

Walking the Tightrope – Recent Developments in Employee Surveillance

Dan Michaluk, Hicks Morley LLP¹

Introduction

Striking the proper balance between the right to manage and employee privacy rights has long been an important exercise for human resources and labour relations professionals. The dialogue on employee surveillance started as early as 1979, when an arbitrator recognized the tightrope that employers walk when using new technology to manage the workplace. In *Puretex Knitting*, Arbitrator Ellis quoted the following statement on the intrusiveness of video surveillance:

The device at hand is not only personally repugnant to the employees, but it has such an inhibiting effect as to prevent the employees from performing their work with confidence and ease. Every employee has occasion to pause in the course of his work to take a “breather”, to scratch his head, to yawn, or to otherwise be himself without affecting his work. As employee, with reason, would hesitate at all times to behave, if his every action is being recorded on TV.²

Since this early statement there have been a great number of cases in which arbitrators have evaluated surveillance systems that detract from employee privacy. In many cases, they have ordered a cease and desist (often entailing the removal of video cameras) when employers have not struck a proper balance between their management interests and employee privacy rights. Similar challenges may now be raised by non-union employees who enjoy newly-enacted statutory privacy rights.

Although the issue is not new, new technology is giving rise to new case law. The limits on video surveillance and computer and e-mail surveillance are now relatively easy to discern, but

¹ I represent clients in all areas of Hicks Morley LLP’s management-side labour and employment practice and specialize in the law that pertains to information, privacy and records management. I am grateful to Sara Luther for the excellent research she provided in support of this paper.

² *Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union* (1979), 23 L.A.C. (2d) 14 (Ellis) at 25.

newer surveillance technologies such as Global Positioning System (GPS) technology, keystroke monitoring technology and Radio Frequency Identification Device (RFID) technology involve different considerations that are yet to be fully articulated in the case law.

In this paper, I briefly examine the most recent and relevant legal developments in the law on employee surveillance. It is divided into two parts. In the first part, and only to the extent necessary to establish a common basis of understanding, I briefly review the legal framework for challenging employee surveillance. In the second part, I review developments in “productivity surveillance” with specific reference to recent cases on GPS surveillance and keystroke monitoring.

The Legal Framework for Employee Privacy Rights – The Basics

To start, I would like to explain that, for the time being, only unionized employees and employees with statutory privacy rights have a practical means of challenging the implementation of surveillance initiatives by their employers.

Although collective agreements rarely contain an express restriction on employee surveillance, arbitrators have assumed jurisdiction over surveillance complaints based on clauses that restrict changes to working conditions or practices³, clauses that specifically specify that work rules must be reasonable⁴, by recognizing implied restrictions on management rights⁵ and by recognizing a right of privacy based on the “common law of the unionized workplace⁶.” Based on the prevailing arbitral case law, employers have a fairly limited ability to raise successful preliminary objections to surveillance grievances by claiming that their unionized employees have no legal basis for making a privacy complaint.

³ See e.g. *Re Thibodeau-Finch Express Inc. and Teamsters Union, Local 880* (1988), 32 L.A.C. (3d) 271 (Burkett) and, more recently, *Re Tri-Krete Ltd. and Labourers’ International Union of North America, Local 506 (Video Surveillance Grievance)*, [2005] O.L.A.A. No. 470 (Whitehead) (QL).

⁴ See e.g. *Re United Food and Commercial Workers Union, Local 1000A and Janes Family Foods (Surveillance Grievance)*, [2006] O.L.A.A. No. 611 (Trachuck) (QL).

⁵ See e.g. *Re Lenworth Metal Products Ltd. and United Steelworkers of America, Local 3950* (1999), 80 L.A.C. (4th) 426 (Armstrong), upheld on judicial review (2000), 29 Admin. L.R. (3d) 258 (Ont. Div. Ct.).

