NEW TECHNOLOGY AND SOCIAL MEDIA IN THE WORKPLACE

November 27, 2009

Carolyn MacEachern and Stephanie James

NEW TECHNOLOGY AND SOCIAL MEDIA IN THE WORKPLACE

I. INTRODUCTION

Employee use of the internet and email, both at work and at home, raises unique challenges for employers given the proliferation of the content on the internet and expanding social networking applications. Employee use of these technologies raises not only performance issues but also questions about the extent to which employers have the right to monitor their employees.

Social networking applications are internet based services that enable online communities of persons to communicate. The current dominant social networking services include Facebook, Twitter, LinkedIn, MySpace and YouTube. These sites, as well as the increasing number of individuals who have personal blogs, create the potential for the very public dissemination of private workplace issues. Many employers use these social networking applications for business purposes, which raises a whole host of issues. However, this paper focuses on performance management and employee privacy issues that arise from employee use of the internet, email and social networking applications.

We also discuss the introduction of Global Positioning Systems ("GPS") as this technology is becoming more prevalent and also raises employee privacy issues when the information collected by GPS is used for performance management purposes.

II. INAPPROPRIATE USE OF TECHNOLOGY: ON-DUTY CONDUCT

While most local government employees likely have legitimate, work-related reasons to be using workplace technology like cell phones, email and the internet, the inappropriate use of these technologies can lead to several concerns.

From a performance management perspective, personal use of workplace technology can amount to a serious negative influence on productivity: various human resource surveys suggest that employees may spend up to one or two hours per workday surfing the internet and sending emails for personal, not work, purposes. While some organizations may permit some personal use, excessive use often causes employers to consider disciplining for time theft.

Apart from the amount of time employees spend engaging in personal use of workplace technology during the workday, when that technology is used to view, collect or disseminate inappropriate content, again employers have cause for concern. Use of workplace computers to access and distribute pornography, for example, frequently results in discipline and workplace harassment complaints. It can also result in serious criminal investigations and actual or potential security breaches of an employer's electronic network.

As the labour and human rights cases described below illustrate, while solid and clear workplace policies are extremely important, arbitrators and decision-makers look to employees to demonstrate common sense in their use of workplace technology.

A. Mi Casa es Su Casa: Using Employer's Technology for Personal Business

A labour arbitration decision from 2009 involving the dismissal of a Telus employee on Vancouver Island highlights the many ways in which an employee can misuse workplace technology *(Telus Communications Inc. v. Telecommunications Workers' Union (Lights Pencer Dismissal Grievance),* [2009] C.L.A.D. No. 189 (Gordon)).

The grievor, an installer/repairer employed by Telus since 1979, was dismissed in 2007 for numerous grounds Telus collectively described as a "breach of our trust" and certain specific breaches of its workplace ethics policy. Telus alleged the grievor used his work computer and cell phone for personal business and to send offensive emails and that he tampered with his computer's hard drives and ultimately deleted computer entries to thwart Telus' investigation into his conduct.

The Arbitrator found clear evidence that the grievor had indeed used his Telus laptop to store customer records from his personal business, and that he deleted those files from the computer prior to surrendering it for investigation. She concluded these actions constituted a breach of trust and violated various provisions of Telus' workplace policies. While she concluded that the actual number of non-Telus related phone calls received or made on the grievor's Telus cell phone was not unreasonable, the fact that they were in respect of his personal business, for which he carried a separate cell phone, rendered them inappropriate. She also found his acts in replying to two spam email messages with vulgar responses not only an inappropriate use of his Telus email account but, more importantly, a serious security violation. In light of the nature of the grievor's violations, his less than honest demeanor at arbitration, and his significant disciplinary record (he was terminated previously and reinstated subject to a last chance agreement), the Arbitrator agreed that the employment relationship had been irreparable harmed and his dismissal was upheld.

