

THE RIGHT TO PRIVACY: FACT OR FICTION?

MELANIE D. MCNAUGHT

This paper is for general discussion purposes and does not constitute legal advice or an opinion.

For legal advice regarding your particular circumstances, please contact us.

TABLE OF CONTENTS

INTRODUCTION	1
OVERVIEW OF PRIVACY LEGISLATION APPLICABLE TO ONTARIO EMPLOYERS.....	2
RECENT PIPEDA DECISIONS.....	2
PIPEDA Case Summary #2009-001	3
PIPEDA Case Summary #2009-011	5
PIPEDA Case Summary #2009-019	7
PIPEDA Case Summary #2010-004	8
COMMON LAW RIGHT TO PRIVACY	9
<i>Jones v Tsige</i> , 2011 ONSC 1475.....	9
UNION EMPLOYEES' RIGHT TO PRIVACY	11
<i>Canadian Timken Ltd. v United Steelworkers of America,</i> <i>Local 4906</i> (2001), 98 LAC (4th) 129	12
<i>Labourers' International Union of North America, Local 625</i> <i>v Prestressed Systems Inc.</i> , [2005] OLAA No. 125	14
<i>Woodbridge Foam Corp. v CAW-Canada, Local 222,</i> [2009] OLAA No 269	16
<i>Kingston (City) v Canadian Union of Public Employees, Local 109,</i> [2010] OLAA No 146	17
CHARTER RIGHT TO PRIVACY	18
<i>R. v Cole</i> , 2011 ONCA 218.....	18

INTRODUCTION

Privacy of personal information is frequently in the news these days.¹ As we conduct more business using computers and mobile devices, it seems that personal information is becoming more vulnerable to theft or unwanted disclosure.

A few weeks ago, Sony revealed that the personal information of approximately 77 million customers may have been compromised. Personal information was stolen from Sony's on-line video game network, including names, addresses and possibly credit card numbers.²

ABC News recently reported that employees are increasingly using cell phones and other digital devices to record conversations in the workplace, and sometimes using the recordings to launch harassment complaints against their employers. The news report suggested that managers should assume that their discussions with employees are being recorded.³

These and other examples highlight the concern of employees and consumers about the privacy of their personal information. Employees are not afraid to challenge management decisions regarding the collection, use and disclosure of their personal information. But do employees actually have a right to privacy?

In many parts of the country there is a privacy vacuum when it comes to employee personal information. In provinces like Ontario, which have not yet enacted broad based private-sector privacy legislation, many private-sector employers apply different standards and levels of privacy protection to customer information than to their employees' personal information.

This paper will discuss the application of the federal private-sector privacy legislation, *Personal Information Protection and Electronic Documents Act, 2000* ("PIPEDA"), and review several recent decisions under PIPEDA. We will also review a recent decision under the *Canadian Charter of Rights and Freedoms* (the "*Charter*"), which found that a school board employee had a right to privacy with respect to his work computer.

¹ Melanie D. McNaught would like to thank Paula Pettit, John-Pierre Karam and Daina Search for their contributions to this paper.

² "Sony PlayStation suffers massive data breach", on-line at <http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426>.

³ "Are you being secretly recorded at work?" on-line at <http://abcnews.go.com/Technology/secretly-recorded-work/story?id=13409126>.

Finally, we will consider the “right to privacy” in both union and non-union settings.

OVERVIEW OF PRIVACY LEGISLATION APPLICABLE TO ONTARIO EMPLOYERS

PIPEDA is federal legislation that applies to personal information collected, used or disclosed in the course of commercial activities by provincially regulated organizations in Ontario. Most instances of the collection, use and disclosure of employee personal information would not be considered a “commercial activity”.

PIPEDA also applies to personal information collected, used or disclosed in the employment relationships of federally regulated works, undertakings and businesses. Federally regulated works, undertakings and businesses include banks, telecommunications companies, and interprovincial or international transportation companies. Federally regulated employers operating in Ontario are therefore bound by PIPEDA with respect to the collection, use and disclosure of employees’ personal information for purposes related to the employment relationship, but provincially regulated Ontario employers are not. The Ontario government may pass privacy legislation that is substantially similar to PIPEDA. Such legislation would very likely apply to provincially regulated employers in Ontario.

