WORKPLACE PRIVACY & SURVEILLANCE

Presented by Joel Deeley and Greg Bartel

Introduction

In the landmark Ontario Court of Appeal decision, which recognized common law privacy protection for the first time in that province, the Court made the following observation[1]:

> For over 100 years, technological change has motivated the legal protection of the individual's right to privacy. In modern times, the pace of technological change has accelerated exponentially…The Internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information…routinely kept electronic databases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled and the nature of our communications by cellphone, e-mail or text message.

Unsurprisingly, Employers have taken advantage of the exponential and continuing growth and reach of technology to greatly enhance their ability to track employees. Whether in relation to workplace computers and email usage, video surveillance both in and out of the workplace, or location monitoring, Employers have more options at their disposal than ever before to keep an eye on their employees and, as a result, the invasion of workers' privacy is pervasive. Employers strive to validate such tactics on the basis of security, safety, deterrence, and a variety of other business reasons or interests. Whereas, for employees, privacy rights are a fundamental and growing concern.

As long ago as 1881, an English Appellate Court recognized: "[I]t is well established that persons do not by virtue of their status as employees lose their right to privacy and integrity of the person."[2] However, while employee privacy rights are not surrendered at the door of the workplace, neither are they always accorded paramountcy. The question, then, is what is the *reasonable expectation of workplace privacy* that an employee is entitled to hold?

As the cases discussed below will illustrate, arbitrators have generally sought to balance the privacy interests of workers with the countervailing, legitimate business interests of Employers. The critical starting point is that once an invasion of workers' privacy has been established, it is the Employer who must justify its privacy invasive action or policy. It is important and useful to understand the circumstances in which an Employer justification may be accepted as reasonable and where limits will be placed on attempts to invade workers' privacy, in order to appreciate how the legal landscape practically affects the rights of Canadian workers and how Unions can act to protect the privacy interests of their members.

---

[1] *Jones v. Tsige*, 2012 ONCA 32, at para. 67.

[2] *Latter v Braddell* (1881), 50 LJQB 448 (CA Eng), cited in *Monarch Fine Foods Co v International Brotherhood of Teamsters, Chauffeurs, Warehousemen and Helpers of America, Local 647 (Gogna Grievance)*, (1978) 20 L.A.C. (2d) 419 (Picher) at para. 8.

Legislation

In Canada, at both the federal level and provincial level, numerous pieces of privacy legislation have been introduced over the last twenty five years.

(a) Federal Legislation

At the federal level there are two privacy statutes: the *Privacy Act*, RSC 1985, c P-21 and the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("PIPEDA"). The *Privacy Act*, introduced in 1983, imposes privacy obligations on approximately 250 federal government departments and agencies by restricting the gathering, using and releasing of personal information.[3]

PIPEDA came fully into force in 2004. It provides privacy rights that apply to private sector organizations, protecting individuals in terms of the information that is collected, used, or disclosed in the course of commercial transactions.[4] PIPEDA also applies in the employment context to federally regulated employees (i.e. business that are engaged in federal works, undertakings, and businesses).[5] As a result, Employers in federal works, undertakings, or businesses must ensure that they collect, use, and disclose employees' personal information only for purposes that a reasonable person would consider appropriate in the circumstances, which is the standard established by PIPEDA.[6]

British Columbia, Alberta, and Quebec have private sector privacy legislation that is deemed to be "substantially similar" to PIPEDA, such that PIPEDA does not apply in these jurisdictions.[7] PIPEDA thus applies to the federally regulated private sector in all other provinces and territories.[8]

In 2013, legislation was introduced in Manitoba that is intended to be "substantially similar" to PIPEDA. Titled *The Personal Information Protection and Identity Theft Prevention Act* ("PIPITPA"), the legislation received Royal Assent on September 13, 2013. However, it has never been brought into force (and it is not clear whether it ever will).

(b) Provincial Legislation

Each province has its own public sector privacy legislation. In Manitoba, *The Freedom of Information and Protection of Privacy Act*, C.C.S.M. c. F175, provides a right of access to records held by public bodies and regulates how public bodies manage personal information.

---

[3] Office of the Privacy Commissioner of Canada, Factsheet: privacy Legislation in Canada, (May 2014), online: < http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp>.
[4] PIPEDA, at s. 4(1)(a).
[5] Ibid at s. 4(1)(b).
[6] Officer of the Privacy Commissioner of Canada, Factsheet: Application of the Personal Information Protection and Electronic Documents Act to Employee Records, (May 2004), online: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_18_e.asp>.
[7] PIPEDA, at ss. 4(3), 26(2)(b).
[8] PIPEDA, at ss. 4(1)(a), 4(3).

The Personal Health Information Act, C.C.S.M. c. P33.5 and *The Mental Health Act*, C.C.S.M. c. M110 are both health specific privacy legislation, governing personal health information.

The Privacy Act, C.C.S.M. c. P125, creates a tort where a person who substantially, unreasonably, and without claim of right, violates the privacy of another person.[9] Surveillance is expressly included in that Act as an example of a potential privacy violation.[10] Various defences are available under the Act to a defendant in an action for violation of privacy of a person.[11]

A review of case law dealing with privacy issues reveals that arbitrators seem somewhat reluctant to consider and apply privacy legislation to disputes before them, more often than not falling back instead on the balancing of interests approach that has traditionally been applied, in which individual worker privacy rights are balanced against the employer's business interests without express regard to any legislative tests, restrictions, and processes. This disinclination will likely change as more privacy protection arguments are advanced on the basis of legislation.

(c) *The Canadian Charter of Rights and Freedoms*

Section 8 of the *Charter* reads "Everyone has the right to be secure against unreasonable search or seizure." The protections of s. 8 apply only to workers whose employer is government for the purposes of the *Charter*. The common law rule is that a government official has no authority to enter private property for the purpose of searching for evidence, and no authority to seize private property for use as evidence, unless authorized by [a reasonable] law.[12] A "search" consists of an examination by agents of the state of a person's person or property in order to look for evidence, and a "seizure" is the actual taking away, by the agents of the state, of things that could be used as evidence.[13]

The protection against unreasonable search and seizure is a privacy right, and not a property right.[14] As such, the case law and commentary focuses on the protection against intrusion on a person's reasonable expectation of privacy against investigative or other criminal justice activities of the state.[15]

Section 8 will not apply where the person searched had no reasonable expectation of privacy.[16] Whether a person has such an expectation will be assessed based more on context than on physical space,[17] and the concept is based on a balance between the public's interest in privacy and the government's interest in advancing goals like law enforcement.[18]

---

[9] *The Privacy Act*, at s. 2(1).
[10] *The Privacy Act*, at s. 3.
[11] *The Privacy Act*, at s. 5.
[12] Hogg 48.2.
[13] Hogg 48.4(a).
[14] *Halsbury's Laws of Canada, Constitutional Law (Charter of Rights)* – 2014 Reissue, IX Legal Rights: Sections 8 to 14, 1. Unreasonable Search or Seizure, HCHR-68 Purpose of right and general approach.
[15] HCHR-68.
[16] Hogg 48.4(b).
[17] HCHR-68.
[18] HCHR-69.

General Approach to Privacy Issues

In jurisdictions that have not enacted privacy legislation applicable to employment matters, employee privacy rights are less clear. In unionized workplaces, arbitral case law has long recognized workplace privacy rights (for example, in relation to drug and alcohol testing, medical information, and searches of employees and their property). However, some arbitrators have rejected the proposition that employees have privacy rights in jurisdictions that are not governed by privacy legislation. Where privacy rights are recognized by arbitrators, they are generally assessed with reference to the applicable collective agreement and approached through a balancing of interests analysis.

In order for an Employer to unilaterally take an action or impose a policy that involves an invasion of workers' privacy, arbitrators have found that it must have reasonable justification to do so. In this regard, arbitrators will generally consider the following:

- Whether the action or policy is reasonably required in the circumstances; and
- Whether the action or policy is conducted in a reasonable manner.

This arbitral balancing approach reflects the well-known *KVP* test, which is applied to unilaterally imposed Employer policies or rules that regulate employee conduct, and requires that such policies or rules be consistent with the collective agreement and reasonable.

In 2013 the Supreme Court of Canada released ***Irving Pulp & Paper Ltd. v. CEP, Local 30*, [2013] 2 S.C.R. 458**. This important decision reaffirmed the *KVP* approach to the assessment of unilateral management rules. In addition, ***Irving*** set the benchmark for assessing such rules in the context of privacy rights (in the context of a random alcohol testing policy). As the Supreme Court noted in ***Irving***, many of the management policy cases balance employer business or operational interests with employee privacy rights.

Workplace Privacy Issues

1) Computer and Email Monitoring

***R. v. Cole*, 2012 SCC 53**

This Supreme Court of Canada decision remains the leading case on workers' privacy rights regarding technology in the workplace. In it, the Court declared that employees have an expectation of privacy with regard to personal information contained on workplace computers where personal use of the computers is permitted or reasonably expected.

In this case, a high school teacher's laptop computer, provided and owned by the school, was found to contain sexually explicit photos of a grade 10 student at the school and other pornographic images on its hard drive by a school technician who, after noticing a large amount of activity between the teacher's laptop and the school's server, remotely accessed the hard drive to perform a virus scan and verify the integrity of the system.

While the Court held that the employer's actions, including searching the laptop, copying the temporary files of the teacher's surfing history and the images onto disks, and turning the laptop and disks over to the police, were justified by its authority under the provincial *Education Act* to maintain a safe school environment "and, by necessary implication, a reasonable power to seize and search a school-board-issued laptop if the principal believed on reasonable grounds that the hard drive contained compromising photographs of a student", it held that the subsequent warrantless search conducted by the police violated the individual's right in s. 8 of the *Charter* to be secure against unreasonable search and seizure. However, the Court found that the breach of *Charter* rights was not egregious in this instance because the investigating officer had acted in good faith and a warrant would have been easily obtainable, and therefore ruled that the illegally obtained evidence (pornographic images) should be admitted at a new trial of the charges against the teacher.

Writing the Court's 6-1 majority decision, Justice Morris Fish declared that "[t]he Court left no doubt in *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, that Canadians may reasonably expect privacy in the information contained on their own personal computers. In my view, the same applies to information on work computers, at least where personal use is permitted or reasonably expected. Computers that are reasonably used for personal purposes – whether found in the workplace or the home – contain information that is meaningful, intimate, and touching on the user's biographical core. Vis-à-vis the state, everyone in Canada is constitutionally entitled to expect privacy in personal information of this kind."

Ownership of the computer by the school board was not determinative of the teacher's expectation of privacy, the Court observed, and while workplace policies and practices might diminish an employee's expectation of privacy, the Court emphasized that these operational realities did not remove the expectation entirely: The nature of the information at stake exposes the likes, interests, thoughts, activities, ideas, and searches for information of the individual user. Such was the case here. [The individual], a high-school teacher, was permitted to use his work-issued laptop computer for incidental personal purposes. He did. He browsed the Internet and stored personal information on his hard drive." The scope of that expectation depended, in the Court's view, on the "totality of the circumstances."