B. Adding Insult to Injury: Using Employer's Technology to Insult Your Boss

One of the earliest recorded decisions in B.C. involving employee misconduct and "new" technology involves a laboratory technologist at Camosun College who decided to send a lengthy email very critical of certain professors and the College administration in general to a Union chat-group using the College's computer network *(Camosun College v. CUPE, Local 2081 (Metcalfe Grievance),* [1999] B.C.C.A.A.A. No. 490 (Germaine)).

The College dismissed the employee, alleging he was insubordinate and had breached his duty of fidelity. The Union grieved, arguing that the email was both confidential and privileged and therefore could not give rise to discipline at all, let alone dismissal.

Arbitrator Germaine upheld the dismissal. In response to the Union's argument that the email was confidential and privileged, he noted that the email in question was not intercepted by any surreptitious monitoring; rather, it came to the College's attention because it was forwarded to administration by a chat-group subscriber. The Arbitrator concluded that this was a consequence the grievor must have, or reasonably ought to have had, in mind when drafting the email. As such, he had no expectation of privacy or confidentiality.

C. They Should Have Known Better: Offensive Text Messages

Two North Vancouver R.C.M.P. officers were dismissed from the force in 2004 following a lengthy investigation and hearing into a series of inappropriate text messages sent and received by them over a five-month period. The offensive messages were displayed through the force's integrated information computer database, and were discovered by another officer when she used one of the offending officer's vehicles after his shift concluded.

The texts were described as including:

- Profanities, obscenities and vulgarities
- Sexually suggestive comments, often in the context of identifiable people including other R.C.M.P. members, telecommunication operators and the general public
- At least one "racially insensitive comment"
- Messages expressing the officers' desire to use excessive force in the course of their job
- Messages indicating the officers avoided taking calls or otherwise neglected their duties
- "A significant number" of messages containing disparaging remarks about other R.C.M.P. members' personal lives, sexual practices, physical attributes and police work

(Kinsey v. Canada (Attorney General), 2007 FC 543 at para.7)

Need we say more?

D. They Should Have Known Better, Part 2: Pornography on the Workplace Computer

There have been several cases in various forums involving employees dismissed for using their workplace computers to view, download or transmit pornography.

In 2001, an Alberta-based Telus call centre employee was terminated after an investigation revealed that he had been using his workplace email account to send emails to coworkers and external email addresses containing pornographic images. The Arbitrator's award *(Telus Mobility v. Telecommunications Workers Union (Lee Grievance)* (2001), 102 L.A.C. (4th) 239 (Sims)) notes that Telus' Code of Ethics and computer use policy had been brought to the employee's attention in a one-on-one meeting that occurred after the employee's supervisor found an initial set of offensive emails. Although the Union argued that there was no specific workplace rule setting out what types of emails could and could not be sent using employees' email accounts, and further that Telus had allowed a workplace culture to develop in which this type of "humour" was acceptable, the extreme nature of the emails sent by the grievor and the fact that he continued to send the emails after the meeting warning him against such conduct appear to have been detrimental to his defence. The Arbitrator noted:

> I find that the conduct established in this case is of such a nature that no specific rule is needed in order to justify discipline. […] it should be self-evident to any employee that using the employer's email facilities to send seriously pornographic material to other employees or elsewhere is unacceptable conduct. I exclude from this the now ubiquitous chain letters with the list of jokes, sayings, reasons why men (or women) are inferior to the opposite sex and so on. I also exclude the relatively innocuous cartoons, even those with a somewhat racy aspect.
>
> However, the materials in this case are well beyond all that and into the realm where no thinking employee would be under the impression they would be acceptable to the Employer. The grievor's receiving, storing and forwarding this material is, without any rule, just cause for discipline. (paras. 71-72)

The idea of employees being required to exercise common sense was reiterated in a 2003 labour arbitration decision involving several disciplined corrections officers at the Kent Institution in Agassiz *(Briar v. Treasury Board (Solicitor General Canada—Correction Service)*, 2003 PSSRB 3 (Taylor)). A total of 54 employees were disciplined for unacceptable use of Correctional Service Canada's electronic network.