⁶ See e.g. *Re Labourers’ International Union of North America, Local 625 and Prestressed Systems Inc. (Roberts Grievance)* (2005), 137 L.A.C. (4th) 193 (Lynk). But see, among others, *A.T.U., Local 569 v. Edmonton City* (2004), 124 L.A.C. (4th) 225 (Alta. Q.B.) and *Re Canadian Timken Ltd. and U.S.W.A., Local 4906 (Hutchin)* (2001), 98 L.A.C. (4th) 129 (Welling).

Legislation is another source of employee privacy rights. Currently, employees in federal works and undertakings (e.g. banks, airlines and communications companies) can file a complaint about workplace surveillance under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).⁷ Similarly, employees in British Columbia⁸, Alberta⁹ and Quebec¹⁰ enjoy statutory privacy rights that can be the basis for a workplace surveillance complaint.

Outside these jurisdictions, non-unionized employees have no practical means of objecting to workplace surveillance on the basis of its intrusiveness. The Ontario Superior Court of Justice has recently given limited endorsement to a common law breach of invasion of privacy tort¹¹ and constructive dismissal claims based on workplace surveillance are a possibility. However, the option of suing a current employer or the option of resigning and claiming constructive dismissal has not proven to be appealing to non-union employees who object to workplace surveillance.

In circumstances in which an employee *can* make a complaint challenging the implementation of workplace surveillance, an adjudicator will balance the business interest of the employer against employee privacy rights and assess whether the surveillance is reasonable in light of the balance. This involves asking the employer (who bears an onus of proof) a series of questions. The Privacy Commission of Canada, for example, has endorsed the following four-part test:

- Is the surveillance demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to that need?
- Is there a less privacy-invasive way of achieving that need?¹²

⁷ S.C. 2000, c. 5.

⁸ *Personal Information Protection Act*, S.B.C. 2003, c. 63.

⁹ *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

¹⁰ *An Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1.

¹¹ *Somwar v. McDonald's Restaurants of Canada Ltd.* (2006), 79 O.R. (3d) 172 (S.C.J.) and *Shred-Tech Corp. v. Viveen*, [2006] O.J. No. 4893 (S.C.J.) (QL). Note that the legislatures in British Columbia, Manitoba, Saskatchewan and Newfoundland have also enacted statutory torts to protect individual privacy.

¹² Most recently applied in *PIPEDA Case Summary #351*, [2006] C.P.C.S.F. No. 28 (QL) and endorsed by the Federal Court in *Eastmond v. Canadian Pacific Railway* (2004), Admin. L.R. (4th) 275 at 319.

It bears noting that this variant of the test is not uniformly accepted. For example, there is a significant debate amongst labour arbitrators about the last question. Arbitrators have differed on whether an employer must establish that there are no other reasonable means of accomplishing its purpose without using surveillance.¹³ Yet even where the availability of less intrusive means is accepted as relevant, arbitrators seemly accept that the use of surveillance should not be ruled out and have treated the existence of another option as only one factor weighing against the overall reasonableness of the surveillance initiative.¹⁴

Setting all debate about the nuances of the test aside, it is a useful means by which employers can evaluate proposed surveillance systems. Employers will significantly reduce their risk of a successful challenge to any surveillance initiative by engaging in a detailed planning process that features a privacy impact assessment and consideration of the same factors that will be considered by an adjudicator in the event of a challenge.

Productivity Surveillance – When can employers manage by technology?

In the balance between business interests and employee privacy rights, an employer's interest in managing the productivity of employees has always carried the least weight. In light of the statement quoted at the beginning of this paper it is relatively easy to understand why this is the case. "Management by video camera" involves the continuous collection of information about the way in which an employee works, including information about the natural (and personal) elements of that process – e.g. yawns, scratches, and all other personal affectations. Although employers are correct to argue they have a right to supervise their employees, productivity surveillance (at least by use of a video camera) is clearly more intrusive than traditional supervision.