The foregoing summarizes the gist of the Court's decision, which involved solely an issue of admissibility of evidence in a criminal prosecution. However, in the course of its decision, the Court endorsed the right of a school board to intrude on the workplace privacy of its employees if this is required by its duty to maintain a safe school environment. As to the law as it affects other public sector employers, as well as private sector employers, and the employees of both, the Court was not explicit, deciding to "leave for another day the finer points of an employer's right to monitor computers issued to employees."[19] Nonetheless, it can be anticipated that, in administering labour law, given their inclination to apply *Charter* values, arbitrators and courts may adopt the following principles laid down by the Court:

[19] Para. 60.

1. Employees have an expectation of privacy in personal information stored on workplace computers where personal use of the computer is permitted or reasonably expected.

2. This privacy expectation may be diminished by the employer's ownership of the computer, but the totality of the circumstances, including workplace policies and practices, will be considered in making such a determination.

3. In this regard, a restrictive employer policy will not necessarily prevail if in practice the employer allows personal use by employees of workplace computers.

4. If an employee's reasonable expectation of privacy is violated, personal information obtained thereby may be excluded as evidence in an arbitration case or a civil suit.

The Supreme Court's affirmation in ***Cole*** that employees do have a reasonable expectation of privacy in the personal component of their workplace computers might seem to enhance the privacy rights of employees. However, the Court also confirmed that Employers may have countervailing rights with respect to their computer equipment, which rights would include the power to discipline employees who commit employment misconduct in the course of using employer-owned computers and communication devices.

The following two cases provide examples of the application of ***Cole*** by Labour Arbitrators, with differing outcomes. It should be noted that both cases are discipline cases and the different outcomes are accordingly fact-driven.

Elementary Teacher's Federation of Ontario v. York Region District School Board. 2022 ONCA 476, 2022 CarswellOnt 8666.

This is a recent case in which the Ontario Court of Appeal applied the principles from ***Cole*** to a case involving worker's personal documents accessed through a Cloud-based application on a workplace computer.

In this appellate decision, the Court of Appeal found that the Board's search of an employer-owned computer breached Section 8 of the ***Charter,*** overturning the Trial Court's decision that the worker's had a diminished expectation of privacy because the document was left in "plain sight."

The facts of this case are that ill will arose between four grade two teachers at a public school due to feelings of preferential treatment by the Principal. Following advice from their Union, the Grievors, S and R kept a log of their concerns related to preferential treatment.

The log was password protected and accessible only to the two grievors; both could contribute to the log and read it. Although the log could be accessed using an internet browser on a workplace laptop, it was not saved on any workplace drive or on the laptops. The log was stored in a Cloud application on S's private Google account.

Three people told the principal of their concerns about the environment in the workplace and the possibility that the grievors were keeping a log. The principal discussed the matter with the Board Superintendent, who advised him to speak with human resources. He did so, and the IT

department searched the Board's online files to see if there were any files shared between the grievors. Nothing was found. A search of the school's hard drives and Google drives also failed to find anything.

The principal entered S's classroom after classes had ended and she had left for the day. He saw that the laptop computer provided by the school for classroom use was open and touched its mousepad. A document called "Log Google Docs" opened on the screen. He read the document and began to scroll through it. He realized that this was the grievors' log and used his cellphone to take screenshots of the entire log.

The Board issued letters of discipline to the grievors for failing to conduct themselves in accordance with the Ontario College of Teachers' Standards of Practice. The letters referred to the fact that the grievors had used Board technology to access and maintain a log during Board time and had made approximately 100 entries about the principal and another teacher. The Board placed written reprimands on their files for three years.

The arbitrator noted that, as in ***Cole***, the laptop computers in question were not for the grievors' exclusive possession and use; they were owned by the Board and were for classroom use by students as well as teachers and the principal. Nor were the laptops secure: one of the grievors had left her laptop password (but not her personal Gmail log password) on a post-it note attached to her laptop. However, the grievors had not stored personal information on the Board's laptop computers. In these circumstances, the arbitrator found that the grievors had a diminished expectation of privacy concerning information that was accessible on the laptop computers. However, the arbitrator found that because Ms. Shen left the grievors' log open on the Board's laptop, she had only a diminished expectation of privacy.

The appeal concerned the principal's actions in reading the grievors' log, taking screenshots of the entries, and sending the screenshots to the Board, which then relied on this evidence to discipline them. The Court of Appeal found that the arbitrator erred in several respects by finding that the grievor’s had a diminished expectation of privacy.

The Court found that the grievors did all that they could to protect the privacy of their communications. Their log was at all times password protected and reserved to their use. The grievors had every reason to expect that their conversation was, and would remain, private. The grievors' subjective expectation of privacy was objectively reasonable and deserving of protection. Their log was simply an electronic record of their private conversations. Many private conversations occur electronically rather than in person or by telephone, through email, texting, or similar means. The potential for personal information being revealed in such conversations is great.

The Court of Appeal emphasized the *potential* for personal information to be revealed citing reasoning in the Supreme Court of Canada decision of ***R. v. Marakah,*** where the SCC found that the objective reasonableness of an expectation of privacy is determined having regard to the potential for personal information to be revealed, not whether the information revealed is in fact personal.

The Court of Appeal found that whether the grievors' log contained intimate details about them was not relevant to whether the grievors' private communications should be protected. The grievors' log was analogous to their diary. They were entitled to record their private thoughts — including complaints about co-workers and supervisors for their own purposes and to expect that those thoughts would remain private.

The Court went on to note that the grievors' reasonable expectation of privacy in their log was not diminished as it would have been if, for example, the grievors had deliberately provided access to the log to third parties; stored their log on the Board's laptop computers where it would be widely accessible; or were otherwise indifferent to their privacy.

Regarding the reasonableness of the search, the Court found that the arbitrator erred in concluding that because the principal found the log by happenstance, the Board was absolved of responsibility for the principal's actions or makes the search reasonable. Once the principal realized he was looking at the grievors' log, it was as though he had found their diary. He had no legitimate purpose in reading it, let alone taking screenshots of it and submitting it to the Board. The principal failed to respect the grievors' reasonable expectation of privacy.

The Court of Appeal concluded that a person's thoughts about others are no less personal to them than their thoughts about themselves. The grievors were within their rights to be judgmental — to criticize the school, their fellow employees, and the principal in their private communications. Their private thoughts were not to be mined by the school principal to address his employment relations concerns, no matter how innocently the principal may have come upon the log or how pressing his concerns were.

Leave to appeal to the Supreme Court of Canada granted in ***2023 CarswellOnt 3510.***

Amalgamated Transit Union, Local 1587 and The Crown in Right of Ontario (Metrolinx) 352 L.A.C. (4th) 219, 2023 CanLii 72192 (ON GSB).

Arbitrator Luborsky dealt with a termination grievance of five bus drivers terminated for alleged sexual harassment after the Employer's investigation concluded they engaged in a series of WhatsApp messages on their personal cell phones which included sexually inappropriate comments about their co-workers that suggested they had obtained promotions in exchange for performing sexual acts on supervisors.

The arbitrator noted that arbitrators "have always drawn a line between employees' working and private lives" and that "an employer has no jurisdiction or authority over what employees do (including where they live), outside working hours, unless it can show that its legitimate business interests are affected in some way." Thus, saying dirty words or expressing reprehensible thoughts amongst one's own friends while off-duty and outside of work, even where some of those friends are workmates, is not the employer's concern unless it can establish a real (as opposed to hypothetical or speculative) nexus to the workplace itself having a negative impact on its business.

The arbitrator found that WhatsApp messaging, unlike other social media platforms which are more public in nature, provides for encrypted private conversations which would reasonably be

expected to be kept private by those engaging in the messaging. In that respect, the conversations were similar to private conversations and, given they occurred after work hours, the Employer did not have the right to investigate and impose discipline.

In reaching his conclusions, the arbitrator was also very critical of the manner in which the employer conducted its investigation including its demand that an employee disclose the contents of his personal cell phone under threat of discipline which violated the employee's right to privacy. This improperly obtained evidence led to the employer conducting a "fishing expedition" to find evidence against the employee's colleagues. Because of this privacy violation, all evidence obtained that implicated the grievors was deemed inadmissible.

"A personal cellphone is a very private device. It is fair to say that for some people, it is part of their very being…Unless the employer can establish a clear contractual right to disclosure of any of the contents of an employee's personal cellphone, or can point to some statutory or judicial authorization for access to the records of anything within that device…the employer has no right to demand, let alone receive, any of the contents of that cellphone."[20]

The arbitrator also concluded that, even if he had allowed the improperly obtained evidence, he would have concluded that there had been no violation of the employer's harassment policy. There was no evidence that the conduct of the grievors (which the arbitrator acknowledged was entirely juvenile and inappropriate) was conduct that occurred in the workplace and was known or ought to reasonably have been known to be unwelcome, or that the words transmitted were demonstrated to have had a negative impact manifested within the workplace.

All of the grievors were reinstated with full compensation and no loss of seniority.

***SGEU and Unifor, Local 481 (Admissibility). Re*, 2015 CarswellSask 278, 255 L.A.C. (4th) 353 (Ponak)**

In this preliminary award, a Saskatchewan arbitrator held that personal e-mails between a public servant and his wife, found on the employer's e-mail system during an investigation into allegations that he was affiliated with a biker gang, were not admissible in the arbitration hearing reviewing his dismissal. He concluded that the employee's privacy rights outweighed the business interests of the employer.

Reviewing the legal framework, Arbitrator Ponak observed that it has long been recognized in arbitral jurisprudence that employees have privacy rights in the workplace, which are to be balanced against an employer's right to manage its workplace, including the right to investigate allegations of employee misconduct. In addition, Arbitrator Ponak observed that with the increasing prevalence of computers, mobile devices, and e-mail, the issue of employee privacy rights on employer-owned devices and networks has received "increasing attention."

Arbitrator Ponak accepted that ***Cole*** was a "leading case" in this area and was "instructive", despite the fact that the Court did not fully explore the issue of an employer's right to monitor

[20] ATU, Local 1587 and Ontario (Metrolinx) (Juteram), Re. 2023 CarswellOnt 11202, 2023 C.L.A.S. 417, 352 L.A.C. (4th) 219 at para 110.

employee computer use, as opposed to access by the police, noting that the Court in that case had determined that the employee had a reasonable expectation of privacy with respect to his information on the employer-owned laptop even though the employer's policies explicitly stated otherwise. Arbitrator Ponak quoted extensively from the decision, including its statement that "[w]hatever the policies state, one must consider the totality of the circumstances in order to determine whether privacy is a reasonable expectation in the particular situation," and that "[t]he closer the subject matter of the alleged search lies to the biographical core of personal information, the more this factor will favour a reasonable expectation of privacy. Put another way, the more personal and confidential the information, the more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest."