Although the Ontario government has not passed broad private-sector privacy legislation, it recently enacted the *Personal Health Information Protection Act* (“PHIPA”). PHIPA protects individuals’ personal health information by regulating the information practices of health information custodians, such as doctors and hospitals, and their agents. Certain provisions of PHIPA may impact an employer’s collection, use and disclosure of personal health information; however, a full discussion of PHIPA is beyond the scope of this paper.

RECENT PIPEDA DECISIONS

After an initial flurry of decisions from the Privacy Commissioner, recently there have been few significant findings. Below are several interesting decisions from the past couple of years that show the Privacy Commissioner’s approach to privacy in federally regulated workplaces.

PIPEDA Case Summary #2009-001

Facts

An employee complained that his employer, an inter-city bus company, was using video cameras to monitor and manage employee performance.

There were 31 cameras in the bus depot. They were located in areas where there was a concern for safety, as well as in areas where there was cash and freight handling. The cameras could not zoom or pan. While the cameras would capture employees' images, they were not directed at employees. The videos were recorded to hard disks on computers in a secured room. The videos were not continuously monitored. They were kept for up to three months and then recorded over if they were not needed. Signs at the entrances to the depot notified of the surveillance.

Decision

The Assistant Commissioner found that the collection and use of personal information through video surveillance was reasonable. However, the employer had violated PIPEDA Principle 4.3.2, which requires knowledge and consent, by failing to make reasonable efforts to explain to employees the purposes of the surveillance.

The Commissioner's Analysis

1. Was the video surveillance reasonable?

Section 5(3) of PIPEDA provides that an organization may collect, use or disclose personal information for purposes that a reasonable person would consider appropriate under the circumstances.

The Office of the Privacy Commissioner of Canada has adopted the following four-part test to determine whether video surveillance is reasonable:

1. Is the use of video surveillance cameras demonstrably necessary to meet a specific need?
2. Is video surveillance likely to be effective in meeting these needs?

3. Is the loss of privacy proportional to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?

The Assistant Commissioner found that the employer had met the first part of the test by establishing that there were issues of safety and security at the bus depot, including drug trafficking, violence, vandalism, theft and vehicle collisions.

The Assistant Commissioner accepted that video surveillance would likely be effective in dealing with these issues.

Further, the Assistant Commissioner found that the loss of privacy was proportional to gain in safety and security at the bus depot. For instance, the cameras were not focused on areas where there was a heightened expectation of privacy, such as washrooms or employee break rooms.

Finally, the Assistant Commissioner accepted that the surveillance system provided an additional level of safety and security, and allowed the guards to monitor the entire property from a central location.

Accordingly, the use of video surveillance was reasonable in the circumstances of this case.

2. Was there implied consent to the collection of personal information?

PIPEDA Principle 4.3.1 provides that consent is required for the collection, use and disclosure of personal information, subject to certain exceptions. PIPEDA Principle 4.3.2 clarifies that organizations must take reasonable steps to advise individuals of the purposes for which personal information is being collected to meet the requirement of “knowledge and consent”. Under PIPEDA Principle 4.3.6, an organization may be able to rely on implied consent if the personal information is less sensitive.

The personal information captured in this case, images of employees and customers in a public place, was not particularly sensitive. Further, the cameras were clearly visible and there were signs advising that the area was under video surveillance. Under the circumstances, the employer could rely on implied consent.

The Assistant Commissioner stated that employee consent should only be implied for purposes which the employee would reasonably expect that the information would be used. The Assistant Commissioner stated,

however, that if a camera collects information that the employer later wishes to use for disciplinary purposes, the employer can use the information under the circumstances set out in paragraphs 7(2)(a) and (b) of PIPEDA.

The Assistant Commissioner found that the employer had violated PIPEDA Principle 4.3.2 by not advising employees of the purposes for which the information would be collected.

PIPEDA Case Summary #2009-011

Facts

The complainant objected to the installation of a Mobile Data Terminal and a Global Positioning System (“GPS”) tracking device in vehicles he drove for a municipal transportation service, which provided door-to-door service for mobility-reduced passengers.

The Mobile Data Terminal allowed for the exchange of information between the driver and dispatcher. This information previously had been exchanged by radio communication and paper driver sheets.

All drivers and the complainant’s union were given prior notice that the devices would be installed.

Decision

The complaint was not well-founded. There was no violation of PIPEDA under the circumstances.