Evidence at the hearing included no less than five employer directives, two policies and two "notes to staff" regarding acceptable and unacceptable use of the electronic network, all of which were circulated to staff at the Kent Institution. Interestingly, the network was also set up with a notice that appeared upon log-on that warned against inappropriate and unlawful use of the network. To access the network and all email programs, an employee had to acknowledge the warning notice by clicking "OK".

Arbitrator Taylor notes that the employer's investigation was not conducted as a broad audit of all employees' email accounts. It was prompted by a complaint about one specific employee, and then expanded to include all employees whose email accounts had sent or received emails to

that individual. The investigator did not actively monitor the affected employees' accounts, but rather took an electronic snapshot of the accounts on a randomly selected date. Discipline was imposed based only on any inappropriate messages or content located on employees' computers that day. The discipline imposed was based on numerous factors including the quantity and severity of messages sent and received, the employee's length of service and disciplinary record, and whether the employee expressed any remorse for the misconduct.

In response to the Union's argument that the grievors were not made aware of the employer's policies or provided adequate training, Arbitrator Taylor noted:

> First, the employer's policies were repeated at least five times between September 1999 and May 2000. Second, from June 2000, the grievors were met with a 'warning' every time they logged on to their email accounts and were compelled to acknowledge that warning in order to obtain access to that account. Third, common sense must prevail. The grievors knew, or ought to have known, that the use of the employer's system for sexually explicit material was inappropriate. (para. 51)

Citing a critical article in the Abbotsford News as evidence that the grievors' email usage was public knowledge, Arbitrator Taylor also noted that the grievors' conduct brought the operation of the Institution into disrepute:

> It must also be said that the Correctional Service is an employer which must continuously strive for public confidence and respect. The activities engaged in by the grievors can only detract from that objective. (para. 68)

The Arbitrator concluded there was just cause for discipline, and that the disciplinary penalties awarded were appropriate.

The recent human rights decision in *D.D. v. H.A.*, 2008 BCHRT 361, provides an interesting, but cursory, examination of the intersection between an employee's alleged mental disability and his misuse of workplace technology. In that case, the complainant filed a complaint with the Human Rights Tribunal alleging his employer, a regional health authority, discriminated against him in his employment because of his mental disability contrary to the *Human Rights Code*. The health authority successfully applied to have the complaint against it dismissed at a preliminary stage.

The complainant worked as a human resources officer in a small satellite office of the health authority. In 2006, he sent an email to his supervisor advising her that he was suffering from psychological difficulties. The supervisor then met with the complainant, helped him access the employee assistance program, and periodically followed up with him to see how he was progressing. During this time, the complainant's work performance was consistent and non-problematic. In the spring of 2007, the complainant reported that he was better and no longer using the counseling services provided by the employee assistance program.

Later in 2007, the health authority's IT manager contacted the supervisor to report that while the IT manager was investigating a different employee's internet use, unusual patterns of use by the complainant were inadvertently discovered. In addition to frequent accessing of social networking sites like Facebook, the IT manager concluded that the complainant spent up to three hours at a time accessing pornography sites from his workplace computer. The supervisor and a senior human resources manager considered that the complainant's internet use was not only inappropriate and in breach of the health authority's policies, but also constituted time theft. They met with the complainant, presented him with his internet usage audit information, and essentially offered him the option of resigning or being terminated. Their evidence is that they specifically cautioned the complainant to take some time to think about his options and to seek legal advice before making a decision. However, the complainant elected to resign on the spot.

A short time later the complainant alleged that the health authority had forced him to resign while he was in a state of mental distress, further claiming that his supervisor should have known he suffered from a mental disability on the basis of the email he had sent over a year prior stating he had psychological difficulties. The health authority declined to reinstate the complainant despite his many requests that it do so. The complainant then filed a human rights complaint.

The Tribunal member granted the health authority's application to dismiss the complaint, finding there was "no reasonable prospect that the complainant would succeed in showing that the respondents knew, or ought to have known, as of September 5, 2007 [the date of his dismissal] that his inappropriate access of the internet was the manifestation of a mental disability, such that the respondents were required to initiate the accommodation process" (para. 91).