Applying these principles to the facts before him, Arbitrator Ponak held that although the express stipulation in the employer's IT policy that employees' communication were not private reduced an employee's reasonable expectation of privacy, it did not "extinguish [it] completely", emphasizing the prevalence of technology in modern society and the inevitability that employees will at some point use their employer-owned cell phones or computers for personal purposes. In his view:

> [T]he SGEU's strong IT policy pronouncements notwithstanding, inevitably some personal emails will be sent and received on the SGEU's system. … Given that it is unrealistic to expect … the SGEU email system to be entirely free of employee personal emails, can the SGEU still claim the right to examine these emails at will? Regardless of what its policy says, the answer must be no. Employees do not automatically lose any right to privacy simply because they happen to send or receive a personal email on the employer's email system. *Cole* is clear in this regard when it says that "written policies are not determinative of a person's reasonable expectation of privacy" (paragraph 53). Neither is ownership as long as it is unreasonable to expect that no personal emails will find their way onto a business email system (*Cole*, paragraph 51). Employees know that there will be at least some leakage of their personal emails onto the SGEU system; this fact translates into some expectation of privacy (*Cole*, paragraph 58).

Consequently, Arbitrator Ponak held that an employer may examine an employee's personal e-mails only where reasonably justified in doing so, articulating the test as whether the search was "reasonable in the circumstances and carried out in a reasonable manner" and stipulating that "while not necessarily the last resort, a search that is very intrusive on privacy ought not to be the first resort, especially if reasonable alternatives exist to acquire the information being sought."

In the circumstances of the present case, Ponak was not satisfied that a search of the grievor's personal e-mails was reasonably justified. Although recognizing that the employer's legitimate concern regarding the allegations of misconduct provided probable cause for an investigation, he did not accept that this extended to examining the grievor's e-mails. In his words: "The legitimate need to investigate did not necessarily give the employer *carte blanche* to conduct a particularly intrusive search of the grievor's personal e-mails." Moreover, emphasizing that "personal communications between a husband and wife are, by definition, among the most intimate and personal of all communications," he determined that the grievor had a heightened expectation of

privacy in these communications. Determining that the search of these e-mails was not reasonable, Ponak reasoned:

> [W]hile the need for an investigation of the grievor was justified, the search of e-mails to and from his spouse was not reasonable at the time it was carried out. Relying only on second or third hand information about the grievor, the employer's first and immediate response was to scrutinize his personal e-mails. There was no evidence that alternatives to this invasive search were considered, possibly because the employer believed that it owned the e-mail system and no barrier existed to such scrutiny. It was also relatively simple to carry out.

Arbitrator Ponak held that "this degree of intrusion into the grievor's personal e-mails was a violation of [his] reasonable expectation of privacy," and constituted an unreasonable search that was not justified in the circumstances. As a result, he ruled the e-mails inadmissible as evidence in the arbitration.

Re University of Manitoba and AESES (B .(A.)) **(2015), 258 L.A.C. (4th) 240, 124 C.L.A.S. 7, 2015 CarswellMan 388 (Peltz)**

The grievor was a highly educated and highly skilled individual. He worked as a Technology Transfer Specialist (TTS) in the University of Manitoba's Technology Transfer Office (TTO). The work of the TTO involved the development, promotion and protection of intellectual properties — the commercialization of the inventions of university researchers. The TTS's worked independently and were accorded a high degree of trust.

The grievor was discharged for breaching that trust and for insubordination. TTS's were provided with employer-issued cell phones for use in their work. The TTO director met with the grievor to discuss his "unusual" cell phone bills, which included excessive personal calls. The pattern and number of calls suggested to the director that the grievor, who was married with children, was involved in a relationship with someone else. The grievor was very concerned that his private life would become exposed. He offered repayment and assured the director that the personal calls would stop (which they did). The director replied that repayment was not necessary. But he offered some "friendly" advice to the grievor to be careful because he was in "dangerous territory". The director was alluding to the affair, which the grievor later admitted he was having and was trying to hide. At the arbitration hearing the grievor gave a somewhat different version of this conversation and stated that in his view the director was threatening him.

Concerned that his private phone records were being inspected, after the meeting the grievor altered university phone records, deleting sections which contained details of personal information. During this process the grievor accidentally deleted similar information from the phone records of other employees. This was contrary to the university's information security policy. The university discovered the altered phone records and convened a meeting with the grievor. A decision had already been made to place the grievor on paid leave, but the director wanted to give the grievor an opportunity to explain his actions.

At the meeting the grievor did not deny altering the phone records, but insisted that the personal components belonged to him and he had a right to alter them. He was told that he was being placed on paid leave pending an investigation regarding the record alterations, his cell phone and his computer. He was therefore given clear notice that his electronic records would be searched. The grievor was told to return his phone and keys. He left the meeting to return to his office to retrieve them. The TTO director, who had followed him, found the grievor in his office with his door closed, wiping his phone. The director repeatedly told him to stop, but the grievor ignored him. He handed over the phone only after it had been wiped clean. The following day management discovered that they could not re-start the grievor's computer. The grievor denied removing the hard drive and suggested that the computer might have been damaged by his "hard shut down" just before he was escorted from the premises.

The management group met to consider their options. There was "shock" that the grievor had deleted the contents of his cell phone after being told, repeatedly, to stop. There was also concern that the grievor might have compromised TTO operations by releasing confidential information of economic value. Although the grievor had an excellent work record and no disciplinary history, the university viewed his actions as irreparably breaching the trust that was so essential in this particular employment setting. Consequently the university decided that discharge was the only option.

The union characterized the grievor's wiping of the cell phone as an impulsive act: The grievor panicked at the prospect of his affair becoming public. The union argued that the grievance should be viewed in light of the growing recognition of privacy rights. The employer replied that the grievor's privacy was never at risk; and in any event he never gave the university an opportunity to invoke its reasonable protocols for protecting personal information, because he unilaterally deleted everything, in defiance of a direct order.

Arbitrator Peltz made two important factual findings which diminished the grievor's credibility: He ruled that in warning the grievor to be careful the TTO director did not threaten him, nor was there any reasonable basis for that perception. He also rejected the grievor's claim that it was too late to comply with the order to stop wiping his phone because he had already initiated a reset before he was told to stop. On the other hand, he found that the university did not establish that the grievor intentionally disabled his computer; the evidence in that respect was inconclusive.

As to the alteration of phone records, the grievor changed university records for the purpose of sheltering his personal calling history; but he had no business doing so:

> It is one thing to say that digital privacy is now highly valued in Canadian society. It is something else to claim a unilateral self-help remedy without even consulting the employer whose records are being altered.

The arbitrator found that upon discovering the alteration of records, the university had reasonable grounds to investigate. Other records could have been at risk.

The alteration of records breached university policies and constituted just cause for discipline. Had the grievor's misconduct ended there, progressive discipline might have been appropriate.

However, the grievor, knowing the employer wanted to examine his phone, wiped it clean in defiance of clear, repeated orders to stop. Although this was an impulsive act, at the same time it was characterized as “clear headed and intentional.”

The union did not deny that the grievor was insubordinate; instead, it invoked the privacy exception to the “obey and grieve later” rule. The problem for the grievor was that he never invoked the exception at the time. The onus was on the grievor to establish that his claim fell within the exception; and to take advantage of the exception, he should have clearly communicated his privacy concerns and allowed the employer an opportunity to respond. Instead, he foreclosed any discussion of the issue. Arbitrator Peltz concluded that under the circumstances, the grievor was not entitled to claim the privacy exception.

The union also pointed out that there was no explicit monitoring policy in place. However, Arbitrator Peltz noted that the employer’s IT policies did confer responsibility on IT security personnel to investigate security breaches. He stated, “given the TTO context where confidential information of great economic value must be preserved, it is inconceivable that the grievor would believe his cell phone contents would be immune from scrutiny.”

Having concluded that the university’s proposed search was reasonable, the arbitrator also concluded that the grievor’s deliberate thwarting of the investigation amounted to just cause; and when the unauthorized alteration of university records was “added to the mix”, the employer was justified in bypassing progressive discipline.

The grievor had some strong mitigating factors in his favour: an excellent work record and no disciplinary history. However, the aggravating factors outweighed the mitigating factors: in particular, the grievor’s refusal to admit wrongdoing and his lack of remorse. In other words, he had no rehabilitative potential, no hope of rebuilding the loss of trust. Accordingly, the arbitrator upheld the penalty of discharge and dismissed the grievance.

Elementary Teacher’s Federation, ATU, SGEU**,** and ***University of Manitoba*** emphasize the significance of the privacy interest in digital devices and the intrusiveness of searches of the devices and digital communications. Yet the privacy rights attaching to these devices are not absolute; they may be modified by legitimate countervailing rights, such as an employer’s right to monitor use of its IT equipment and to investigate suspected wrongdoing.

The decision of the Ontario Court of Appeal in ***Elementary Teacher’s Federation*** found that the search of a log stored on the grievors’ Cloud application was a breach of s. 8 of the Charter, emphasizing the importance of the reasonable expectation of privacy having regard to the potential for personal information to be revealed, not whether the information revealed, was in fact personal. Similarly, in ***ATU*** the communications between coworkers using WhatsApp was found to be akin to private communications because of the encrypted nature of the communication. As such, the Employer did not have the right to investigate and impose discipline for the private communication. Further, in ***SGEU*** the highly personal e-mails between the grievor and his wife were ruled inadmissible, not because the employer lacked grounds to investigate serious allegations of misconduct, but because there really was *no investigation*. The employer immediately rushed to search the grievor’s messages; it neither considered nor attempted less

intrusive means of determining whether the grievor was involved in activity which could undermine the employer's operations — less intrusive options being a factor considered important by many arbitrators when assessing breaches of employee privacy rights. By contrast, in ***University of Manitoba*** the grievor deprived the employer of any chance to investigate. Alerted to a pending investigation, he precluded that prospect by wiping his cell phone. Given the sensitive nature of information he handled in his job, the arbitrator accepted that the university would be alarmed by the grievor's actions and found the proposed search of all the grievor's records to be reasonable.

Given the prevalence of cell phones and related devices, it is unrealistic to expect that there will be no mixture of personal and work use when employees are issued cell phones in the course of their employment. But with or without policies permitting personal use, asserting employer ownership in the devices, or warning of monitoring, it is equally unrealistic to expect that personal messages on such devices will be immune from employer scrutiny. Discovery remains a possibility; and the above cases, despite their differing outcomes, highlight the wisdom of anticipating such a possibility.[21]

Association of Management, Administrative and Professional Crown Employees of Ontario (Bhattacharya) v Ontario (Government and Consumer Services), 2016 CanLII 17002

This case offers a different application of ***Cole*** – to a government employee's personal USB stick. The Board found that the grievor had only a limited expectation of privacy over certain personal files on the USB key and declined to exercise its jurisdiction to exclude the evidence found during searches of it.

The grievor began working as a business analyst for the Ministry of Government and Consumer Services. Several years later, a series of four anonymous e-mails were sent to various individuals within the provincial government. The e-mails made unsupported allegations about the conduct of the grievor's Branch Manager, Mr. Tee.

Following this series of e-mails, a USB key was found in the grievor's workplace and was eventually given to Tee. The USB key bore no identifying marks. Fearing that government documents may have been on the device, Tee opened files on the key at least four different times before submitting it for a forensic investigation. During these searches, Tee identified what appeared to be government documents, as well as several of the grievor's personal files.

