WORKPLACE SEARCHES AND SURVEILLANCE VERSUS THE EMPLOYEE'S RIGHT TO PRIVACY

Michael G. Sherrard*

Introduction

The right of an employer to maintain the safety, security and productivity of its operations has long been recognized as a fundamental aspect of labour and employment relations. However, in the modern Canadian workplace, employers are under increasing pressure to meet a number of obligations that extend well beyond their traditional interests. For example, in addition to matters such as internal theft and property damage, employers are under a duty to protect their employees from human rights violations and the physical violence of co-workers and third parties. The onerous nature of such obligations often motivates employers to consider the methods at their disposal to monitor their workplaces and the individuals they employ.

Employers as a matter of course continue to use traditional methods of investigation, such as body searches and searches of workplace storage areas. However, as the millenium draws to a close, we continue to witness an impressive expansion in the technologies available to employers to keep track of and record information. At the same time, the number of users of these technologies increases daily.

In light of these developments, labour and employment law practitioners are wrestling with a number of controversial questions. Does an employer have carte blanche to conduct searches and surveillance of its workforce? Can an employer use any method at its disposal to protect its interests, or are there limits to an employer's ability to scrutinize its employees? What sorts of restrictions, if any, should there be on an employer's ability to use the information obtained through searches and surveillance? Does the principle of an individual's right to privacy in the workplace arise solely from a moral argument that such activities are dehumanizing, or is there a legal basis to support this principle?

This paper will focus on the delicate balance to be struck between the employee's right to privacy and the employer's need to monitor and manage the workplace. This balance can be introduced best by a comparison of two commentaries made early in the arbitral assessment of these competing interests. The employer's perspective has been described in the following manner:

---

*Partner, Ogilvy Renault, Toronto and an alumnus of the University of New Brunswick. Michael Sherrard is a specialist in labour and employment law, acting on behalf of management.

> The right of privacy concerns an individual's right to not have his statements, actions, etc. made public without his consent. But this serves only to protect him against the publication of his private statements or private actions. It should be evident that an employee's actions during working hours are not private actions... One of the supervisor's principal functions is to observe the employees in the workplace. Surely such supervision cannot be said to interfere with an employee's right to privacy. Add an electronic eye to the human eye. An employee has a much better chance of knowing when he is being watched where there is no camera. But this is a difference of degree, not a difference of kind.[1]

However, an arbitrator who favoured the employee's view of the issue focused on the principle of the right to privacy and beyond that the more general idea, of which the right to privacy is only one facet, of the crucial importance of preserving and nurturing the historically fragile concept of human dignity... electronic surveillance is the ultimate socializing device and the public controversy which always attends its use attests to people's instinctive identification of its fundamentally anti-human character.[2]

As these quotations suggest, there has been considerable legal debate on the appropriate balance to be struck between the employer's and employee's competing interests. The majority of helpful comment on this issue is found in arbitration cases, where arbitrators have been called upon to interpret specific collective agreement provisions governing workplace relationships. This paper begins with a brief outline of the legal sources of the right to privacy, then reviews the case law on various types searches and surveillance engaged in by employers. Finally, the paper provides guidance as to the proper use of search and surveillance techniques in the Canadian workplace.

The Right to Privacy

There are a number of legal sources for the protection of an individual's right of privacy. First, the right is well-recognized in the common law. Second, the *Criminal Code of Canada* makes it an offence to intercept private audio communications by a

---

[1] *Re: FMC Corp. et al. and U.A.W., Local 724* (1966) 66-1 ARB 3992, para. 8287.

[2] *Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union* (1979), 23 L.A.C. (2d) 14 at 30 .

mechanical device[3]. Third, the Canadian *Charter of Rights and Freedoms* declares that everyone has the right to be secure against unreasonable search or seizure. However, the Charter applies only to government actors and does not directly restrict the actions of private individuals or companies.

In addition to these sources, privacy legislation is rapidly evolving in both provincial and federal jurisdictions[4]. Until recently, documents rather than persons have generally attracted the interest of legislators; however, several jurisdictions have enacted privacy legislation pertaining to individuals. Chief among them with respect to influencing arbitral jurisprudence is British Columbia's *Privacy Act*, which states in part, at s. 1(1), that:"It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another." The move towards codification of the right to privacy is creating an actionable tort which is otherwise unavailable at common law.