III. INAPPROPRIATE USE OF TECHNOLOGY: OFF-DUTY CONDUCT

As discussed above, the inappropriate use of the internet and email while at work can result in numerous concerns for employers, many of which may be addressed through disciplinary measures. A more difficult situation arises when employees misuse these communication media off-duty by, for example, posting inappropriate messages in a personal blog.

Although it is a well-established principle that employers are not the custodians of their employees' private lives (i.e., off-duty conduct is generally not subject to workplace discipline), employee misuse of electronic communication is perhaps one of the few areas where arbitrators and decision-makers are increasingly willing to consider whether discipline is warranted. As with on-duty conduct, off-duty communication can become problematic if it is harassing or discriminatory, if it is insubordinate of management or the employer, or if it discloses confidential workplace information.

A. Bloggers Beware

In *Chatham-Kent (Municipality) v. CAW-Canada, Local 127 (Clarke Grievance)* (2007), 159 L.A.C. (4th) 321 (Williamson), a municipal employee learned the hard way that ignorance of the public nature of a MySpace blog will not excuse insubordinate postings and confidentiality breaches.

The employee, a personal caregiver at a residential care facility, was terminated after her supervisors became aware of her public blog. The blog contained photographs of co-workers and residents along with a diary detailing the ins and outs of the employee's job, including references to co-workers and residents by initials, thinly veiled pseudonyms, or by their real first names. Arbitrator Williamson succinctly summarized the blog's contents: "the ill-written blog is blunt and laced with coarse language, and could generally be described as bitchy in style with an attempt at humour" (para. 4).

The facility required all employees to sign a confidentiality agreement regarding the privacy of residents, their families, and other employees. The grievor had signed the confidentiality agreement twice and reviewed it annually as part of her workplace training.

The grievor professed to be "not a very computer literate person", claiming she thought the MySpace page was private and only accessible by three co-workers. At the arbitration hearing, the employer introduced extensive evidence detailing all of the screen shots the grievor would have seen at the time she created the blog. These clearly established that the grievor was required to fix the blog's settings as either "public" or "private", and the blog postings themselves indicated the grievor contemplated an audience broader than the three co-workers she knew to be actively reading the page.

In response to the Union's argument that the employer lacked any specific rules prohibiting the creation of personal MySpace pages, the Arbitrator concluded "it cannot be said that all employee conduct is acceptable unless there is some specific rule prohibiting it," (para. 21) and further:

> The rule is to not disclose any confidential information. All possible ways in which information may be disclosed or disseminated do not have to be spelled out in order to make the rule clear. The employer's requirement that residents' personal information be kept confidential by employees is seen to be clear and unequivocal. (para. 29)

The dismissal was upheld.

An Alberta arbitration panel came to a similar conclusion with respect to a provincial government employee who was dismissed because of the contents of her personal blog, which contained unflattering comments about her co-workers and management (*Alberta v. Alberta Union of Provincial Employees (R Grievance)*, [2008] A.G.A.A. No. 20 (Ponak)).

The grievor started a blog during a low point in her personal life, taking seriously her counsellor's recommendation to write things down as a way of venting her anger. Like the *Chatham-Kent* grievor, she used thinly veiled pseudonyms to describe her co-workers in the blog postings. Unlike the *Chatham-Kent* grievor, she was fully aware that her blog was publicly accessible.

The government's dismissal letter to the grievor indicated she was being dismissed for breaching the workplace Code of Ethics, though there was no evidence of this Code at the hearing and the government's arguments at that time focused more on the insubordinate nature of many of the comments in the grievor's blog postings. The majority of the panel agreed that the postings amounted to insubordination warranting discharge, dismissing the Union's argument that there was no real harm done to the employment relationship because very few people in the workplace were actually aware of the blog prior to the grievor's dismissal. The panel concluded that actual knowledge of the content was irrelevant: the key issue was the fact that the content was offensive and was publicly accessible. By posting her comments in a public domain, the grievor lost control over who could or would read them.