The results of the forensic investigation came back and of the hundreds of files on the USB key, 106 files were identified that were "government related documents." These "government related documents" included PowerPoint presentations that the employer described as "very sensitive and confidential." The forensic investigation also revealed a draft of one of four anonymous e-mails about Tee.

[21] Willis & Winkler on Leading Labour Cases 2016, III: CURRENT DEVELOPMENTS IN LABOUR RELATIONS, Chapter Five — Informational Privacy in the Workplace.

When he met with the employer to discuss the results of the investigation the grievor denied knowledge of the PowerPoint presentations and the anonymous e-mail, but eventually admitted that the device was a USB key he had misplaced. The grievor was dismissed.

As a preliminary matter, the Association sought to exclude the evidence obtained through the searches of the grievor's USB key.

The Board accepted the approach outlined in ***Cole***, but did not find that it was directly applicable in this case because, unlike a computer, the owner of a USB key decides what is and is not stored on the device:

> A USB key, on the other hand, is [a] storage device. It does not have independent connectivity to the internet. I would not expect it to contain an "electronic roadmap of … cybernetic peregrinations", and there is no evidence in this case that the USB key in question does. Further, a USB key has no independent capacity to create, copy, scan, save or delete documents, and thus has no independent usage history of such activities. It must be connected to some other device which has the capacity to perform these functions. The user determines what content of the other device to copy to the USB key. It is unlikely the entire contents or usage history of the other device will be copied to the USB key.

However, the Vice-Chair also declined to endorse a low threshold for admission of evidence found through surveillance, i.e. mere relevance. Rather, he noted, Board jurisprudence directed Vice-Chairs to exclude otherwise relevant evidence if an employer's interests do not outweigh the privacy interests of an employee.

After making these initial observations, the Vice-Chair held that the grievor had a reasonable expectation of privacy over certain personal files on his USB key. Specifically, he ruled that, while the Ministry's I&IT Policy required IT resources to be used for work purposes, this broad policy did not eliminate the grievor's reasonable expectation of privacy. Referring to ***SGEU***, the Board observed that it was equally reasonable to assume that the presence of work-related documents on a personal USB key would not completely remove the grievor's expectation of privacy.

However, the Vice-Chair did point to one significant element distinguishing the informational content of the e-mails in ***SGEU*** and the files on the grievor's USB key. In the former case, the arbitrator was dealing with e-mails between the grievor and his wife; in the present matter, the USB key contained both personal files and work-related documents. Therefore, while the grievor retained a reasonable expectation of privacy over family photographs and passport applications, he had no such expectation in respect of work-related documents he intended to share. Further still, when analyzing the actual files Tee accessed during his limited searches, the Vice-Chair found that "… while some of the informational content viewed by Mr. Tee touches upon the biographical core of the [grievor], the touch is fleeting at best."

The Board considered the reasonableness of conducting these searches in the first place. Since Tee had suspicions that the USB key could contain work-related documents, the Board determined that Tee had a rational basis to conduct limited searches.

In short, when the grievor's limited expectation of privacy was balanced against the employer's reasonable and limited searches, the Board concluded that the evidence found on the USB key was admissible.

For the same reasons, the Vice-Chair concluded that the Association's arguments about a breach of s. 8 of the *Charter* were without merit. In any event, he ruled, the employer's broad I&IT Policy gave the employer the legal authorization needed to conduct a search in accordance with the *Charter*. However, in Anderson's view, the evidence from the searches was important enough to outweigh any minor breach of s.8.

Although the grievor was ultimately unable to exclude the evidence found on his USB key, the recognition that he had a reasonable expectation of privacy over some of the documents follows the general trend of expanding the right to privacy. Additionally, this case is a good example of how arbitrators can adapt privacy law to new forms of technology. In this award, the Board compared and contrasted a USB key with laptop computers, and, in doing so, was able to use established case law to create a framework that applied to this particular device. As new forms of digital technology enter the workplace, decision-makers can utilize a similar line of analysis.

2) Background Checks

Privacy interests are also engaged by a request to submit to a criminal background search. A request for such a search is not unusual when individuals apply for employment in work with vulnerable populations, however, a distinction has been drawn in the case law between prospective employees and existing employees.

Re Rouge Valley Health System and ONA (13-40) (2015), 259 L.A.C. (4th) 125, 2015 CarswellOnt 16480 (Stout)

In this case, the hospital in question had an existing policy of conducting criminal record checks for volunteers. An HR/payroll audit process recommended that the hospital conduct criminal background checks as part of its hiring process. The hospital's board of directors approved a new policy to that effect. However, the hospital went one step further and decided to apply the criminal background check policy to all existing employees. The policy required both a criminal record check ("CRC") and a vulnerable sector check ("VSC"), which involved a much more extensive search, including information concerning all police contacts: unproven allegations, complaints and pardoned offences — records which were not readily available to the public. As the hospital conceded, the application of such a policy to existing employees was unprecedented.

The nurses' bargaining unit challenged that aspect of the policy which applied to existing employees, arguing that a search of existing employees' records violated the *Criminal Records Act*, and regulations thereunder. ONA also argued that the policy represented an unreasonable exercise of management rights because the searches in question violated employees' privacy rights. Arbitrator Stout agreed with the union on both counts.

The arbitrator first dealt with the issue of the vulnerable sector check ("VSC"). Such a search would disclose convictions for certain types of offences where a "pardon" had been granted. He found that based on the legislation, the exception in the *Criminal Records Act* for disclosure of

such information only applies to persons *seeking employment* and *not those existing* employees that were captured by the hospital's policy. Since the policy required VSC for *existing* employees, that part of the policy was invalid as contrary to the *Criminal Records Act*. Arbitrator Stout found support for this conclusion in the legislative history, which provided the context for the amendments to the *Criminal Records Act* that included the new exception to the general rule of nondisclosure of pardoned records. Additionally, the *Criminal Records Act Regulations* referred to "applicant[s]" and "making application", which also supported his determination. He found the language in the *Criminal Records Act* to be clearly aimed at prospective employees and not existing employees.

The arbitrator also found, however, that if he was wrong in his interpretation of the *Criminal Records Act*, then the Policy was an unreasonable exercise of management rights.

The arbitrator began his balancing of interest analysis by indicating that arbitrators have long acknowledged the right of employees to privacy. Although he acknowledged that some information sought in a criminal background check may be part of the public record, for instance, a criminal charge or conviction, he nevertheless stated that these records are not something readily accessible to the general public and are still considered private. Moreover, records that may be disclosed by a VSC contain a tremendous amount of information that is not available to the public, including information about police contact (such as allegations, complaints, and mental health information). Accordingly, Arbitrator Stout found that there was a reasonable expectation of privacy attached to the records that were searched as a part of the hospital's policy.

According to the arbitrator, the union quite rightly did not take issue with the part of the policy that required checks for new employees; the problem lay in the application of the policy to existing employees. In his view, there was a distinction between the application of this kind of search to individuals seeking employment and those already employed — choice. Applicants had the option of walking away from the prospect of a job which entailed an intrusive personal search, whereas existing employees were in a more "precarious" position:

> The evidence is clear that the Hospitals' Policy includes termination as a very real possibility for those who do not consent to have a criminal background check (including VSC). The consent in relation to the RNs in this case is clearly one given under threat of losing their ability to continue working for the Hospital. [para. 206]

The hospital's interest was primarily in patient safety, although the employer identified a number of other interests such as protecting their assets, property and reputation. Nevertheless, hospital patients were not a uniformly vulnerable population; there was a range of vulnerability in that regard. In addition, the hospital had in place a number of standard security features, such as cameras and locked units. Most importantly, there was no evidence of risk, the assessment of risk being a factor which, contrary to the employer's submission, was an intrinsic component in the assessment of proportionality — that is, in balancing employer interests (patient safety) and employee interests (privacy). Nor had the hospital considered less intrusive options:

> In this case, there is certainly an inherent risk that comes with having a vulnerable patient population. However, the evidence of the Hospital was more about trying to identify

> problems before they happen, as opposed to addressing a current problem and real risk. What concerns me is that it does not appear that the Hospital considered any less intrusive measures to contain any risk. Instead, the Hospital opted for a blanket policy of criminal background checks, including the most intrusive check (VSC), for all employees and volunteers without considering whether or not other less intrusive measures would suffice.

The employer provided no evidence of any patient safety problem.

Accordingly the arbitrator allowed the grievance, ruling that the policy as it applied to existing employees was unreasonable. Recognizing that the employer nevertheless had a genuine concern to protect patients, employees and assets, he directed the hospital to amend the policy in a fashion which would more appropriately balance the interests at stake. In his view, given that nurses were a regulated health profession, a self-reporting policy was a more proportionate response.

CUPE, Local 1550 and Health Sciences Centre, Re. 2018 CarswellMan 274, 136 C.L.A.S. 283 (Gibson)

In this case the union submitted two policy grievances in response to a requirement imposed by the Employer for security and criminal record checks in the case of existing employees. The parties entered a consent order agreeing to, among other things, certain changes to the policy. However, arbitrator Gibson provided clarification on the application of the new policy terms to the circumstances of generic examples.

The policy read: “Security Check(s) may be required by the employer when a current employee is the successful candidate for a new position. Determining whether a Security Check is required for any successful candidate for a new position must be assessed on an individual basis. In determining whether a Security Check is required, the employer will consider, in addition to any other relevant factors such as whether the employee has a Security Check on file and when that Security Check was provided,” and whether, among other things, the position has access to vulnerable individuals.

In reviewing the ***Criminal Records Act,*** the arbitrator noted that section 6.3(3) states that:

“At the request of any person or organization responsible for the well-being of a child or vulnerable person and to whom or to which an application is made for a paid or volunteer position, a member of a police force or other authorized body shall verify whether the applicant is the subject of a notation made in accordance with subsection (2)”

In distinguishing ***Rouge Valley,*** arbitrator Gibson agreed with the employer that that decision involved a determination of the reasonableness of a health authority policy which required all current employees to consent to criminal record checks, including a vulnerable sector check, in order to maintain their existing positions. It did not consider the issue of internal applications for positions which would otherwise meet the criteria of positions of trust or authority over vulnerable persons. She also agreed that internal applicants for new positions are no less "applicants" as covered by section 6.3(3) of the Criminal Records Act than prospective employees new to the organization.

In reviewing several hypothetical situations, Arbitrator Gibson emphasized that the critical concerns are the type of position (including the amount of contact with vulnerable patients in the case of varying EFTs) and the existence of security checks on file. This includes the recency of those checks, which she found relevant regardless of the obligation to self-declare any changes.

The Arbitrator differed from the reasoning in ***Rouge Valley***, because in that case there was a statutory obligation on the nurses to disclose and the failure to comply on the part of a registered nurse could threaten the status of his or her licensure. Further, the policy in this case dealt with employees transferring to potential safety sensitive position. Whereas in ***Rouge Valley,*** the employer applied the policy to all existing employees. There is a balancing act in establishing the reasonableness in requiring an employee provide a security check.