Searches

A general guiding principle for the protection of an employee's personal effects has been stated as follows:

> The right to be free from unreasonable searches and seizures is a long-standing and hallowed principle of the common law, and one enshrined in our Constitution since the Canadian Charter of Rights and Freedoms. In my view, it takes more than a reasonable expectation that such an intrusion will take place to justify it; it requires consent,

---

[3]R.S.C. 1985, c. C-46, s. 184. The relevant portions of s. 184 provide:

(1) Everyone who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence

b. Subsection (1) does not apply to

i. a person who has the consent to intercept, express or implied of the originator of the private communication or of the person intended by the originator thereof to receive it ...,

A "private communication" is defined in s. 183 of the *Code* as being:

"any oral communication, or any telecommunication, that is made in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any other person other than the person intended by the originator to receive it...".

[4]*Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31; *Privacy Act*, R.S.C. 1985, c. P-21 and *see* Bill C-54 for the proposed *Personal Information Protection and Electronic Documents Act* introduced October 1, 1998. *Privacy Act*, R.S.S. 1978, c. P-24; *Privacy Act*, R.S.B.C. 1979, c. 336.

> express or implied, or a specific authorization arising from the general law, to justify anyone, even an employer, in engaging in such an intrusion.[5]

Body Searches / Property in Possession of Employee

The extent to which an employee's belongings should be protected from employer searches is often dependent on the nature or location of the item to be searched. Personal property such as purses, wallets and clothing are in the personal possession of the employee; as a result, they lend themselves to a presumption of privacy. However, physical contact is often required to effect a search. This type of search will therefore be subject to greater restrictions than the area in the workplace in which personal items are stored, such as employer owned lockers.

An example of the legal protection of property in the employee's personal possession is found in *Re Canada Post Corp. and C.U.P.W. (Plant Security)*, where the arbitrator stated that:

> an employee's right to privacy does not extend merely to his or her body, but goes to his or her effects as well. A police officer encountering a citizen on the street has no more right to inspect that citizen's handbag than the citizen's pockets, and no more right to search through the citizen's outer clothing than the citizen's inner clothing. In the absence of express or implied consent to the contrary, I think precisely the same considerations apply to the corporation's relationship with its employees, pursuant to a reasonable interpretation of the management rights clause, which expresses the entirety of the corporation's rights to control the freedom of its employees.[6]

Indeed, in most cases arbitrators will hold the employer to a very high standard to justify a search of an employee's personal property. In *Re Board of Governors of Riverdale Hospital and C.U.P.E., Loc. 43*[7], the majority of the arbitration board determined that the employee's express or implied consent must be given before a search is conducted or, in the absence of such consent, there must be a "real and substantial" suspicion of theft. Should the employee refuse to be searched, the employer's recourse is to seek the aid of the police.[8] In those limited circumstances where the search is justified by legitimate business concerns (such as theft or safety), the

---

[5]*Re Canada Post Corp. and C.U.P.W. (Plant Security)* (1990), 10 L.A.C. (4th) 361 at 387.

[6]*Ibid.*, at 391.

[7](1977) 14 L.A.C. (2d) 334.

[8]*Ibid.*, at 337.

employer must ensure that the search is conducted in a systematic and non-discriminatory manner.[9]

Locker and Desk Searches

Although one could suppose that an employee's privacy may take a back seat where personal property is stored in employer owned property, the employer is not given more latitude to search lockers or desks. Arbitrators have held that the employer's ownership of storage areas does not automatically remove the privacy rights of employees with respect to their personal working space. Although consent is not as significant a factor in cases dealing with searches of employee lockers, the employer should observe the following rules:

- conduct the search only if there is adequate cause to justify it;
- conduct the search in a non-discriminatory manner; and
- exhaust other alternatives prior to conducting the search.[10]

Those conditions were met in *Re University Hospital and London & Dist. Service Workers' Union, Loc. 220*. There, the arbitrator allowed a locker search on the grounds that,

> in addition to having sufficient cause for an inspection, the hospital carried out the inspection in a manner which avoids the discriminatory dimension of spot checks ... In carrying out its locker inspection the hospital requested all employees at work that day in the dietary department, including management staff, to submit to the inspection. In contrast to what would happen in a spot check, no employee was singled out; therefore no single employee was put at risk of being suspected by others of having engaged in wrongdoing simply by the fact that he alone was asked to open his locker.[11]