The Commissioner’s Analysis

This decision also dealt with implied consent and the reasonableness of collection using electronic means.

1. Was there implied consent for the collection and use?

As stated above, an organization may be able to rely on implied consent where the personal information is not particularly sensitive.

The Assistant Commissioner found that the personal information collected and used in this case was not sensitive.

The Assistant Commissioner found that it was reasonable for the employer to assume it had the drivers’ implied consent to collect their personal information using GPS because they continued to provide their

services after being advised of the devices' installation. Drivers and the union had the opportunity to object to the use of the device at the time of its installation, but did not.

Further, it was reasonable for the employer to assume it had the implied consent of its customers to collect and use their personal information using the Mobile Data Terminal. Customers must have been aware that the employer and its drivers required their name, pick-up location and drop-off location. The Assistant Commissioner determined that the information collected and used did not differ substantially in type or quantity from that collected and used under the previous system.

2. Was the information collected for a reasonable purpose?

An organization may collect, use or disclose personal information for purposes that a reasonable person would consider appropriate under the circumstances.

The Assistant Commissioner applied the four-part test discussed above:

1. Is the measure demonstrably necessary to meet a specific need?
2. Is measure likely to be effective in meeting these needs?
3. Is the loss of privacy proportional to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?

The purpose of the collection of personal information through GPS and the Mobile Data Terminal was to improve efficiency and the quality of service. The Assistant Commissioner found that these improvements could not be achieved without the use of GPS and the Mobile Data Terminal. There was minimal impact on privacy and it was outweighed by the benefits. Accordingly, the collection and use of the personal information was for a reasonable purpose.

There was no evidence to corroborate the allegation that the personal information collected through GPS was used for performance management.

PIPEDA Case Summary #2009-019

Facts

The complainant alleged that his employer, a telecommunications company, accessed his personal email account to support disciplinary actions against him.

In a private meeting, the employer presented the complainant with a copy of one of his emails, which appeared to be evidence that he had distributed the company's copyrighted material in an on-line labour union discussion forum.

The employer had a policy regarding the acceptable use of email in the workplace, and required employees to familiarize themselves with the policy by completing an annual training course. The policy indicated that the employer reserved the right to access and disclose all messages sent over its email system for any purpose. Additionally, the policy stated that company email should be used only for business purposes, must not interfere with normal business activities, and must not potentially embarrass the company.

Decision

Pursuant to paragraphs 7(1)(b) and 7(2)(d) of PIPEDA, the employer was entitled to access the complainant's corporate email account.

Analysis

Despite the complainant's assertion that his employer accessed his personal email account, the evidence suggested that the complainant had forwarded the emails in question from his personal account to his corporate account.

The employer had a justifiable reason to access the complainant's corporate email account, as it was investigating a breach of the employment agreement. The email account was only accessed after conducting an external investigation, which led the employer to believe that the person posting material on the union discussion forum was likely an employee who worked in the same geographical region as the complainant, and had the same initials as the complainant.

The Commissioner found two exceptions to the requirement to obtain consent applied. In her view, the employer was entitled to collect the complainant's personal information pursuant to paragraph 7(1)(b), and to use it pursuant to paragraph 7(2)(d). These exceptions allow for non-consensual collection and use of information, including employee emails, for purposes of investigating a possible breach of an employment agreement. The employer was responding to specific concerns related to an identifiable individual who was using corporate email in contravention of an established policy.

PIPEDA Case Summary #2010-004

Facts

An employee complained that a manager advised other employees of his compensation and said that his job performance did not measure up.

The employer was federally regulated. The employer's personnel policy required employees to refrain from the discussion of personal information with any person, including fellow employees. Moreover, it required employees to act in accordance with any federal or provincial laws that exceeded the confidentiality obligations of the personnel policy.

The employer argued that there was no breach of PIPEDA because the statement regarding compensation was inaccurate and because the employee had given implied consent by allowing his compensation to be disclosed in financial statements.

Decision

The Commissioner found a breach of PIPEDA and made several recommendations to the employer concerning privacy policies and procedures.

Analysis

Even if the disclosed amount did not correspond exactly to the complainant's actual compensation, the information could still be considered personal information for the purposes of PIPEDA. Personal information can be defined as "information...about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with

other information.”⁴ The Commissioner noted that opinions about identifiable individuals may also be considered personal information under PIPEDA.

