employee privacy rights. However, given the increasing frequency with which biometric devices are being used by corporations, one can surmise that it is only a matter of time before a privacy complaint is

35 *Transit Windsor* (2001), 99 L.A.C. (4th) 295.
36 *Ross v. Rosedale Transport Ltd.*, [2003] C.L.A.D. No. 237.
37 *Unisource, supra* note 18.
38 *PIPED Act Case* Summary #273.
39 *PIPED Act Case* Summary #268.
40 Graeme Smith "Is Big McBrother invading workplace privacy?" The Globe and Mail (13 January 2004) online: http://www.globeandmail.com.

made. Employee surveillance using biometric devices necessitates the gathering of very personal information, such as fingerprints, and the potential for misuse of this information has privacy watchdogs on alert.

VI CONCLUSION

Corporate security and employee privacy are important issues facing all organizations today. The advent of computers, e-mail and the Internet, and their widespread use in the modern workplace have forced corporations to deal with a new brand of security threats. Among the concerns faced by corporations are time and property theft, computer viruses, computer hacking, and increased liability for the misuse of e-mail and the Internet.

While advances in technology are the source of many of these new threats to corporate security, technology has also provided corporations with new monitoring and surveillance tools to defend against security breaches. E-mail and Internet monitoring, video surveillance and biometric devices are just some of the ways in which corporations are attempting to protect themselves. In addition, the use of properly crafted restrictive covenants can assist corporations in protecting their technological developments and other confidential corporate information.

In developing security strategies that involve employee monitoring and surveillance, corporations must be aware of the legal implications of their actions. A review of the law in this area suggests that corporations have a right to monitor the actions of their employees in order to ensure security. However, that right is subject to restrictions and must be balanced with the privacy rights of employees.