Drug Testing

On its face, drug testing appears to be a more intrusive form of employer surveillance than either body or locker searches, because it is a form of self-incrimination. It is the employee himself or herself who produces the evidence that gives rise to discipline. It may also constitute an investigation into off-duty conduct which may not affect, in any manner, the employee's ability to perform in the workplace. Unlike theft, malingering

---

[9]*Re Inco Metals Co and U.S.W.* (1978), 18 L.A.C. (2d) 420 at p. 424.

[10]*Re University Hospital and London & District Service Workers' Union, Local 220* (1981), 28 L.A.C. (2d) 294 at 302.

[11]*Ibid.*, at 301.

or fraudulent behaviour, even though prohibited drug use is a criminal offence, it is unlikely to attract discipline if it does not adversely affect the legitimate business interests of the employer.[12]

Arbitrators have held that employers can demand that an employee undergo a drug test where the safety of fellow workers or the public is at risk.[13] However, arbitrators will hold the employer to a high burden of proof to justify such an intrusion into what is essentially the off-duty conduct of an employee. As one arbitrator stated,

> the right that an employer may have to demand that its employees be subjected to a drug test is a singular and limited exception to the right of freedom from physical intrusion to which employees are generally entitled by law. As such it must be used judiciously, and only with demonstrable justification, based on reasonable and probable grounds.[14]

The arbitrator also observed that when drug tests are conducted, the evidence generated by the test can be challenged like any other type of scientific evidence:

Any such test must meet rigorous standards from the standpoint of the equipment, the procedure and the qualifications and care of the technician responsible for it. The result of a drug test is nothing more than a form of evidence. Like any evidence, its reliability is subject to challenge, and an employer seeking to rely on its results will, in any subsequent dispute, bear the burden of establishing, on the balance of probabilities, that the result is correct.[15]

Employers should also be aware that the information that drug tests can provide is fairly limited. The most common type of test, a urine screen, can detect only the presence of a narcotic or alcohol. It cannot discern when the chemicals were ingested, how much was ingested or if the employee was actually impaired at the time of the test. These limitations may reduce or eliminate the usefulness of the evidence to the employer, and should therefore play a role in the decision to test an employee.

A two-step test has developed which an employer must meet before it can demand a drug test:

1) was there adequate cause or evidence of a drug and/or alcohol problem in the workplace to justify a test; and

---

[12]*Re Canadian Pacific Ltd. and U.T.U.* (1987) 31 L.A.C. (3d) 179 at 189.

[13]*Ibid.*

[14]*Re Canadian National Railway Co. and U.T.U.* (1989), 6 L.A.C. (4th) 381.

[15]*Supra* note 12 at 186.

2) were there no reasonable alternatives available to the employer to combat the problem in a less intrusive way.[16]

With respect to the first part of the test, adequate cause must be more than simple suspicion. In one case, drug testing was allowed when the RCMP discovered marijuana at the employee's residence and criminal charges for cultivation and possession were laid. However, where an employer has no evidence to corroborate its suspicions about an employee's actions, even if the employee has admitted to social drug use, testing is not permitted.[17]

In certain cases, the business activity of an employer will necessarily justify the employer's demand for a drug test of certain employees. This is especially true of employers with safety-sensitive workplaces. For example, railway conductors have been held to be in a class of employees of which drug tests can be demanded. In *Re Canadian Pacific*, the arbitrator stated:

> where ... the employer is a public carrier, and the employee's duties are inherently safety sensitive, any reasonable grounds to believe that an employee may be impaired by drugs while on duty or subject to duty must be seen as justifying a requirement that the employee undergo a drug test. Given contemporary realities and the imperative of safety, that condition must be seen as implicit in the contract of employment, absent any express provision to the contrary.[18]

Other arbitrators have held that random testing can be prescribed for safety-sensitive employees for a reasonable period to monitor rehabilitation or after a significant work accident, incident or near miss.[19]

However, it must be remembered that the nature of the workplace is not the sole criteria for justifying a drug test. Employers that already engage in less intrusive monitoring of safety and productivity may have to show that these measures are inadequate in the circumstances before they can resort to more intrusive means.[20]

---

[16]*Re Esso Petroleum Canada and C.E.P., Loc. 614* (1994) 56 L.A.C. (4th) 440 at p. 447.