The Commissioner disagreed that the employer had implied consent because the employee had not objected to his salary being disclosed in financial statements. There was no evidence that the employee had provided a blanket implicit consent to cover all purposes for which his salary information could be disclosed by his employer. Further, the complainant had a reasonable expectation of privacy, given that the employer’s own personnel policy manual instructed employees to treat information from employee files as strictly confidential.

Paragraph 7(3)(h.1) of PIPEDA provides an exemption to the requirement of consent for information that is both publicly available and is specified by the regulations. The regulations create an exemption for personal information that appears in a registry collected under a statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry.⁵ This exemption did not apply because the disclosure did not relate to the purpose for which the information was disclosed in the financial reports.

COMMON LAW RIGHT TO PRIVACY

Some decisions, such as *Somwar v McDonald’s Restaurants of Canada, Ltd.*, (2006) 263 DLR (4th) 752, have suggested that courts can enforce a right to privacy at common law. This would mean that non-union employees could sue their employers for breaching their privacy. A recent decision of the Ontario Superior Court casts doubt on that conclusion.

***Jones v Tsighe*, 2011 ONSC 1475**

Facts

The Plaintiff and the Defendant worked for the Bank of Montreal (“BMO”) and were also BMO customers.

The Defendant was involved in a relationship with the Plaintiff’s former husband. Over approximately three years, the Defendant used her workplace computer to view the transactions in the Plaintiff’s BMO

⁴ *Gordon v Canada (Health)*, 2008 FC 258 (CanLII).

⁵ *Regulations Specifying Publicly Available Information*, SOR/2001-7, s. 1(c).

accounts. The information accessed included account balances, debit and credit transactions, bill payments and account transfers. When BMO became aware of the Defendant's conduct, she was promptly disciplined.

The Plaintiff commenced a civil lawsuit against the Defendant for invasion of privacy and breach of fiduciary obligations. The Plaintiff moved for summary judgment, and sought general, punitive and exemplary damages and a permanent injunction to restrain any similar conduct by the Defendant in the future.

The Defendant moved to have the action dismissed. The Defendant asserted no tort of invasion of privacy exists in Ontario and that she did not owe fiduciary obligations to the Plaintiff.

Decision

The Court held that there was no tort of invasion of privacy and dismissed the Plaintiff's action.

The Court's Analysis

The Plaintiff relied on a line of authority that seemed to suggest that the courts are beginning to recognize a tort of invasion of privacy. In one such case, *Somwar v McDonald's*, a motion judge of the Ontario Superior Court refused to strike a claim for breach of privacy. While the Court did not explicitly recognize the tort of invasion of privacy, it could not conclude that no such tort existed because the law was not sufficiently settled.

In contrast, Whitaker J. found that there was no tort of invasion of privacy in Ontario. He followed the decision of the Ontario Court of Appeal in *Euteneier v Lee*, (2005) 260 DLR (4th) 145, which was decided shortly before *Somwar v McDonald's*, but not discussed in that case. In *Euteneier v Lee*, the plaintiff sued the police following a strip search. Although she did not sue for breach of privacy *per se*, the Court of Appeal stated that there was no "free standing right" to privacy at common law and declined to recognize a tort of invasion of privacy.

Whitaker J. stated that there are at least four statutes imposing privacy obligations in Ontario. In particular, PIPEDA applies to the banking sector. As a result, the Plaintiff was not barred from a remedy. Whitaker J. held at paragraph 56:

I would also note that this is not an area of law that requires ‘judge-made’ rights and obligations. Statutory schemes that govern privacy issues are, for the most part, carefully nuanced and designed to balance concerns and needs in an industry-specific fashion.

Accordingly, the Court dismissed the claim based on breach of privacy. Further, the Court held that the Defendant did not owe the Plaintiff a fiduciary duty and dismissed the claim on that basis.

This decision has been appealed to the Ontario Court of Appeal, which will have an opportunity to decide whether or not to recognize the tort of invasion of privacy.

Interestingly, when Whitaker J. was a labour arbitrator, he stated that there is “some (albeit limited) recognition by the courts of a common law right to privacy” and held that video surveillance evidence could not be admitted into evidence unless it passed a reasonableness test.⁶ The reasonableness test and unionized employees’ right to privacy will be discussed below.