For this reason, there has been a relatively clear pattern in the video surveillance case law. Employers who attempt to justify video surveillance as a management tool can expect to have a difficult time. For example, in 2005 the Privacy Commissioner of Canada's Office found that an

¹³ See *Re Leon's Mfg. Co. and R.W.D.S.U.*, Loc. 955 (2006), 153 L.A.C. (4th) 155 (Pelton) at 164 – 166.

¹⁴ *Ibid.* at 166 and *Prestressed Systems*, *supra* note 6, at 211.

internet service provider breached PIPEDA by installing video cameras in the workplace.¹⁵ The employer claimed that the cameras, one of which was trained on help desk employee workstations, were needed for safety-related purposes but also claimed they were needed to supervise employees because it could not afford to hire a supervisory staff that could monitor employees over a sixteen hour work day. The adjudicator doubted the employer had raised a *bona fide* safety rationale and held that its productivity interest did not outweigh employee privacy rights.

This outcome is different from the outcome in the many labour arbitration cases in which an employer is able to prove a *bona fide* safety or security justification for video surveillance. In these cases, arbitrators have generally allowed video cameras to stay provided they are trained on security points such as entrances and exits and not work areas¹⁶ or provided they are only turned on outside of working hours.¹⁷ If there are special circumstances justifying the use of cameras that are trained on workstations, they may be allowed, but likely not without restrictions. For example, in a 2003 decision called *Pope & Talbot*¹⁸, Arbitrator Munroe crafted a creative remedy to resolve a dispute about the surveillance of a facility for unloading wood chips from a barge that was located about 800m from a pulp and paper mill. He refrained from making an order to de-activate a camera on an undertaking from the employer to limit surveillance to supervisors and lead hands and to only turn the camera on for a 20 minute period during a shift change (corresponding with a proven productivity problem) and periodically for a maximum of five minutes at a time.

Striking the right balance between employer and employee rights in assessing video surveillance systems is made somewhat easy by the fact that video cameras can often be re-directed away from workstations and turned on and off without frustrating the purpose of the surveillance system. GPS monitoring systems – which involve tracking employee location information – can

¹⁵ *PIPEDA Case Summary #279*, [2004] C.P.C.S.F. No. 24 (QL).

¹⁶ See e.g. *Puretex Knitting*, *supra* note 2, *Janes Family Foods*, *supra* note 4 and *Leon's Manufacturing*, *supra* note 13.

¹⁷ See e.g. *Tri-Krete*, *supra* note 3.

¹⁸ *Re Pope & Talbot Ltd. and Pulp, Paper and Woodworkers of Canada, Local 8 (2003)*, 123 L.A.C. (4th) 114 (Munroe).

be more challenging because there are not as many options to limit the scope of the surveillance while maintaining the efficacy of the system.

The Office of the Privacy Commissioner of Canada recently addressed this challenge in *PIPEDA Case Summary 351*¹⁹ - a decision that outlines some important limits that employers should observe in designing and implementing GPS monitoring systems.

The system under challenge was implemented by a telecommunications company and collected information about field maintenance employees' location through GPS units installed in work vehicles. The employer raised three purposes:

- managing productivity (locating, dispatching and routing employees to job sites and planning for and managing this activity);
- managing safety and development (allowing for follow-up when vehicles were stationary for an inordinate period of time and allowing for the management of dangerous driving habits); and
- promoting asset protection and management (by allowing for the recovery of stolen vehicles and reducing the wear on vehicles by through better route management).

Although the adjudicator did accept the legitimacy of the employer's safety and property protection purposes, she clearly gave the most weight to its interest in improving productivity in locating, routing and dispatching its field employees: "As the system will be integrated with its dispatch system, it was easy to understand how GPS could improve efficiency by minimizing the amount of time employees spend on the road getting to work."²⁰ She balanced this interest against the invasiveness of the system and ultimately held that the company's monitoring system was reasonable.

In assessing the invasiveness of GPS monitoring, the adjudicator rejected the employer's argument that GPS monitoring of field employees is privacy-neutral because an employer has a

¹⁹ [2006] C.P.C.S.F. No. 28 (QL).