[17]*Supra* note 14 at 390.

[18]*Supra* note 12 at 185-186.

[19]*Supra* note 16 at 448.

[20]*Re Metropol Security, a division of Barnes Security Services Ltd. and U.S.W.A., Loc. 5296 (Drug and Alcohol testing)* (1998), 69 L.A.C. (4th) 399 at 408.

Video Surveillance

In the labour relations context, video surveillance can be broken down into two different forms, surveillance conducted within the business premises and surveillance conducted on employees outside of the workplace.

Surveillance Conducted Within the Business Premises

Surveillance conducted in the workplace is nothing new and generally all employees recognize the need of employers to monitor the actions of its employees within its workplace. However, at what point should an employee's right to privacy prevent an employer's investigation into matters arising in and concerning its place of business? Early American arbitrators were of the belief that employees should not expect privacy on the shop floor. However, Canadian arbitrators have backed away from this extreme view and have developed case law which recognizes that a balance should be maintained between the privacy interests of the employee and the business interests of the employer.

An example of the Canadian view is found in an early arbitration award concerning video surveillance in the workplace. In *Puretex Knitting*, it was determined that:

> it is clearly a matter of balancing competing considerations after recognising that any use of cameras that observe employees at work is intrinsically seriously objectionable in human terms, with the degree of objection depending on the way the cameras are deployed and the purpose for which they are used and ranging from unacceptable in the case of constant surveillance of conduct and work performance to probably non-objectionable in the case of short-term individual application for training purposes.[21]

Employees have resisted the introduction of cameras into the workplace as an over-extension of employers' management rights to monitor production.

In *Re Thibodeau-Finch Express Inc.*, the union grieved the unilateral decision of the employer to install cameras.[22] The employer attempted to justify their installation as a method of deterring theft. However, the cameras had movement and recording capability, enabling them to be used for monitoring production and for broader discipline purposes. While it avoided these issues, a majority of the Board ordered the cameras removed because their installation was contrary to past practice. The Board stated that the installation of cameras into the workplace for surveillance purposes was a change of an "operational practice" as defined in the collective agreement. While there was no prohibition in the agreement against installing cameras, in order to alter a

---

[21] *Supra* note 2 at 30.

[22] (1988), 32 L.A.C. (3d) 271.

long-standing workplace practice there must be a change in circumstances to warrant the change in the practice.

A more recent decision struck a balance between employee and employer interests in addition to considering management and union rights. In *Re Saint Mary's Hospital*, the arbitrator placed the onus on the employer to justify the encroachment upon the employees' right to privacy by applying the following test. The employer must demonstrate:

- that there is a substantial workplace problem and that there is a strong probability that surveillance will assist in solving the problem;
- that initiating use of the specific form of surveillance is not in contravention of any terms of the collective agreement;
- that it has exhausted all reasonable alternatives and that there is no less intrusive means of correcting the problem; and
- that the surveillance was conducted in a systematic and non-discriminatory manner."[23]

The employer had installed a hidden camera to monitor a manager's desk where a theft had allegedly taken place. The installation was found to be improper. The arbitrator reasoned that the privacy of a group of employees must be protected as much as possible, and the employer must therefore take all reasonable steps to secure its property before it will be entitled to initiate clandestine surveillance. Prevention of workplace problems in general should be more important to the employer than the identification of specific wrongdoers. This principle may be less important where a single employee is suspected of wrongdoing. However, where a wrongdoer can only be identified by intruding into the privacy rights of a whole group of employees, the employer must first ensure that nothing else can be done to protect its property.[24]

Surveillance Conducted on Employees Outside of the Workplace

In cases dealing with surveillance conducted outside of the workplace, arbitrators have focused on the admissibility of the video tape as opposed to addressing the legitimacy of the action. Arbitrators in British Columbia and Ontario have, for the most part, been divided in their views on the admissibility of video tape. B.C. arbitrators have had to consider the application of provincial privacy laws in their decisions and have shown a greater tendency to consider Charter arguments on privacy.