UNION EMPLOYEES’ RIGHT TO PRIVACY

Arbitrators have recognized that unionized employees have a right to privacy in a number of cases. Sometimes this right comes from legislation, such as PIPEDA; sometimes from the collective agreement; and sometimes it appears to be an independent right stemming from arbitral case law.

It is fairly widely accepted that unionized employees have some right to privacy while they are work; for instance, the right to be free from unreasonable video surveillance in the workplace.⁷

Unionized employees’ right to privacy may also apply outside of the workplace, giving them rights that non-union employees may not have. This is exemplified in cases regarding video surveillance during sick leave. In several decisions, arbitrators have found that unionized employees have a right to privacy outside of the workplace. If this right is breached by video surveillance, which the arbitrator finds to be unreasonable, the video may not be admitted into evidence at arbitration.

⁶ *Teamsters, Local 419 v Securicor Cash Services* (2004), 125 LAC (4th) 129.

⁷ For recent examples see: *William Neilson Dairy and Teamsters, Local 647* (2009), 182 LAC (4th) 403 and *Cascade Aerospace, Inc. and C.A.W.-Canada, Local 114* (2009), 186 LAC (4th) 26.

Several years ago, two distinct lines of cases began to emerge. One line held that employees have a right to privacy that must be balanced against the employer's business interests.⁸ Admissibility in those cases was determined by assessing the reasonableness of the intrusion on the employee's privacy interest. The other line concluded that unionized employees in Ontario do not have a right to privacy, unless the collective agreement provides for it.⁹ In those decisions, evidence was admissible if it was relevant.

In earlier arbitral case law, several arbitrators analyzed the existence of employee privacy rights. Recently, arbitrators have focused much less on whether or not a general right to privacy exists. Instead, the main issue for arbitrators has been whether to employ a reasonableness or a relevancy test for the admissibility of video surveillance evidence.

The following paragraphs will review two leading video surveillance decisions – one from each of the divergent lines of cases. Then, we will review two recent decisions in which the right to privacy was not expressly decided. The divergence in the arbitral jurisprudence persists, which makes it difficult for employers (and their counsel) to predict whether video surveillance evidence is likely to be admitted.

Canadian Timken Ltd. v United Steelworkers of America, Local 4906
(2001), 98 LAC (4th) 129

Facts

The company dismissed the grievor for misrepresenting his ability to work following a back injury. The company had surveillance evidence showing the grievor in situations that compromised his claim of disability. The union argued the video surveillance should not be admitted into evidence at the hearing because it violated the grievor's right to privacy.

Decision

The grievor did not enjoy a general right of privacy. The video surveillance tapes were admissible evidence because they were relevant to the issues in the case.

⁸ *Labourers' International Union of North America, Local 625 v Prestressed Systems Inc. (Roberts Grievance)*, [2005] OLAA No. 125, 137 LAC (4th) 193.

⁹ *Canadian Timken Ltd. v United Steelworkers of America, Local 4906*, (2001) 98 LAC (4th) 129; *Kimberly-Clark Inc. I.W.A. – Canada Local 1-92-4* (1996), 66 LAC (4th) 266; and *Toronto Transit Commission v A.T.U., Local 113* (1999), 79 LAC (4th) 85.

Analysis

1. Do unionized employees in Ontario have a general right to privacy?

Arbitrator Welling distinguished several British Columbia arbitral awards finding a privacy right because there was both a legislative basis for such a right in B.C. and because the employers conceded that such a right existed.¹⁰

Arbitrator Welling disagreed with arbitral awards that determined the admissibility of surveillance evidence by assessing the reasonableness of the surveillance. He held that a balancing of employee and employer interests can only be done where there is a legal right to privacy created by a statute.

Although an employee might have a reasonable expectation of privacy, that is not a sufficient legal basis to conclude that a right to privacy exists. Individuals may be at liberty to enjoy privacy, but that liberty may be interfered with by the state or other individuals. The common law determines when and how those interferences may (and may not) occur. While the video surveillance may have violated the grievor's expectation of privacy, the absence of any statutory or common law right in Ontario meant that the grievor had no right to privacy.

2. Which test is the preferred approach for the admissibility of evidence?

Arbitrator Welling stated that he did not understand how the reasonableness test for the admissibility of video surveillance evidence could be applicable unless a right to privacy was found to exist. When determining whether to admit evidence, an arbitrator must consider only its relevance. Excluding evidence “has to do with rules clearly grounded in legal principle, not with arbitrator’s preferences as to how people should behave in society, or with arbitrators’ conclusions about whether people behaved reasonably”. If the video surveillance tapes contain evidence that may be relevant to the case, they are admissible.