***Ottawa (City) v. Ottawa Professional Firefighters Assn. (Criminal Record Check Grievance)*, [2007] O.L.A.A. No. 731, 169 L.A.C. (4th) 84 (Picher)**

In this case the union grieved a policy whereby all firefighters were compelled to provide written consent to the disclosure of any criminal record which they may have had, every three years, the results of which were recorded in the employee's personnel file. The union acknowledged the employer's right to require such a check at the time of hire, but objected to the employer's demand of checks at any time, let alone every five years as the policy required. Ultimately, the arbitrator found that the policy was an unreasonable invasion of firefighters' privacy, not within the authority of management rights. (para. 51)

One principle discussed by Arbitrator Picher was that there is a "significant distinction between the point of initial hire and the normal course of business in an ongoing employment relationship." (para. 43):

> 43 … The person who presents himself or herself at the door of a business or other institution to be hired does so as a stranger. At that point the employer knows little or nothing about the person who is no more than a job applicant. In my view, the same cannot be said of an individual who has, for a significant period of time, been an employee under the supervision of management. The employment relationship presupposes a degree of ongoing, and arguably increasing, familiarity with the qualities and personality of the individual employee. The employer, through its managers and supervisors, is not without reasonable means to make an ongoing assessment of the fitness of the individual for continued employment, including such factors as his or her moral rectitude, to the extent that it can be determined from job performance, relationships with supervisors and other employees, and such other information as may incidentally come to the attention of the employer through the normal social exchanges that are common to most workplaces. <u>On the whole, therefore, the extraordinary waiver of privacy which may be justified when a stranger is hired is substantially less compelling as applied to an employee with many months, or indeed many years, of service.</u>

The above comments have been repeatedly adopted by other arbitrators following this decision.

The arbitrator acknowledged that there could be work situations where periodic consent to the disclosure of criminal history would be justified:

> 44 Are there work settings in which it can be said that the rights of management must, absent clear and unequivocal language to the contrary within a collective agreement, be taken to understand that the employer can demand that the employee provide periodic consent to the disclosure of his or her ongoing criminal history? I think that the answer must be in the affirmative. There are obviously some types of employment which, by their very nature, justify ongoing scrutiny of the criminal record of an employee. It is therefore not surprising that in Greater Toronto Airport Authority and Public Service Alliance of Canada, Local 0004, cited above, Arbitrator Brent found that it was reasonable for the employer to maintain a policy requiring all employees to maintain their security clearance as a condition of ongoing employment. Given the security dimensions of airport operations, particularly in the management of restricted areas, the handling of valuables passing through the airport, as well as issues of contraband and terrorism, renewed periodic security checks appear as a reasonable, indeed necessary, condition of employment. In the Arbitrator's view the same might be true of persons employed as civilians within a police force, particularly if they have access to sensitive law enforcement information. It might well also apply within the framework of municipal employment. While the question is not four square before us in the case at hand, it would not be surprising for an employer to demand periodic consent to review the criminal history of social workers who work closely with vulnerable children, for example. Similar considerations might apply to persons employed as security guards. The common thread running through these examples is relatively obvious: the employment, by its very nature, is such as to require continuing scrutiny with respect to the character and trustworthiness of the person exercising a particularly Sensitive function.

But, he added that "to the extent that a position is less security sensitive, the employer's legitimate interest in ongoing disclosure of criminal records is obviously less compelling" and continued:

> 45 … The mere fact that an employee may have personal contact with individuals during the course of their work, or that they may occasionally be called upon to visit or enter private premises is, of itself, questionable as a basis for justifying a full waiver of the statutory Protections of Privacy which the Legislature has seen fit to attach to an individual's criminal record. If it were otherwise, legions of employees, from house movers to appliance repairmen and couriers, would effectively be stripped of any statutory protection under the Municipal Freedom of Information and Protection of Privacy Act.
>
> 46 In support of the application of its policy to firefighters the City has called little or no evidence to give any specificity to the interests which it maintains are to be protected by demanding that firefighters provide a written waiver of their protections under the Act. The Arbitrator is referred in general terms to the position of respect held by firefighters and their stature within the community. Reference was briefly made that firefighters might, for example, speak to students, perform the inspection of private premises or enter businesses and homes in the course of their duties. With respect, in the Arbitrator's view,

> that renders them essentially indistinguishable from a myriad of tradespersons and professionals whose work would involve the normal attendance at a variety of premises. In my view that, standing alone, falls substantially short of the compelling employer interest in demanding an ongoing security check, as might for example be justified in highly sensitive police or airport services, or as might be expected the services which involve security guards or the handling and transportation of substantial sums of money or other valuable goods. On what basis can it be argued that a firefighter who visits a classroom needs criminal security clearance to do so when the teacher who occupies that same classroom is held to that standard only by extraordinary and specific legislation. (See, e.g. The Education Act, R.S.O. 1990, c. E.2 -- O.Reg. 521/01)

Arbitrator Picher went on to identify situations where demanding consent to criminal record searches could be justified. For instance, where information came to the attention of the employer that would indicate the firefighter was the subject of a criminal conviction, the nature of which might bear meaningfully on his or her ongoing employment or the performance of his or her duties.

But, “beyond the standard of reasonable grounds, however, the Arbitrator cannot affirm the position of the City in these proceedings, which is that it is entitled, by reason of management rights, to demand a blanket consent of all of its firefighters, regardless of their personal circumstances, to gain access to confidential information concerning their possible criminal or police record.”

The decision was upheld on judicial review (**[2009] O.J. No. 2914**).

***Vancouver Firefighters' Union, Local 18 v. Vancouver (City)*, 2010 CanLII 81705 (BC LA),**

In contrast to ***Ottawa (City)***, Arbitrator Moore upheld the City of Vancouver’s policy requiring employees in its Fire & Rescue Services Department, who held "designated positions of trust," to submit police record checks every five years as a legitimate exercise of the employer's management rights. Although accepting the "general proposition that employees have a privacy interest in the non-disclosure of past criminal charges or convictions," he held that "overriding that privacy right is not, per se, unreasonable where the information that would be revealed under the policy of disclosing the record is directly related to the employment and necessary for the employer's program to operate properly and effectively."

In addition to determining that he was not bound by the ***Ottawa (City)*** decision, Arbitrator Moore considered the fact that the Ottawa policy involved a blanket requirement of a criminal record check, rather than one that was limited to particular employees, to be a key distinguishing feature. Nonetheless, Arbitrator Moore agreed with the ruling in ***Ottawa (City)*** that "employers do not have a presumptive right to access the criminal history of their employees."

3) Video Surveillance

a) Inside the Workplace

Employer rules or policies instituting video surveillance of employees at work are usually motivated by a concern to ensure security and protect property and equipment, or to deter

misconduct or trespass. In other instances, surveillance may be initiated as an ad hoc measure to investigate suspected theft or vandalism.[22]

S*t. Mary's Hospital (New Westminster) and H.E.U.* (1997), 64 L.A.C. (4th) 382 (Larson)

This has become a leading case on the extent to which an employer may resort to video surveillance of employees inside the workplace.

The employer was experiencing an escalating problem of theft and vandalism in the workplace. A report was stolen from a manager's office. Although the office was locked during non-working hours a number of people had access to it and the desk drawer in which the report had been kept did not have a lock. In an effort to identify the culprit, the employer installed a hidden surveillance camera in the office. The union objected on the basis that the surveillance violated employees' privacy rights. The issue was therefore whether the employer could engage in surreptitious on-site video surveillance of employees.

Following an exhaustive review of the jurisprudence, Arbitrator Larson held that the right to implement video surveillance is analogous to the right to search an employee's personal effects, in that both involve a conflict between individual privacy interests and management's interest in maintaining the security of its business. The arbitrator noted that while most arbitrators have recognized a right to workplace privacy, which should be preserved, this right is not absolute and its scope will depend on what is reasonable in the circumstances. Citing criteria established in several cases, including ***Doman Forest Products Ltd. and I.W.A., Local 1-357*** **(1990), 13 L.A.C. (4th) 275 (Vickers)**, Arbitrator Larson concluded that clandestine video surveillance will be allowed only where three conditions have been met:

> (1) There are reasonable grounds for the surveillance;
> (2) The surveillance is carried out in a reasonable and non-discriminatory manner; and
> (3) No other, less intrusive alternatives were open to the employer to protect its legitimate business interests.

The type, purpose, place, and frequency of the surveillance are all factors that will be weighed in applying these criteria. For example, surreptitious video surveillance is considered more intrusive than overt video surveillance, and may require more convincing justification by the employer. Further, Arbitrator Larson found that the balancing of interests analysis involved several considerations, including: whether or not there is a substantial problem, and whether or not there is a strong probability that surveillance will assist in dealing with the problem; whether or not the surveillance contravenes the collective agreement, whether or not the employer exhausted all available less intrusive alternatives prior to engaging in surveillance; and whether or not the surveillance was conducted in a systematic and non-discriminatory way.

While the problem of vandalism and theft was serious, the employer failed to take the very basic precaution of securing the documents in a locked drawer. As the employer must do everything

[22] *Leading Cases on Labour Arbitration*, at 14.2.3

reasonably possible to secure its property before engaging in clandestine surveillance, the arbitrator concluded that resort to a hidden camera was premature.

It should be noted that cases decided in British Columbia, and in particular ***Doman Forest Products***, have adopted an analysis that gives some recognition to the statutory guarantee of a right to privacy found in s. 1 of the provincial *Privacy Act*, R.S.B.C. 1996, c. 373. This section is very similar to *The Privacy Act* of Manitoba, discussed above. ***Doman Forest Products*** and certain other British Columbia decisions also take the view that the analysis of the appropriate balance between employee interests and management interests should be informed by the right to privacy enshrined in s. 8 of the *Charter*, even though the *Charter* does not apply to private employment relationships. For the most part, arbitrators in provinces where similar privacy legislation has not been enacted have approached the British Columbia precedents with caution, and have found, furthermore, that the *Charter* has no application to disputes regarding video surveillance in a private sector workplace.

***Fairmont Royal York Hotel and UNITE HERE, Local 175*, 2011 CanLII 78471, 215 L.A.C. (4th) 62 (Trachuk)**

This is an Ontario case dealing with surreptitious surveillance carried out as part of an investigation into a pattern of misconduct at the worksite. The employer retained an undercover investigator to pose as a cleaning contractor, and instructed him that if he observed misconduct, he was to film the activity using a pinhole camera hidden in his shirt button. Arbitrator Trachuk determined that the decision to undertake a covert investigation, and then to conduct video surveillance, met the "reasonableness" requirement to which management's rights were expressly made subject under the collective agreement. There was "sufficient cause" to suspect significant misconduct, she found, and the investigator did not commence the surveillance until he had witnessed apparent breaches of the code of conduct.

Nonetheless, it was held to be unreasonable to conduct filming inside the employees' change room and that portion of the surveillance evidence was excluded. Even though the change room was where much of the improper activity was allegedly occurring, she noted, the employer's right to obtain such evidence had to be balanced against the privacy rights of all employees, not just the ones committing disciplinary offences.