²⁰ *Ibid* at para. 29.

right to know where its employees are working and would only make field employees as visible as office employees. She did, however, say that the GPS system was not a “particularly privacy-invasive measure” in the circumstances. Although this statement does not offer employers a significant degree of guidance, the Privacy Commissioner herself made the following comment just several days after *PIPEDA Case Summary 351* was published:

I think there is a qualitative difference between video surveillance and GPS in a vehicle. The information collected by a video camera is far more intimate. When a video camera is pointed at you, you can't even pause to scratch your nose without that information being collected. GPS can't do that.²¹

PIPEDA Case Summary 351 also includes some important limiting statements on the use of GPS monitoring for employment management purposes. The adjudicator criticized the employer for failing to give employees' clear notice of its employment management purpose. She also held that an employer using GPS monitoring for other legitimate business purposes (e.g. dispatch and routing purposes) should limit the extent to which it uses GPS monitoring for employment management purposes:

While the Assistant Commissioner could accept its use in certain situations, which are defined and communicated to employees beforehand, GPS data should not be used as a matter of course in employee management situations. Should the company contemplate using GPS for such employee management purposes, we asked that it be clear to employees about such purposes and establish a policy outlining an appropriate process of warnings and progressive monitoring. We asked that the company ensure that only through that process should GPS data be collected and used for employee management purposes.

The company provided us with a copy of a policy on GPS data utilization for performance management. This document spells out the situations in which the

²¹ Jennifer Stoddart, “Finding the right workplace privacy balance” (30 November 2006) online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/speech/2006/sp-d_061130_e.asp>. For a somewhat more conservative view on the privacy implications of GPS technology see Tom Wright, “Geographic Information Systems” April 1997 online: Office of the Information and Privacy Commissioner/Ontario <<http://www.ipc.on.ca/images/Resources/gis.pdf>>.

company will use GPS data for performance management. These include investigating a complaint from a member of the public; investigating concerns raised internally; and addressing productivity issues.²²

This important statement suggests that managers should be able to look at employee location information and use it for route planning and management, for example, while refraining from using it for employee management. While this may seem like it creates an artificial distinction, restricting the use of personal information by policy despite giving access to it is a common way of managing privacy and confidentiality. Confidentiality and non-disclosure agreements, for example, grant a right of access to information on the condition that the information is only used and disclosed for a limited purpose. Protecting employee privacy by workplace policy is also not new. Even in the 1979 *Puretex Knitting* decision, Arbitrator Ellis suggested that restricting the use of information by policy is means by which an otherwise improper surveillance system could be saved:

Changes in the quality and purpose of the surveillance may also lessen its "inhuman" quality so that less compelling considerations of efficiency would be seen to justify its use. Thus, where a company gives assurances that cameras will not be resorted to for disciplinary purposes or for supervising production work, even constant surveillance may be justified in order to deal with a massive intractable security problem.²³

Despite this statement, the positioning of video cameras (and not workplace policy) has been the central issue in most video surveillance disputes.²⁴ Yet based on *PIPEDA Case Summary #351*, employers can expect that GPS monitoring systems will be assessed differently, with policy restrictions being they key determinant of whether an employer has given proper consideration to employee privacy rights.

²² *PIPEDA Case Summary #351*, supra note 19 at para. 29 (emphasis added).

²³ *Puretex Knitting*, supra note 2, at 30.

²⁴ See, however, *Re Calgary Herald and C.G.I.U., Loc. 34M* (2004), 126 L.A.C. (4th) 386 (Tettensor) for a case where a surveillance grievance was dismissed but where the arbitrator declared the system should only be used for disciplinary purposes related to the purpose of installing the cameras (maintaining the safety and security of equipment).