The approach taken by Arbitrator Welling is in contrast to the approach adopted by Arbitrator Lynk in the following decision.

¹⁰*Doman Forest Products Ltd. and I.W.A., Loc. 1-357* (1991), 13 LAC (4th) 275; *Steels Industrial Products and Teamsters Union, Loc. 213* (1992), 24 LAC (4th) 259.

*Labourers' International Union of North America, Local 625 v
Prestressed Systems Inc., [2005] OLAA No. 125*

Facts

The grievor was dismissed because the employer believed that he had misrepresented the severity of a back injury sustained at work. The employer intended to rely on video surveillance evidence that it had covertly captured while the employee was off-duty. The union objected to the use of the video surveillance tapes at the arbitration hearing.

Decision

Arbitrator Lynk held that employees in a unionized workplace have a general right to privacy. In so doing, he upheld the union's preliminary objection and determined that the video tapes were inadmissible, stating that "the Employer did not establish that it was reasonable, in all of the circumstances, to undertake the surveillance."

Analysis

1. Do unionized employees in Ontario have a general right to privacy?

Arbitrator Lynk stated at paragraph 32 that the general right of an employee to some degree of privacy has been recognized by labour arbitrators "with sufficient regularity and volume in recent years to be now considered as forming part of the 'common law' of the unionized Ontario workplace."

In rejecting several arbitration decisions holding that employees do not have a right to privacy, Arbitrator Lynk stated that those decisions improperly ignored the existence of the 'common law' of the unionized workplace, noting at paragraph 37:

Any statement on the scope of labour arbitration law would be deficit [sic] and incomplete without also including the interpretive function that arbitration awards play in building upon and adding to the law on workplace relations.

When an arbitral rule or principle is adopted by a number of arbitrators, it ultimately crystallizes and becomes part of this common law, and in Arbitrator Lynk's view, this occurs even without a governing statute or provision in the collective agreement.

Arbitrator Lynk determined that unionized employees in Ontario have a general legal entitlement to privacy in the absence of a statutory or collective agreement right.

2. Which test is the preferred approach for the admissibility of evidence?

Arbitrator Lynk held that in determining the admissibility of evidence an arbitrator must strike the appropriate balance between the employee's privacy interest and the employer's legitimate business interests.

Although the reasonableness test sets a higher standard for employers than the relevancy test, Arbitrator Lynk stated it is "neither onerous or unfair" because the employer's legitimate interests are still protected. The factors to be considered as part of the test are as follows:

1. whether the employer had a reasonable basis to engage in the covert surveillance; and
2. whether the surveillance was conducted in a reasonable manner.

Reasonableness will be measured on an objective standard. What is reasonable will depend on the context, including the basis for the employer's suspicion, the nature of the potential harm to the employer's business, the degree of impairment to trust, the alternatives available to obtain the required information, and the degree of intrusion caused by the particular surveillance method. The employer must explain why some readily available and less intrusive methods could not have accomplished the same goal.

Based on his authority to exclude evidence under s. 48(12)(f) of the *Labour Relations Act, 1995*, Arbitrator Lynk held that the video surveillance evidence was inadmissible because the employer did not establish the reasonableness of its decision to undertake video surveillance of the grievor.

The decisions in *Canadian Timken* and *Prestressed Systems* both focus on whether or not employees have a right to privacy in determining which test to apply in admitting video surveillance evidence. However, recent arbitral jurisprudence focuses more on the appropriate test to apply

in determining whether surveillance evidence is admissible than on the existence of a privacy right.¹¹

Woodbridge Foam Corp. v CAW-Canada, Local 222, [2009] OLAA No 269

Facts

The grievor applied for short-term disability benefits, alleging that she strained her back slipping in her shower. This was the grievor's 39th absence, in comparison to the plant average of seven for the same period of time. The grievor had made a total of 27 short-term disability claims, eight of which were for "slips and falls" occurring in or around her home, including two previous slips in the shower.

The employer put the grievor under video surveillance based on the similarity of the claim to two previous claims and the severity of her medical restrictions.