The British Columbia labour arbitration decision in *EV Logistics v. Retail Wholesale Union, Local 580 (Discharge Grievance)*, [2008] B.C.C.A.A.A. No. 22 (Laing) does an excellent job summarizing long-standing arbitral principles about discipline for off-duty conduct and applying them in the context of internet-based communication.

In that case, the grievor was dismissed after an anonymous co-worker complained about the content of his personal blog, which Arbitrator Laing described as ranging "from banal and bizarre to disturbing and hateful" (para. 52). The anonymous complainant expressed concerns primarily about entries on the blog that were disrespectful of persons of East Indian decent (the Arbitrator noted that approximately 40% of the grievor's co-workers were of East Indian decent). While some entries were inappropriate but benign (e.g. graphic details of the grievor's colon cleanse), many were scary, violent and hateful (e.g. fantasies about crushing people in cardboard compactors or pushing them down stairs, committing suicide in a meat grinder, detailed descriptions of his collection of Hitler paraphernalia and his quest to purchase a World War II SS uniform).

Of particular note, the blog clearly identified the employee as its author and included the employer's name and a description of its business activities. Further, the employer was at the time experiencing problems with racially-motivated graffiti and vandalism in the workplace.

Reviewing the arbitral law with respect to disciplining employees for off-duty conduct, particularly where actual harm to the employer or the employer's reputation has not been proven, Arbitrator Laing concluded:

> Obviously, measurable harm caused to an employer will make the case for an employer clearer and stronger. However, where the employment identity is linked to off-duty conduct that is sufficiently abhorrent or reprehensive, harm can be presumed, provided of course there is public access to the conduct. That condition applies here. […] <u>The Internet is a unique universe to which anyone with a computer has access and entry, which obviously includes customers, suppliers, the public, employees and potential employees. Clearly, there was a serous reputation risk to</u>

> the employer and the employer had the right to respond to the misconduct that caused that risk. (para. 60)

Given the grievor's clean disciplinary record, lengthy apology and true expression of remorse, the Arbitrator determined dismissal was excessive and reinstated the grievor with no back pay.

IV. LESSONS FOR EMPLOYERS

A. Privacy is Paramount: Use Least-Intrusive Means to Investigate Possible Violations

As entities subject to the *Freedom of Information and Protection of Privacy Act* ("FOIPOPA"), local governments have added duties to ensure that—even in respect of managing internal workplace matters—the privacy rights of their employees are upheld. FOIPOPA treats employees in the same manner as it does every other person about whom a local government may possess personal information. As such, all of the local government's statutory obligations under FOIPOPA, including the restrictions on what personal information may be collected, how it may be used and disclosed, and where and how it must be stored, apply to employees' personal information.

The difficulties employers subject to FOIPOPA face in administering internet use policies and investigating important matters like time theft are highlighted in the Information and Privacy Commissioner's 2007 decision in *Order F07-18: Re University of British Columbia*. In that case, UBC dismissed a unionized employee after investigating his personal internet use during work hours by installing software that surreptitiously tracked his internet activity. In addition to challenging the admissibility of the evidence before the labour arbitrator, the grievor filed a complaint under FOIPOPA alleging UBC lacked the statutory authority to collect the information and, in the alternative, if UBC did have the authority to collect the information, the manner in which it was collected violated the method of collection provisions in FOIPOPA. The grievor sought an order from the Commissioner's Office that the computer data be destroyed, knowing that if it was destroyed UBC would not be able to defend the concurrent labour grievance.