This same approach is likely to prevail in disputes over keystroke monitoring, as illustrated by a decision of the Alberta Privacy Commissioner in *Re Parkland Regional Library* – a case where the Commissioner found that an employer had violated the *Alberta Personal Information Protection Act* by installing keystroke monitoring software on an employee's computer without the employee's knowledge and without adequate grounds.²⁵ Although the employer claimed that it had reason to be concerned about the employee's productivity, the Commissioner doubted this claim and ultimately upheld the employee's complaint. Although he clearly established a high standard for using keystroke monitoring technology to monitor employee productivity, he did not rule out using this highly-invasive technology provided it was based on an appropriate accepted use policy. He said:

In my view, information collected by keystroke logging software becomes "necessary" within the meaning of section 33(c) of the Act only when there is no less intrusive way of collecting sufficient information to address a particular management issue. Furthermore, surreptitious use of the software will result in "necessary" information only where forewarning employees that such a program will be used means that information needed for management cannot be collected.

For example, if keying in text were the primary task for a job, and speed and accuracy were agreed performance measures, the use of keystroke logging software might be justified. The information could be "necessary" in such a case because other indications of performance would not be as effective or efficient. However, there would be no reason not to inform the employee that such a measure would be taken, either consistently or periodically. To give another example, if an employer had reason to believe an employee was using office equipment to surf the net on office time, information collected by keystroke logging software could become "necessary". However, this would be only after the employer had developed and conveyed to the employees a written "accepted use policy" relative to their computers.²⁶

²⁵ [2005] A.I.P.C.D. No. 23 (QL).

²⁶ *Ibid.* at paras. 30, 31.

This statement by the Alberta Commissioner contemplates addressing the use of keystroke logging technology through an acceptable use policy (also often called a “computer use policy”) and embedding into the policy a needs-based standard for managerial use. Although the precise standard is yet to be determined (and will vary in the context), *Parkland Regional Library* provides another good example of how workplace policy can be used to strike an appropriate balance between employee and employer rights.

Does *Parkland Regional Library* mean that a computer use policy must also restrict managers from reviewing employee electronic communications unless they have reasonable grounds? Although many employers choose to include statements in their computer use policies by which they undertake not to review employee communications unless certain conditions exist, labour arbitrators have generally given employers much greater leeway in monitoring employee communications.²⁷ Even the Privacy Commissioner of Canada has recently recognized that it may be inappropriate to apply a balancing approach to the monitoring of employee communications: “In other areas, however, I see Canada adopting a more U.S.-style approach. Companies can look at what we’re doing on the internet – if they tell us – because we are surfing on company time and with company and equipment and energy.”²⁸ Employers should always exercise their right to monitor employee communications prudently but *Parkland Regional Library* is not inconsistent with the Privacy Commissioner of Canada’s relatively permissive view nor is it inconsistent with the prevailing arbitral case law.

Conclusion

The case law I have described in this paper provides a good illustration of how management rights and employee privacy rights have been balanced by labour arbitrators and privacy adjudicators, and the real hesitance of these decision-makers to endorse technology as a means of improving employee productivity. We can expect the advent of more new technologies with the potential to improve how employees are managed. I would encourage employers to evaluate

²⁷ See e.g. *Re International Association of Bridge, Local Union No. 97 and Structural and Ornamental Ironworkers and Office and Technical Employees Union, Local 15*, [1997] B.C.C.A.A. No. 630 (Bruce), *Re Insurance Corporation of British Columbia* (27 January 1994, Weiler) and *Re British Columbia and British Columbia Government Employees’ Union (Bradley)*, [1995] B.C.A.A.A. No. 171 (Bird).

²⁸ Finding the right workplace privacy balance, *supra* note 21.

these opportunities, and in doing so recognize their obligation to balance employee privacy rights with their own interests by conducting a privacy impact assessment as part of their evaluation and planning process. I am positive about cases such as *Pope & Talbot, PIPEDA Case Summary #351* and *Re Parkland Library* because they highlight that the proper balance can be struck in subtle ways. Employers should do more than just ask, “Yes or no?” Rather, they should also ask, “How?” Those employers who do, and who are able to implement a system that they can defend as striking a reasonable balance may find their creativity is rewarded.

April 20, 2007