---

[23](1997) 64 L.A.C. (4th) 382.

[24]*Ibid*, at 400.

The B.C. approach is best summarized in the *Re Alberta Wheat Pool* case, where the arbitrator commented that:

> in reference to the employee/employer relationship, there is a line of authority from both judicial and arbitral jurisprudence which generally holds that conducting surveillance on an employee and videotaping his or her conduct without knowledge or consent will amount to a breach of the employee's right to privacy, unless such intrusive conduct can be demonstrably justified by the employer. The onus of establishing that justification rests with the employer. The right to privacy in the workplace is an important right but it is not absolute. The employer has every right to expect its employee to honour his or her commitment to the employer for which compensation is paid. This includes an obligation to be honest and forthright with the employer in all respects, including absence from employment for sickness or disability. In this regard, the employer has every right to investigate the reasons for an employee's absence, particularly where suspicious circumstances exist. In the course of that investigation, however, before the employer goes so far as to intrude on the right to an employee's privacy, it must be able to justify that such a course is the only one open to it and the only way in which the truth can be ascertained.[25]

As set out in *Doman Forest Products,* the approach most commonly followed in determining whether video evidence should be admitted into evidence engages in balancing the employee's right to privacy against the company's right to investigate misconduct (in this case, abuse of sick leave). Questions to be answered include whether it was reasonable, in all of the circumstances, to obtain evidence through surveillance, whether the surveillance was conducted in a reasonable manner and whether there were other alternatives open to the company to obtain the evidence it sought.[26]

The experience in Ontario has been a greater acceptance of the admissibility of videotape surveillance. This greater acceptance is due to a lack of reliance upon privacy legislation and doubt concerning the application of Charter principles.[27]

One arbitrator has even interpreted the Ontario *Labour Relations Act, 1995* as denying him the discretion to exclude evidence that would otherwise be admissible in a court.[28] In *Re Kimberly-Clark Inc.*, he pointed out the weaknesses in the case law excluding video evidence.[29] The arbitrator noted that these awards do not explain

---

[25](1995), 48 L.A.C. (4th) 322 .

[26](1990), 13 L.A.C. (4th) at 282.

[27]*Re Labatt Ontario Breweries (Toronto Brewery) and Brewery, General and Professional Workers Union, Loc. 304* (1994), 42 L.A.C. (4th) 151 at 158-160.

[28](1996), 66 L.A.C. (4th) 266.

[29]*Ibid.*, at 287-288.

whether the evidence is offensive due to the means used to acquire it or in the use of outside specialists or in the planned nature of the information gathering. In the absence of a specific rationale for scrutinizing such evidence, the arbitrator believed it was not clear why the product of some types of covert surveillance should be inadmissible but not others. He concluded that, in practical terms, it would not make sense to exclude the videotapes but allow the investigators to present their written reports or give testimony. The arbitrator also did not understand why the investigators' recording activities should make them ineligible to testify about their observations or to submit their written reports.

Despite the differences in the B.C. and Ontario approaches, the general trend in both provinces has been to apply a cumulative two-part test based on the questions set out in *Doman Forest Products*. The first component of the test is whether it was reasonable, in all the circumstances, to undertake surveillance of the employee's off-duty activity. The second is whether the surveillance was conducted in a reasonable manner which was not unduly intrusive and which fairly acquired information pertinent to the employer's legitimate interests.[30]

Arbitrators have generally held that before an employer may resort to video surveillance, it must act out of a reasonable suspicion that the employee is committing a disciplinary offence and that all less intrusive alternatives to modify the employee's behaviour have been exhausted. Grounds for reasonable suspicion include a previous history of malingering and fraudulent claims involving Workers' Compensation[31] or sick leave benefits[32]. Lack of information from the employee or unexplained lengthy absences may also allow an employer to pursue video surveillance to gather necessary facts.[33] However, under the two-part test employer must still consider less intrusive alternatives to surveillance. Although in certain circumstances it may be counterproductive for the employer to alert the employee to its concerns, arbitrators have found that less intrusive alternatives include questioning the employee on the nature of child care arrangements[34]; offering modified work[35]; requesting a medical certificate[36]; and making direct inquiries of the employee's doctors.[37]

---

[30]*Re Canadian Pacific Ltd. and B.M.W.E. (Chahal)* (1996), 59 L.A.C. (4th) 111 at p. 124.