The union argued that the video surveillance evidence should not be admitted because it did not pass the reasonableness test set out by Arbitrator Lynk in *Prestressed Systems*. The employer argued that the evidence should be admitted because it was relevant.

Decision

The video tapes were not admitted at the arbitration hearing, because they did not meet the reasonableness test.

Analysis

Arbitrator Crljenica found that the reasonableness test in *Prestressed Systems* may be more difficult for employers to meet than the reasonableness test applied in other cases. He held that the following two-step test should be employed when determining the admissibility of surveillance evidence:

1. Was it reasonable, in all the circumstances, to undertake surveillance of the employee's off-duty activity?

¹¹ *Re Greater Toronto Airport Authority and Public Service Alliance of Canada* (2007), 158 LAC (4th) 97; *General Electric Canada and C.E.P. Local 544 (Re)*, [2007] OLAA No 8; and *Ready Bake Foods Inc. v United Food & Commercial Workers International Union, Local 175*, [2009] OLAA No 308m; *Thames Emergency Medical Services*, [2010] OLAA No 315.

2. Was the surveillance conducted in a reasonable way, which is not unduly intrusive and which corresponds fairly with acquiring information pertinent to the employer's legitimate interests?

In this case, the grievor's short-term disability history did not necessarily indicate dishonesty. Since there was no concrete basis for suspecting the legitimacy of the claim beyond the grievor's history, the employer could not establish that it was reasonable to undertake the surveillance. The video surveillance tapes were inadmissible.

Given that there was no express provision in the collective agreement and no statutory basis for this finding, it can be inferred that Arbitrator Crljenica found that employees have some right to privacy that constrains the ability of employers to conduct video surveillance where they are unable to meet the reasonableness test. The balancing of employee and employer interests inherent in the reasonableness test presupposes that unionized employees have some general privacy right or interest.

Kingston (City) v Canadian Union of Public Employees, Local 109,
[2010] OLAA No 146

Facts

The grievor was dismissed for faking a back injury and fraudulently collecting sick leave benefits. The grievor had competed in a golf tournament while he was on leave. The employer obtained video surveillance evidence of the grievor engaging in other demanding physical activities.

The union grieved the termination. At the beginning of the hearing, the union objected to the admissibility of the video surveillance evidence on the basis that it was a violation of the grievor's right to privacy.

Decision

An employee does not have an expectation of privacy in a public place. The video surveillance evidence was admissible because it was relevant to the issues in dispute.

Analysis

Arbitrator Starkman considered the two approaches that have been employed in the arbitral jurisprudence relating to the admissibility of video

surveillance evidence. He noted that the reasonableness test assumes employees have a right to privacy, and that the right must be balanced against the employer's right to investigate. In contrast, the relevance test is based on the notion that preventing relevant evidence from being submitted is a violation of the principles of natural justice.

Arbitrator Starkman concluded that the video surveillance evidence was admissible because it was relevant to the grievor's termination, but that there may be "circumstances in which issues about how, why, or where the surveillance was carried out might need to be examined", to determine if video surveillance is admissible. In this case, the surveillance had been performed in a public place, where there would be no expectation of privacy.

Arbitrator Starkman's reasons suggest that a reasonable expectation of privacy may render relevant surveillance evidence inadmissible, at least in certain circumstances, but no such circumstances were present in this case.

CHARTER RIGHT TO PRIVACY

In some circumstances, employees may have a right to privacy under the *Charter*. The *Charter* regulates government action. Accordingly, government bodies and their agents, which may include those acting on behalf of the police, may be vulnerable to employee claims that a search or seizure violated their reasonable expectation of privacy.¹²

Section 8 of the *Charter* guarantees the right to be free from unreasonable search and seizure. If s. 8 of the *Charter* is violated in gathering evidence, it may be excluded from evidence at trial.

Below is a summary of a recent decision of the Ontario Court of Appeal that held that a teacher had a reasonable expectation of privacy in his work computer.

***R. v Cole*, 2011 ONCA 218**

Facts

Cole was a high school teacher who taught computer science. He was issued a laptop computer by the School Board. The School Board's Policy and Procedures Manual (the "Policy") permitted personal use of the

¹² *R v Broyles*, [1991] 3 SCR 595.

computer, but provided that it was not be used for inappropriate content, including sexually explicit material. The Policy also provided that “all data and messages generated on or handled by Board equipment are considered to be the property of the Rainbow District School Board and not the property of the users of the technology.” However, the Policy did not provide for the search of the computers, except as it related to email. The Policy provided that the administrative team could “legally open private email if that action seems necessary for the ongoing ‘health’ of the system or if inappropriate use is suspected.”