***New Flyer Industries Ltd. and C.A.W., Local 3003*, [2011] M.G.A.D. No. 27 (Peltz)**

In this Manitoba case, an employer's decision to install a series of fixed-view cameras was primarily for the purpose of deterring vandalism and pilferage. While the "live feed" was continuous, employees who came into the cameras' field of view while performing their duties were not observed regularly or systematically, and access to both the live feed and recorded footage was restricted to designated personnel.

In Arbitrator Peltz's view, the number of cameras, the cameras' positioning, and the regime of restricted access were both rationally related to the employer's security objectives and were reasonably respectful of employees' privacy. In so ruling, Arbitrator Peltz expressly disagreed with

the proposition in that an employer was required to exhaust less intrusive alternatives before resorting to surveillance, at least where the surveillance was overt. Nonetheless, he noted, the availability of such alternatives was a factor to be considered in determining whether the surveillance met the reasonableness standard.

Arbitrator Peltz also took the view that an employer who is dealing with significant security or safety risks does not need "to wait for the occurrence of a serious breach". He wrote:

> The Union doubted that these problems were as serious as claimed by the Company but did not challenge the legitimacy or bona fides of the concerns — security and safety. In my view, if the Company has reasonable apprehensions, it need not wait for the occurrence of a serious breach before it is allowed to take preventative steps to protect security and safety. I was not persuaded by Union arguments that there was only one past act of vandalism in the machine shop ($100,000 impact), low level pilferage in the mix rooms and only minor safety incidents in the gun rooms to date. As stated in *Calgary Herald*, supra (at para. 91):
>
> I have little difficulty accepting that this Employer, like the operators of commercial enterprises in general, has bona fide security concerns. In my view, while an employer must demonstrate there are real security issues, I don't accept the view that there must always be recent serious events to justify the implementation of a security system. Where the consequences could be severe, if there is objective evidence supporting the conclusion there is a significant risk, this constitutes a security issue.

***Kadant Carmanah Design and IAMAW, District 250 (Video Surveillance), Re*, 2015 CarswellBC 3521, [2016] B.C.W.L.D. 335 (Lanyon)**

This is another example of a dispute over video surveillance inside the workplace. The Union in this case claimed that the Employer had installed surveillance cameras in the workplace, contravening the Collective Agreement, Provincial legislation, and arbitral policy. It sought to have these cameras removed. The Employer replied that the purpose of the surveillance cameras was to achieve greater security and safety in the workplace. It asserted that the scope and use of these cameras was a reasonable exercise of its management rights.

The parties referred to two B.C. statutes applicable to the issue of camera surveillance in the workplace: the *Privacy Act*, 1996, c.373 and the *Personal Information Protection Act*, 2003, c.63 (PIPA). Arbitrator Lanyon found that PIPA balances an individual's right to privacy with the "need" of an organization to collect, use and disclose personal information and that one word, "reasonableness", captures the statutory standard required by PIPA. With respect to the *Privacy Act*, he observed that the test in s. 1 is that the nature and degree of privacy to which a person is "entitled to in a situation", or "in relation to a matter", is that which is "reasonable in the circumstances, giving due regard to the lawful interest of others." In addition, the circumstances of the violation must be examined as well as the relationship between the parties. Once again, there is a balancing of rights combined with the test of reasonableness. Arbitrator Lanyon explained that this same standard of reasonableness has been established in the arbitral jurisprudence when assessing the balance between an individual's right to privacy and the right

of the Employer to manage and protect the workplace. He articulated the most current version of the test to address this balancing of interests as follows: “Where the reasonableness approach is taken, arbitrators assess first whether the surveillance of an employee’s activity was reasonable, and secondly, whether the surveillance was conducted in a reasonable manner, proportional to the employer’s legitimate interests.”

Arbitrator Lanyon also affirmed the arbitral distinction between overt and covert surveillance, and found the right to privacy remained the same in both circumstances; that is, an employee’s right to privacy is balanced with the employer’s right to manage and protect its workplace. In his view, that standard is clear in both the arbitral jurisprudence and in the legislative scheme. However, he found that “covert surveillance is a more egregious violation of privacy because it is capable of causing more distress, anguish and embarrassment. This is because privacy is an integral part of a person’s psychological integrity and personal identity. Accordingly, covert surveillance requires a higher standard of reasonableness because it is highly offensive to the reasonable person.” He stated that within the assessment of whether management rights have been exercised reasonably, which was a less stringent standard than that required for covert surveillance, the following factors may be considered:

a. Whether the concern for safety and/or security is bona fide (recognizing there will be a subjective element of whether a concern exists; and, an objective element which relates to the circumstances of the workplace, but which does not require evidence of a historical problem of security or safety);

b. Whether there is a direct link or nexus between the installation of cameras and the issue of safety and/or security (i.e. whether or not there is evidence that the installation was for reasons other than safety or security);

c. Whether the surveillance has been implemented and utilized in a reasonable manner (e.g. the number of cameras, place of installation, use of footage, etc.);

d. Whether there are other reasonable alternatives; and

e. Any other relevant circumstances in the context of the specific case.

There were eight visible cameras in total at the Employer’s workplace. Four were dedicated to security. The Union had no objection to these cameras. The remaining four cameras were directed at the Employer’s production areas, for the purposes of safety and security. The scope of these cameras covered approximately 50% of the production area. The cameras were focused on the machines and not on specific employees, but the more time an employee spent on one machine, the greater amount of video coverage there would be of that employee. However, there was no real time monitoring of employees by the cameras. The footage was viewed only when there had been a triggering event, specifically, a safety infraction. In the past year, the video recordings had been viewed approximately six to eight times. These recordings were overwritten, or erased, every two weeks.

Arbitrator Lanyon took note of the evidence submitted with respect to a number of safety and security incidents and based on this evidence, and in balancing the employees’ right to privacy

with the Employer's right to manage and protect the workplace, concluded that the Employer had demonstrated sufficient past incidents of safety violations to justify the installation of the overt cameras.

b) Outside the Workplace

In contrast to cases involving the use of permanent on-site video monitoring, the case law on whether an Employer may subject its employees to surveillance outside the workplace has arisen almost entirely in the context of disciplinary investigations into suspected abuse of sick leave, fraudulent benefit claims, or other similar offences. Thus, the disputes referred to arbitration in such instances usually revolve around the admissibility of the surveillance as evidence in the proceedings. Nevertheless, the issue of whether employees have an enforceable privacy right that is required to be balanced against the employer's legitimate prerogatives in managing the enterprise — and if so, to what extent, and according to what criteria — is also a common thread throughout the jurisprudence.[23]

In particular, arbitrators in Ontario are sharply divided over the admissibility of surreptitious employer surveillance of employees and on the appropriate test to be applied in determining whether such surveillance is admissible in arbitration proceedings.

The two general approaches to this issue are a relevancy approach and a reasonableness approach[24].

The relevancy approach to admissibility asks itself first and foremost whether the video surveillance is relevant. That single question becomes the fundamental and primary determinant of admissibility. If the video evidence is found to be relevant, that is likely the end of the matter. Underpinning the relevancy approach is the idea that excluding relevant evidence interferes with the ability of a party to present its case and constitutes a denial of natural justice. Absent a compelling reason to exclude the video surveillance, it will be found to be admissible.

In contrast to the relevancy approach, the reasonableness approach determines the admissibility of surreptitious video surveillance from the perspective of whether the use and nature of the surveillance was reasonable in all of the circumstances. The reasonableness approach generally adopts a two-step analysis. First, arbitrators ask if the circumstances at issue reasonably justified the decision to direct surveillance. If the first question is answered affirmatively, arbitrators then ask if the manner in which the surveillance was carried out was also reasonable. If this question is also answered affirmatively, then the video will be admissible.

The core issues upon which these two approaches are divided is whether there is a general right to privacy in private sector Ontario workplaces. The relevancy approach holds there is no such right while the reasonableness approach holds that there is. Manitoba Arbitrators, in contrast, have consistently accepted that employees have a privacy interest that must be balanced against Employers' interests; perhaps because of the presence of *The Privacy Act*, which does not have

[23] *Leading Cases on Labour Arbitration*, at 14.2.3.
[24] *Brown & Beatty* Focus 10 – EMPLOYER SURVEILLANCE.

an equivalent in Ontario. Thus, it can be argued that case law applying the relevancy approach should not be relied upon in Manitoba.

New Flyer Industries Ltd and CAW Canada, Local 3003 **(1999), 57 CLAS 16** is the foundational case in Manitoba on the issue of the admissibility of video surveillance evidence. The grievor was absent from work due to medical restrictions and was receiving temporary disability benefits under the collective agreement. The employer received an anonymous telephone call suggesting that the grievor was working at his home in a manner inconsistent with his injury claims. The employer carried out an investigation, which included video surveillance of the grievor. As a result of the investigation, the employer concluded that the grievor had falsified his injury claims and the employee was terminated.

Arbitrator Peltz considered the preliminary motion of the union to exclude the video evidence and ultimately rejected it, allowing the evidence to be considered. In reaching this conclusion, he noted the reasons in ***Doman Forest Products***, referenced above.

At the time this case was decided, Arbitrator Peltz noted only one decision that had been provided to him by the employer in which a strict relevance test was used as opposed to a reasonableness test. It is apparent, however, that at least in Ontario, the relevance test has gained support over the years and is now a well-represented line of authority in that province.

It should also be observed that Arbitrator Peltz made reference to *The Privacy Act*, CCSM c P125:

> Section 7 of the Manitoba Act, which has paramount status over other legislation due to section 8, leads inexorably to the question of whether the surveillance has breached the grievor's right of privacy under the Act. In turn, this leads to the section 5(c) defence raised by the Employer in the present case - that the particular surveillance was reasonable, necessary and incidental to the protection of the company's lawful rights and interests in the operation of the disability benefits scheme under the collective agreement. Either way, whether by application of arbitral precedent or application of the statutory provisions, we arrive at the same need to balance the reasonableness of the legitimate and competing interests of the parties.

In his second award on surveillance, ***New Flyer Industries Ltd (Re)*****, [2000] 85 LAC (4th) 304**, Arbitrator Peltz explained that regardless of its precise formulation, reasonableness must be the determinative concern:

> In my Interim Award, I considered the principles applicable to arbitral review of an employer's use of video surveillance evidence. Whether one proceeds under the Doman three part test (Arbitrator Vickers), the Canadian Pacific two part test (Arbitrator Picher) or the statutory test set out for Manitoba cases in The Privacy Act, there is a need to balance the reasonableness of the legitimate and competing interests of the parties. The development of these various textual formulas, all of which amount to substantially the same approach in the end, illustrates that an arbitrator must have regard to the overall reasonableness of admitting surveillance evidence in each particular case.

Given that the admissibility of the surveillance evidence was being dealt with as a threshold issue, Arbitrator Peltz observed at paragraph 63:

> It is a serious matter indeed to exclude highly relevant evidence at the outset of a civil proceeding, particularly a proceeding which normally operates with a less rigid and formalistic approach to the admission of evidence. If the preliminary evidence (the voir dire) reveals no plausible basis for the employer's resort to surveillance - that is, there is really nothing unusual except for suspicion by the employer - then a definitive ruling excluding the evidence is appropriate.