[31]*Re Steels Industrial Products and Teamsters Union, Local 213* (1991), 24 L.A.C. (4th) 259.

[32]*Re Pacific Press Ltd. and Vancouver Printing Pressmen, Assistants and Offset Workers' Union, Loc. 25 (Dales)* (1997), 64 L.A.C. (4th) 1.

[33]*Re Canada Safeway Ltd. and U.F.C.W., Loc. 2000 (Falbo)* (1997), 71 L.A.C. (4th) at 97.

[34]*Re Toronto Transit Commission and A.T.U., Loc. 113 (Adams)*, (1997), 61 L.A.C. (4th) 218.

[35]*Re Labatt Ontario Breweries (Toronto Brewery) and Brewery, General and Professional Workers Union, Loc. 304*, (1994) 42 L.A.C. (4th) 151.

[36]*Supra* note 25.

[37]*Supra* note 26.

While the majority of the cases are determined on the first prong of the test, one recent award considered whether the actions of the private investigators hired to obtain video evidence for the employer were unreasonable. [38] In this case, the grievor was suspected of operating his private hang-gliding school while on sick leave. During the first two days of surveillance at the employee's home, the investigators were unable to tape anything useful to the employer. As a result, one of the three investigators called the employee's business to arrange a hang-gliding lesson. The other two investigators, posing as friends, taped the lesson; in so doing, they caught the grievor, who had complained of shoulder pain, handling the glider. The arbitrator found that creating a situation that would produce evidence to discipline the employee was equivalent to entrapment and was therefore unreasonable. It follows from this decision that activity which includes a tort, such as trespass, will likely also be considered unreasonable and result in the exclusion of the evidence obtained.

Electronic Surveillance

As businesses move towards greater electronic integration through computer networks, voicemail and the Internet, arbitrators will be faced with an increasing number of cases dealing with the level of privacy which should be afforded to employees and their use of these technologies in the workplace. As the use of electronic mail increases and more people become comfortable with the Internet, arbitrators will eventually have to consider whether a business has an operational interest in monitoring their employees' use of computer systems.

Already, employers have methods at their disposal for scrutinizing these forms of communication. Employers are now capable of saving automatically and indefinitely all of their employees' e-mail, voicemail, and Internet searches. There is even software which allows an employer to search e-mail for key words such as offensive terms.[39] The question is no longer whether employers can monitor electronic communication, but whether they should. While this issue is still in its infancy in Canada, it is becoming prominent in the United States The American experience may well be mirrored north of the border.

The US Approach to Electronic Surveillance

American jurisprudence and scholarship have addressed the issue of privacy of electronic communications in response to an increasing number of suits involving

---

[38] *Supra* note 28.

[39] Dana Hawkins, "Who's watching now? Hassled by lawsuits, firms probe workers' privacy", *US News & World Report*, 123-10 (September 15, 1997) at 56-58.

improper use of a company's e-mail system. Both Morgan Stanley, a Wall Street brokerage firm, and Citibank have faced multi-million dollar lawsuits brought by employees who have accused fellow employees of disseminating racist material through the companies' e-mail systems, thereby creating a "hostile work environment".[40] Unlike in Canada, the US's history of large jury awards has quickly brought the issue of electronic monitoring to the forefront of the law. Discussion in the US has centered on two legal documents, the Fourth Amendment to the *United States Constitution* and Federal legislation known as the *Electronic Communications Privacy Act of 1986* ("ECPA") and its amendments.

The Fourth Amendment mirrors section 8 of the Charter and grants individuals "the right ... to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures". While the right to privacy is not mentioned, it has been read in by the US Supreme Court.[41] Nonetheless, the *Fourth Amendment* may grant only moderate protection to employees. First, it applies only to government actors. Second, the right exists only where a court finds that the employee had a "reasonable expectation" of the privacy of his or her communication. For example, in *Bohach v City of Reno*,[42] two police officers claimed that the City had violated their Fourth Amendment rights when it accessed messages created by the officers' paging system and stored on the police department computer. The District Court of Nevada found that there was no reasonable expectation of privacy with respect to the stored messages, because the City had notified its employees that messages would be stored on the network and the network was accessible to anyone using the computer system.