In the course of monitoring the school’s network, one of the school’s information technologists remotely accessed Cole’s browsing history and one of his drives and found nude photographs of a young woman. The technologist took a screen shot, confirmed the young woman was a student and immediately informed the principal. Cole surrendered his computer to the principal upon request. The School Board’s technicians copied the photographs and Internet file onto a disc and provided them to police with the computer. Cole had accessed a student’s email account, found the photographs, and copied them onto his computer.

Police determined that a search warrant was unnecessary, as the school authorities had represented that they owned the computer and the data thereon. Police viewed the material and charged Cole with possession of child pornography and fraudulently obtaining data from another computer hard drive.

The trial judge excluded the evidence based on a breach of Cole’s s. 8 *Charter* rights. The summary conviction appeal judge overturned the decision, holding that Cole did not have a reasonable expectation of privacy in his computer’s contents.

Decision

The Ontario Court of Appeal held that, in the absence of a clearly worded employer policy, “the appellant had a reasonable expectation of privacy in the personal use of his work laptop.... Access to that information on the hard drive potentially exposed intimate details of the appellant’s personal choices and could have exposed intimate details of a personal nature.... This warrantless search [by the police] was not reasonable. Therefore, the police violated the appellant’s s. 8 [*Charter*] rights when they searched the laptop and the disc with the temporary internet files.”

The Court's Analysis

The Court considered the following issues:

1. Did Cole have a reasonable expectation of privacy in the contents of the laptop?

Based on the totality of the circumstances, the Court ruled that Cole had a reasonable expectation of privacy in the personal use of his work laptop. The School Board gave teachers explicit permission to use the laptops for personal use and to take them home on evenings, weekends and summer vacation. The teachers used their computers for personal use, they employed passwords to exclude others from their laptops, and they stored personal information on their hard drives. There was no clear and unambiguous policy to monitor or search the teachers' use of their laptops.

2. Did the school authorities breach s. 8 of the *Charter*?

The Court assumed for the purposes of this appeal that the *Charter* applied to the School Board and its employees.

The technologist's actions did not breach s. 8 of the *Charter*. Cole's reasonable expectation of privacy was modified to the extent that he knew that the employer's technologist could and would access the laptop as part of his role in maintaining the technical integrity of the school's information network. Having discovered the potentially illegal photographs, the technologist acted reasonably by taking a screen shot, confirming the girl was a student and contacting the principal.

Likewise, the principal did not violate s. 8 of the *Charter*. His search and seizure of the laptop were all implicitly authorized by law pursuant to s. 265 of the *Education Act* and the common law.¹³

The Court also found no fault with the School Board's subsequent actions because they were investigating a serious allegation of teacher misconduct and a threat to the school environment.

¹³ Specifically, *M.R.M.*, [1998] 3 SCR 393, a case involving a search by a junior high school principal of a student believed to be in possession of drugs on school property in which the Court held that teachers and principals must be able to act quickly to protect students and to provide an orderly atmosphere required for learning, and that a school official should not be held to the same stringent standard as police when conducting searches of students.

3. Did the police breach s. 8 of the Charter by searching the laptop and the compact discs without warrant?

The Court held that even though the discs and laptop were lawfully seized by the School Board and delivered to the police, the police still needed to obtain a warrant based on reasonable and probable grounds to conduct a search and seizure.

The Court had a different view of the photographs. The Court reasoned that the photographs were taken from the school's network, using the school's computer and were the subject of the privacy interest of a student and thus Cole had no personal privacy interest in the data. The photographs were found in plain view by the technician and so did not engage Cole's s. 8 *Charter* rights.

4. Did the trial judge err in excluding the evidence?

The Court ordered that the laptop and the mirror image of its hard drive be excluded from the evidence in Cole's trial. With regard to the disc containing the temporary Internet files from Cole's online browsing, the Court held that "such information can disclose personal preferences and interests, as well as freedoms of thought and association, which [Cole] would have a high expectation would remain private," and ordered that it be excluded as well, but with the proviso that the trial judge could re-assess its admissibility if the evidence became "important to the truth-seeking function" during the trial.