Arbitrator Peltz concluded that the employer was not acting solely on suspicion and this was not a case of “an electronic web, cast like a net, to see what it might catch.” The employer had reasonably reliable information in the anonymous tip and these initial suspicions were further confirmed in the employee’s attendance record, which showed a pattern of long absences during the summer months that was consistent with abuse of the disability plan. There had also been complaints at the work place from fellow employees about the grievor’s suspected behaviour. Arbitrator Peltz rejected the union’s suggestion that if the employer had suspicions then additional medical information could have been requested and found that this would only alert the grievor to the fact that the company was conducting an investigation.

Finally, Arbitrator Peltz felt that the evidence was lacking in terms of the manner in which the surveillance was conducted and merely noted that the union was not making an objection on the ground that the surveillance was conducted in an unreasonable matter. It should be noted that the evidence was tendered subject to the union's continuing objection to admissibility and he stated that the parties could address admissibility and weight at the conclusion of the case, as part of final argument. After the hearing, Arbitrator Peltz ultimately concluded that termination was excessive in all the circumstances.

In ***New Flyer Industries Ltd and CAW Canada, Local 3003*****, [2003] 115 LAC (4th) 57**, Arbitrator Chapman took into consideration the findings of Arbitrator Peltz in the earlier case between the parties when he decided the union’s preliminary motion to exclude video surveillance evidence of a grievor who remained off work on a disability claim. However, Arbitrator Chapman distinguished the case before him from the circumstances that were before Arbitrator Peltz and excluded the video evidence. He found that the only information the employer had was some alleged comments by unidentified employees that were made to a supervisor who was not directly involved with the grievor. Such information alone did not justify the use of video surveillance, as the employer could have investigated the matter by other alternatives. Most important to Arbitrator Chapman was his finding that the employer had “nothing but suspicion.”

Arbitrator Peltz again had occasion to consider the admissibility of video surveillance evidence as a threshold issue in ***New Flyer Industries Ltd and CAW Canada, Local 3003*** **(unreported, February 17, 2003)**, this time in relation to an employee who remained off work on a claim under Workers Compensation Benefits. He applied the law from his previous decision, discussed above, and found that the evidence in this case was inadmissible.

First, the grievor had received independent medical opinions confirming his injury and those opinions were unchallenged by the employer. Second, other medical suspicions had been confirmed by the employer without resort to video surveillance or the need to invade the grievor's privacy. Third, no attempts (beyond video surveillance) were made by the employer to investigate its suspicions that the grievor had actually injured himself while working in his own private moving company. Fourth, the grievor continued to receive medical care and to supply the employer with medical updates on the status of his injury. Finally, although the medical evidence may not have been exactly what the employer had desired, it was not so limiting as to justify the invasion of privacy that naturally flows with the use of video surveillance.

Arbitrator Peltz concluded that while suspicions existed and while further investigation and inquiry may well have been prudent, it did not follow that evidence acquired by electronic surveillance will always be admissible in arbitration.

The video surveillance evidence at issue in ***Dauphin Consumers Co-operative Ltd v United Food and Commercial Workers Union, Local No 8321*****, [2006] 87 CLAS 167**, was distinguished by Arbitrator Simpson from the evidence considered in earlier Manitoba cases like those described above, as it was not "the more usual case of surveillance being established to monitor a particular location or watch for a specific activity." Instead, in this case, he found that the grievor's manager used the video and still photography to corroborate what he was personally witnessing. The manager had driven by the grievor's sister's house on the information of another staff member and observed a pile of sand, which indicated to him that construction was being undertaken. He drove by the house again days later and saw the grievor working in his sister's yard. At that time he went home and picked up both a still and a video camera so that he could substantiate what he had seen. Arbitrator Simpson stated that the video evidence simply depicted visually that to which the manager attested in his oral evidence. He therefore found that the video evidence should be admissible in the particular circumstances of the case before him. It should also be noted that while there was no specific discussion by Arbitrator Simpson as to whether the proper approach to admissibility of the video evidence was relevance or reasonableness, he framed the employer's and the union's arguments in terms of the reasonableness of the video tape in the circumstances (paragraph 8).

In ***Praxair Canada Inc. v General Teamsters Local Union No 979*****, [2007] 91 CLAS 288, 93 CLAS 118**, the grievor in this case had sustained injuries on October 31, 2006, as the result of a fall in the Company's parking lot. The injuries were to the grievor's left shoulder; he also experienced some pain and stiffness in his neck and lower back. He continued to work in the days and weeks following October 31, 2006. However, several weeks after the accident, the grievor was placed on modified duties as a result of his worsening symptoms. Thereafter, certain issues arose as to the limitations on his regular duties which ought to apply as a result of his injuries. The Company suspected that the Grievor was playing sponge hockey ("spongee") on a regular basis during the 2006-2007 winter. The Company's position was that if the grievor was playing spongee, such activity would be inconsistent with some of the physical limitations he was reporting at work, and would also be inappropriate because participating in that sport would involve the risk of aggravating his injuries, and prolonging his recovery. The Company undertook surveillance of the grievor on February 16, 2007, and February 20, 2007. On the basis of this

surveillance, the Company concluded that the grievor was playing spongee. The Company received a copy of the report of the surveillance which was dated February 27, 2007, and terminated the grievor's employment shortly thereafter.

The union argued that the grievor did nothing wrong, and that playing spongee was consistent with the medical advice the grievor had received. The union also said that this case was important because it involved an employer attempting to limit the activities in which an employee may engage outside of regular working hours. In the alternative, the union maintained that if the grievor's conduct was disciplinable, discharge was harsh and excessive in the circumstances.

After considering the authorities submitted by both parties, Arbitrator Graham concluded that he preferred the reasonableness approach to the relevance approach and noted that “a majority of arbitrators have concluded that privacy considerations are important, and must be given some weight.” He described the test to be applied in determining the admissibility of covert surveillance evidence as being the same three-part test Arbitrator Peltz outlined in ***New Flyer Industries Ltd* (1999)** and that originated in ***Doman***.

Arbitrator Graham found that the first requirement of the test was met by the Company, namely, that it was reasonable for the Company to have conducted surveillance. The Company argued that covert surveillance was reasonable because of the suspicious circumstances regarding the injury itself, the unusual course of the grievor's recovery from the injury, and the grievor's inconsistent reporting of his own limitations.

Next, Arbitrator Graham held that the second part of the test was met, in that the surveillance was conducted in a reasonable manner. In this regard, he noted that not only was the surveillance conducted in a public place, but in an outdoor recreation area with spectators in attendance. He stated, “Although covert surveillance involves an infringement on an individual's right to privacy, it cannot be said that the Grievor had much expectation of privacy playing spongee in an organized league in a public place.”

Arbitrator Graham found that the Company failed to meet the third test requirement and concluded that there were other alternatives open to the Company, which it ought to have pursued before resorting to covert surveillance. For example, he found that while the evidence satisfied him that the Company had spoken to the grievor on or about January 3, 2007 about his participation in spongee, and had received a less than forthcoming answer, the evidence did not establish to his satisfaction that similar, or more specific questions were asked on other occasions, or that if they were, evasive and deceitful answers had been given. He believed that more pointed questions could and should have been asked by the Company regarding the spongee, before reaching the conclusion that the grievor had not been, and would not be truthful, and that surveillance was therefore necessary. Arbitrator Graham also noted that the Company’s communication with the grievor’s doctor about his ability to perform job functions did not occur until after an investigative firm had already been retained to conduct surveillance. Additionally, he explained that a representative of the Company could simply have attended one of the grievor’s spongee games personally in order to substantiate the Company’s concerns. Arbitrator Graham also observed that the Company could have relied upon an article of its collective agreement with the union,

which allowed it to require that the grievor submit to a medical examination by the physician of its choice.

Arbitrator Graham's last point was as follows:

> Finally, I note that in this case, unlike many other reported cases involving disputes over surveillance evidence, the Grievor was at work and performing modified duties, which were of some value to the Company, at the same time as the surveillance was being undertaken. It was therefore open to the Company to observe the Grievor while at work performing various tasks to determine the range of functions he could perform. This is not a situation in which the Grievor was claiming to be unable to perform any duties, and was off work but receiving pay. He was at work, but claiming not to be able to perform all of his duties. I certainly do not condone any employee's attempts to lessen his or her workload by exaggerating the effects of an injury, but circumstances in which an employee engages in such conduct are less serious than circumstances in which an employee fabricates a claim of total disability and is paid for doing no work. I consider the relative seriousness of the conduct involved to be an appropriate factor to consider when assessing the alternatives the Company had to obtain the information it sought.

***Ottawa-Carleton District School Board and OSSTF, District 25 (Donnelly), Re*, 2015 CarswellOnt 7439, 257 L.A.C. (4th) 1**

One of the central issues in this case was the scope of an employee's reasonable expectation of privacy in a situation where he had been covertly filmed while on break smoking marijuana adjacent to the property of the school where he worked. He was wearing a shirt bearing school board insignia at the time. On the question of the employee's reasonable privacy expectations in this kind of circumstance, the arbitrator outlined the governing principles this way:

> The case law also recognizes that in the application of these questions, many factors come into play. As the Supreme Court held, it is important to determine the "reasonable expectation" of privacy in each situation. For example, it is recognized that an employee has a much higher expectation of privacy in his/her own home than s/he could expect in a shopping mall or the shop floor. Therefore "location" is an important factor. So too are considerations with regard to whether we are dealing with on or off duty conduct, the nature of the Employer's interest and the degree of intrusion. Video surveillance is not prohibited in the employment context *per se*. No case suggests that. Further, these parties have accepted the notion that this Employer can use video surveillance equipment, even covertly, by incorporating the concept into the Collective Agreement. Therefore, the important questions become whether the circumstances indicate that the surveillance has intruded "to an unreasonable degree" or whether it violated the Collective Agreement…

Applying these principles to the case before her, Arbitrator Knopf found that the grievor had a low expectation of privacy in the circumstances, given that he was at work, wearing a uniform, and in a public space where passersby could observe him. In her view:

> [I]t is difficult to accept that a "reasonable expectation of privacy" existed in those circumstances. An employer has a legitimate interest in the activities of an employee during working hours, while in uniform and standing immediately adjacent to the place of work. … In contrast [to a criminal police investigation context], while employees do not lose all their rights of privacy at the beginning of a shift, those rights do not have a very high ranking in a scale of privacy concerns when the activity is during working hours, adjacent to the workplace and in a public setting. Further, given the present reality of life, where there are security cameras in many public spaces and almost everyone carries a device capable of recording sound, motion and images, it is naïve to retain an expectation that we will never be recorded when we stand in a public place. … [I]t is a difficult stretch to accept that his private affairs were being invaded in an offensive way without any legitimate excuse, all of which are necessary to found an argument that his right to "seclusion" was violated.