The ECPA is intended to regulate the use of the ever-changing array of electronic communication technologies. It prohibits "the intentional or wilful interception, accession, disclosure or use of one's wire, oral or electronic communication."[43] However, US commentators have stated that while "none [of] the provisions in the ECPA or its legislative history appear to limit its applicability to employer monitoring of employee e-mail communications, the ECPA contains three primary exceptions that may have the same practical effect."[44] These exceptions are the provider exception, the ordinary course of business exception and the consent exception.

---

[40]Kevin J. Baum, "E-Mail in the Workplace and the Right of Privacy" (1997), 42 Villanova Law Review 1011 at 1015-1016.

[41]*Katz* v. *United States*, 389 U.S. 347 (1967).

[42]932 F. Supp. 1232 (D. Nev. 1996).

[43]Kevin P. Kopp, "Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy" (1998), 8 Seton Hall Const. L.J. 861 at 869.

[44]*Ibid.*, at 870-871.

The provider exception focuses on the ownership of the network service. Private employers likely enjoy an unrestricted right to monitor e-mail communications in their workplace in situations where they own both the computer software and the hardware used by the employee to access the e-mail system.[45]

The ordinary course of business exception first arose primarily out of the monitoring of employee telephone communications. US courts have focused on two different aspects of the communication: context and content. The context approach allows an employer to monitor all "business-related" communications. This approach is the least likely to apply to the monitoring of electronic communications. However, it could apply to companies whose trademark and technology secrets need to be protected or to workplaces where there is a suspicion of insider trading.

The content approach allows the employer to monitor communications where it has a legitimate business or legal interest in the subject matter of the communication. Therefore, where the subject matter could render the employer liable for a lawsuit, as in the Morgan Stanley and Citibank cases, or the employer must ensure that codes of conduct are being followed, then the employer will likely have a legitimate interest in monitoring its employees. As was stated in *Smyth v. Pillsbury*, in these circumstances "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[46]

However, the employer's use of this particular exception is limited to reasonable intrusions into the otherwise private and personal communications of its employees. Initially, employers would only be allowed to investigate up to the point of determining whether or not the message is business-related before taking further action.[47]

Finally, under the third exception, express or implied consent given by the employee will allow the employer to monitor e-mail communications. Where the employer disseminates a clear policy concerning the use of e-mail in the workplace, consent will be implied.[48]

Possible Canadian Approaches to Electronic Surveillance

When they are faced with the question of employer surveillance of an employee's electronic communications, arbitrators in Canada will have to decide what level of

---

[45] *Ibid.*, at 871.

[46] 914 F. Supp. 97 (E.D. Pa. 1996).

[47] *Supra* note 40 at 1027.

[48] *Ibid.*

privacy is appropriate in the circumstances. For example, an arbitrator dealing with an employer who has obtained information from an employee's computer may decide that the search of the computer is equivalent to the search of a locker. In this case, the item being searched is the property of the employer.

However, this may not eliminate or limit the privacy expectation an employee may have concerning the files stored in the computer. If it is reasonable for employees to be protected from a search of their desks and the reading of their personal correspondence, it may be no less reasonable that they be protected if the correspondence is stored on a computer rather than on paper and in a desk drawer. Ownership of the item, in this analysis, becomes irrelevant and it is the employee's expectation of privacy that governs. Following this model, an employer would require reasonable cause to justify the search, would have to conduct the search in a non-discriminatory manner and would have to exhaust other alternatives prior to conducting the search.

Alternatively, arbitrators may decide to apply the reasoning used in video surveillance cases. With this approach, the valid business interest of the employer in the integrity of his communication system would be balanced against the privacy rights of the employee. An important similarity between electronic surveillance and video surveillance is the subtle means by which an employer can conduct the surveillance (as opposed, for example, to a body search). Computer networks allow information to be stored automatically and accessed freely by authorized personnel without the employee becoming aware that his or her files are being reviewed. Also, under this model, the employer will have to demonstrate that it had reasonable cause to conduct the search, that the search was carried out in a reasonable manner and that the employer had no other reasonable alternatives at its disposal.