Emphasizing that "surveillance can be considered appropriate and reasonable if it is undertaken in a reasonable manner and for a reasonable purpose," Knopf held that the employer's interests justified the decision to initiate surveillance, reasoning:

> This employer had received reports that it considered to be credible alleging the use and trafficking of marijuana during work hours by custodians on the premises of an elementary school. Given the nature of the employer and the location, it is obvious that such conduct would cause concern and would not be tolerated. … When the interests of this public school board and the interests of those employees are then compared, the interests of the employer far outweigh the interests of the employees. Further, if the "reasonableness" test is applied to the situation in this case, it must be concluded that even if there was an infringement on the employees' privacy, it did not do so to such an unreasonable degree that the surveillance would warrant a label of impropriety under even the most liberal reading of the case law. The surveillance was in place for only three days…. Further, the video recording was only taken of employees seen to be smoking marijuana. No other activities were recorded. Therefore, the recording was done in a reasonable manner and to a reasonable degree under these circumstances.

Despite the employer’s failure to follow certain procedural aspects of its policy pertaining to video surveillance, the Arbitrator found that the employer had substantially complied with the policy. She further found that the employer's interest in deterring drug use at the school far outweighed the employee's privacy interest, which was minimal given that the misconduct took place in a public place while on duty. The Arbitrator accordingly held that the highly relevant evidence should be admitted.

4) Location Monitoring

For employees that do not work in a static location, employers may choose to track their whereabouts. Common examples of this are delivery and transportation industries. In some cases, the employee tracking is incidental, as the location is tracked for other purposes, such as determining the amount of time before a parcel will be delivered, however, in others the monitoring is intentional and directed at measuring productivity or monitoring the usage of employer vehicles.

Arbitrators seem to have a higher degree of tolerance for location monitoring, as compared with other privacy invasive actions by employers, distinguishing it from video surveillance, for example.

***Otis Canada Inc. and I.U.E.C., Local 1*, 2010 CanLII 83120, [2010] B.C.C.A.A.A. No. 121 (QL) (Steeves)**

In this case, company vehicles, to be used during the day to attend at work sites, were assigned to each of the employer's mechanics. The employer decided to equip the vehicles with so-called "telematics" devices, which utilized satellite technology to record certain types of information about the vehicle's use (the date and time the engine was started and turned off per trip, the number of kilometers driven during a trip and over the course of the day, the time spent driving as well as idle time, the stop time between trips, and gas consumption). This information was available to designated members of management, along with the name of the mechanic to whom the vehicle had been assigned. However, as the devices were not equipped with GPS capacity, they could not track the actual location of a vehicle. According to the employer, the devices had been installed for the purposes of improving the efficiency of its fleet, reducing fuel costs, ensuring regular maintenance, and identifying unauthorized or inappropriate use of vehicles by employees. The union launched a grievance, arguing that the data obtained by the devices was "personal information" within the meaning of B.C.'s PIPA and as such could not be collected or used without the employees' consent. Under PIPA, "personal information" is defined, in part, as "information about an identifiable individual."[25]

Arbitrator Steeves dismissed the grievance, holding that the PIPA was inapplicable in this case because the information provided by the telematics devices did not constitute "personal information" as defined by the legislation, and that the employer's right to install the devices was not otherwise circumscribed by the collective agreement or applicable legislation.

At the outset, the arbitrator noted that in the absence of contractual or statutory limitations, an employer was free to implement methods for recording the working time of employees, pursuant to its general management rights. On the facts before him, Arbitrator Steeves found that as the telematics devices were not GPS-enabled, they were unable to transmit information regarding a vehicle's geographic location, and only allowed the employer to make an approximate assessment of the movements of mechanics. Turning to the issue of whether the data recorded by the devices was "personal information" under PIPA, the arbitrator concluded that while the technology did identify individual employees, it was not information "about" an identifiable individual. In this respect, he found, the purpose of the devices was not solely to track the location of employees. Rather, their primary function was to reduce fleet costs. The data, although it could suggest unauthorized use of a vehicle, did not in itself reliably determine employees' activities. In fact, apart from the name of the employee, all of the information in question related to vehicle operation. The collection of such information about company vehicles, which also included the driver's name, did not, in the arbitrator's view, amount to "personal information" for the purposes of the Act. Furthermore, while the data could lead to the imposition of discipline against an employee, this did not transform it into "personal information". The information was "professional

[25] PIPA, at s. 1.

and non-personal" in nature. Its collection was not "fundamental to the dignity and integrity" of employees, and did not engage the right to privacy.

Moreover, on the basis that monitoring and supervision of company vehicles was an inherent prerogative of management, the arbitrator concluded that the system did not breach either the parties' collective agreement or B.C. labour legislation.

***PIPEDA Case Summary No. 351*, 2006 CanLII 42313 (PCC), [2006] C.P.C.S.F. No. 28**

Notably, a different analysis was applied in a case decided under the federal PIPEDA. Where a complaint arose out of the use of technology similar to that in ***Otis Canada***, but with the addition of GPS capability, the Assistant Privacy Commissioner held that the data collected was in fact "personal information" for the purposes of the Act, because it could be linked to specific employees driving the vehicles and the drivers were identifiable. Although she ultimately upheld the employer's right to deploy the technology as meeting PIPEDA's requirements, the Assistant Commissioner expressed concern about using the devices to manage employee performance. In such circumstances, she noted, the use would "shift the balance significantly toward the 'loss of privacy' end of the spectrum."

IUOE, Local 793 and Earth Boring Co., Re. 2021 CarswellOnt 7188, 148 C.L.A.S. 372.

In this decision, Arbitrator Rogers reviewed a grievance challenging the Employer's introduction of a requirement to use the app "ExakTime," which the Employer characterized as an electronic timesheet. Local 793 grieved that the Employer had "violated the privacy of its employees by enforcing unreasonable management rights, by asking them to install an application that uses GPS/photos on their personal communication device to track their whereabouts". Local 793's requested remedy was that the Employer "immediately cease and desist in its intent on forcing its employees to install and use an application on their personal communication device that violates their rights and freedoms."

The ExakTime application as implemented by Earth Boring required the use of smartphones or comparable devices with GPS that would permit employees to take photographs of themselves and fix their locations when doing so.

The Arbitrator went into depth about the function of the app. The evidence was that employees downloading and starting their use of ExakTime would be invited to accept the privacy policy published by ExakTime Inc. — without the acceptance of which the application is not available. The privacy policy included:

> This policy describes how we may share your information for marketing purposes. You may contact us with any questions and, to the extent applicable, to request once a calendar year a list of third parties to whom we may disclose information for their own marketing purposes and the categories of information we may disclose.
>
> Please be aware that your personal information and communications may be transferred to and maintained on servers or databases located outside your state, province, or country. Please be advised that we process and store information in the United States.

> The laws in the United States may not be as protective of your privacy as those in your location. By using the Sites, you agree that the collection, use, transfer, and disclosure of your personal information and communications will be governed by the applicable laws in the United States.[26]

Further, the Arbitrator commented that the ExakTime Inc. materials addressed the application's Geotrakker capacity and ExakTime's Photo-ID feature as follows:

> Keep track of employee location data for traveling workers or crews on the job site. Get breadcrumbing data in real time on their location and speed of travel while they are on the job — with very little data usage, and no tracking off the clock.
>
> It is possible to have biometric confirmation without the hassle of fingerprints. FaceFront Biometrics uses your device's front-facing camera to snap a photo of each worker when they clock in and out. Goodbye, buddy-punching.[27]

The Arbitrator found that the if the employee left the app running in the background the geo-location tracker would be active in the geofenced areas. The Arbitrator cited the Union's expert witnesses report, stating:

> "He explained that minimizing the application is not to be confused with closing it; minimizing or exiting the application does not close it; when the application is minimized and "its operation is not immediately apparent to the user", it "continues to run in the background; closing the application "requires additional steps to render the app inoperative."

In conducting the privacy interests analysis, the Arbitrator relied on the decision in ***PIPEDA,*** where the Assistant Commissioner noted that the purpose of the Act is to balance the individual's right of privacy with respect to their personal information and the need of organizations to collect, use, or disclose personal information for appropriate purposes in the circumstances.

The Employer conceded that the use of ExakTime constituted a privacy incursion. They posited that the balance heavily favoured its justification for the introduction of ExakTime and its insistence on its use by bargaining unit employees. However, the Arbitrator noted that the incursion was a material privacy intrusion with virtually no evidentiary basis for the Employer's attempt to justify requiring Employees to use the app.

In analyzing the continuous tracking capabilities of the app, the Arbitrator commented that:

> "[The Employer] contended that Earth Boring's employees have their location tracked only when they clock in and clock out — when they are at the workplace — and that they needed to provide their photograph only when they are at work. In keeping with the cases that recognize the distinction between an employee's rights and expectations at work and away from the workplace, Earth Boring argued that the information it collected via

[26] IUOE, Local 793 and Earth Boring Co., Re. 2021 CarswellOnt 7188, 148 C.L.A.S. 372 at para 26.
[27] Ibid.

> ExakTime was information an employer is legitimately entitled to have in operating its workplace. That was said to be particularly so with the Employer's highly mobile workforce — creating a situation in which "it is substantially more difficult to supervise employees directly".
>
> There was no evidence of difficulties encountered in the supervision of a "mobile workforce" or of employees' assigning themselves to work, projects or sites independently of their supervisors. Furthermore, using ExakTime, Earth Boring learned precisely where Mr. Pierson was on 254 occasions when he clocked in or out beyond the GeoFence set up for the Seaton site. That is to say, Earth Boring had his location on those occasions regardless of the configuration of the GeoFence and regardless of the knowledge it sought to acquire."[28]

In comparing the evidence of the employer against the Union's evidence, Arbitrator Rogers commented:

> The Employer's evidence concerning the extent to which ExakTime could track and has tracked its employees was not reliable. In contrast, the positive evidence of Mr. Costa established that the application will track an employee and the data were capable of being played for review if the employee failed to carry out one of four steps. He wrote:
>
> > The Geotrakker on the other hand tracks and records time, location and movement information of employees regardless of any GeoFence, which information it then incorporates and "maps" onto Google Maps, creating a detailed visual record of employees' movements through time and space. This record can be both monitored as it updates via pings, and "re-played" after the fact as if in real time.[29]

Arbitrator Rogers concluded that the "Employer's requiring employees to use the ExakTime application as it is currently configured, enabled and exploited or open to exploitation violates and is contrary to the privacy interests of the bargaining unit employees" because it processes, retains, and transmits their facial images, records, retains, and transmits their geo-locational data, including data that are not restricted to the employees' work sites and working hours, and provides access to and permits the use of these data by ExakTime Inc. and other third parties without restriction and without the informed consent of the affected employees of Earth Boring.

Conclusion

Privacy is an important interest and core value of many workers and with the plethora of tracking options available to Employers today as a result of advances in technology, Unions must be vigilant of Employer attempts to monitor workers in ways that are privacy invasive.

While privacy rights are never absolute, whether at common law or pursuant to legislation, it must be emphasized that Employers have the burden to prove that any privacy invasive employee tracking tactics they choose to unilaterally implement are reasonable under the balancing of

[28] Ibid at para 311.
[29] Ibid at para 339.

interests approach that has been adopted by arbitrators. Violations of privacy are difficult if not impossible to remedy in most cases, so Unions must act quickly and assertively when employee tracking issues arise.