One indication that the video surveillance model may be preferred comes from a recent B.C. decision. In *International Association Of Bridge, Structural and Ornamental Ironworkers, Local 97 and Office and Technical Employers' Union, Local 15*, the arbitrator found that where the computer belongs to the employer, the employee has no absolute right to privacy.[49] In this case, the employer retrieved computer files directly off the hard drive of the business computer assigned to the employee. Citing *Alberta Wheat Pool*, the arbitrator upheld the suspension imposed by the employer on the employee for engaging in personal activity on company time.

[49][1997] B.C.D.L.A. 500.24.10.00-12.

Summary and Conclusion

Hierarchy of Privacy Rights

This discussion of the case law dealing with searches and surveillance indicates that there is a hierarchy which governs protection of the privacy rights of employees:

1. The greatest legal restrictions are imposed on employer searches which involve physically touching the employee, such as a medical examination or body search. Such searches may occur only where there has been express or implied consent granted by the employee. "In such cases, there can be no question of balancing of interests because the employer does not obtain a right to commit trespass or an assault on an employee by virtue of the employment relationship."[50]

2. Searches involving personal effects or spaces are subject to the next highest level of protection. In these cases, it is generally accepted that an employee should enjoy some level of privacy. However, this right must be balanced against the right of the employer to ensure the security of its property or workplace.

3. The next category of cases involves passive surveillance both inside and outside the workplace. From supervisors to time clocks to video cameras, these cases give greater weight to the employer's right to monitor its workforce. In these cases, employers may engage in various forms of monitoring employees. However, they must have reasonable justification to engage in surveillance, must have rights under the collective agreement to employ their chosen method of surveillance, and must conduct that surveillance in a reasonable and non-discriminatory fashion.

4. Finally, we have seen the introduction of more subtle forms of electronic surveillance, primarily of employees' electronic communications from the workplace. These forms of surveillance are least likely to violate the personal privacy rights of employees. However, the method of surveillance must be the least obtrusive to the employee. Where the surveillance is conducted in a reasonable manner on a particular individual for a short period, the employer has acted out of reasonable suspicion and requires additional information after having exhausted alternatives (such as locking desks or installing pass keys), then this form of surveillance may require a lower level of justification.

Balancing Interests

In order to minimize the negative effects of searching and monitoring employees while effectively protecting legitimate employer interests, all employers (unionized or not) are

---

[50]*Ibid.*, at p.397.

well advised to adhere to the legal principles established by Canadian labour arbitrators. Employers must balance their needs against employees' privacy interests, and ensure that the search and surveillance methods they use are commensurate with their legitimate business interests. For example, limiting surveillance to determining the time, origin, destination and length of an e-mail transmission or telephone conversation will allow an employer to determine if the communication was for business or personal purposes. By restricting monitoring in this way, employers can protect their interests without accessing the content of personal communications. With respect to the Internet, the types of websites visited by an employee will indicate whether an employee is using the Internet for personal or business use and whether the employee is accessing illegal or inappropriate material.

Further, employers should establish policies regarding proper monitoring procedures for e-mail, Internet and phone usage. The policies should make clear to employees the scope and intent of the monitoring, including:

- the purpose of the monitoring;
- the extent to which monitoring will be conducted;
- the fact that telephones, voice mail, e-mail and the Internet are to be used for business purposes only;
- how business use will be distinguished from personal use;
- how monitoring will be accomplished and its proposed frequency; and
- clear demarcation between what is considered to be a public versus a private communication.

Monitoring policies should also emphasize that employees have a reduced expectation of privacy in the workplace. If possible, such policies should be made part of the terms and conditions of employment at the time of hire. Employers should also consider seeking signed acknowledgements from employees indicating that they understand the policy and consent to monitoring consistent with the policy.

Monitoring employees' use of e-mail, the Internet, voice mail and telephones *can* be done from a technical point of view. It *may* be done legally in many circumstances. Employers certainly have a legitimate interest in ensuring that their resources are used in an appropriate manner and that their workplaces are secure. Nonetheless, it is not self-evident that employers *should* monitor employees to the full extent of their ability to do so, since the corresponding erosion of employee privacy may also have negative effects on the workplace to the employer's ultimate detriment.

In the final analysis, employers must keep in mind that positive employee relations are fundamental to maintaining a productive workplace, and that this interest should be at the heart of any decision to conduct searches or surveillance of employees.