UBC argued that its use of surreptitious internet monitoring software was authorized under FOIPOPA as it was collecting personal information that related directly to and was necessary for an operating program or activity of the University. The employee conceded that UBC's human resources management and its management of workplace behaviour were operating programs of UBC and those programs may require the collection of some personal information to discipline employees. However, UBC collected much more than information about the amount of time the employee spent accessing the internet: it collected specific data about the nature of the employee's banking transactions, copies of his personal correspondence, and detailed screen shots of the sites he visited. The adjudicator found that none of that information was relevant to or necessary for any UBC program. The adjudicator further found that since the employee had always been very open and transparent about his use of the workplace computers, his integrity was not a "core issue" that justified surreptitious surveillance "when the employer had taken no other steps to address this issue, and there was no real evidence that alternative means of

addressing the problem would have been ineffective" (para. 90). The adjudicator concluded that UBC lacked the authority to collect the information.

Although the adjudicator did not need to go on to consider whether the manner in which UBC collected the personal information was lawful, she did so. First, the adjudicator concluded that the internet use data had been collected directly from the employee (generally a requirement under FOIPOPA) because it was recorded as a result of his own activities. However, FOIPOPA also required that UBC notify its employees that their personal information was being collected and the purpose and authority for the collection, unless one of the limited statutory exceptions allowing surreptitious collection applied. The adjudicator found that none of the exceptions applied, and therefore UBC failed to lawfully collect the information.

The UBC case makes it clear that employers monitoring employees' internet use must consider all methods by which they might be able to obtain the necessary information, and to use the least-intrusive method possible. It also suggests that surreptitious surveillance by employers subject to FOIPOPA will rarely be lawful.

The Alberta Information and Privacy Commissioner reached similar conclusions in a 2005 decision involving an employee of a public library board (*Order F2005-003: Re Parkland Regional Library*). Like the UBC case, the Commissioner agreed that "information that allows employers to know how employees are using their working time may, depending on the nature of the information, be necessary for the purposes of managing" (para. 12) and therefore a permitted ground for collecting personal information under the relevant privacy legislation. The Commissioner also concluded that there were less intrusive means of monitoring the complainant's personal internet use during working hours than the library had used (it had installed keystroke logging software on employees' computers), and that in any event the library's motivations or justifications for collecting the information in this specific case were not sufficiently clear to justify the significant privacy invasion.

B. *Charter* Rights

Despite the fact that several of the cases discussed above involve government and quasi-government employers to which the *Charter of Rights and Freedoms* apply, it is interesting that none of them have involved an analysis of the rights and freedoms protected in sections 2(b) and 7 of the *Charter*: the right to freedom of expression and the right to be free from unreasonable search and seizure. We think it is only a matter of time before these issues come to the forefront of labour and employment disputes with an employee or his or her union challenging the validity of discipline imposed by a government employer because of alleged *Charter* violations.

When drafting internet use policies, investigating possible misconduct, and making decisions about discipline for inappropriate use of workplace technology, we encourage local governments to keep these important rights and freedoms in mind. Proceeding with an appreciation for general *Charter* "rules of thumb" (like ensuring there is a well-identified and justifiable reason for a rule or decision, and using means that minimally impair an affected person's rights) should help employers rebut *Charter*-based challenges to their workplace disciplinary decisions.

V. INTERNET USE POLICIES

The proliferation of the use of the internet in the workplace and social networking applications and blogs presents difficult challenges for local governments in the management of their employees. As noted above, concerns related to employee productivity, inappropriate use of the internet, and off-duty blogging are just some of the issues facing employers. Other issues include inappropriate use of business email addresses and disclosure of confidential information.

Local governments need to be concerned about their own liability for inappropriate use by an employee of the internet or a business email address. This includes issues related to harassment by way of email or dissemination of inappropriate material such as pornography, disclosure of confidential information, defamatory comments in emails, and accidental or purposeful transmission of a computer virus.

Internet use policies are one tool local governments can use to set out their expectations regarding the use of the internet, types of prohibited conduct, to what extent internet use and email will be monitored and consequences for breaches of the policy. Obviously, productivity concerns with employee e-mail and internet use is one of the major issues that employers need to address in such policies. The policy should clearly set out if and when employees are permitted to use the internet and whether their business email address may be used for personal purposes. Internet use policies should explicitly forbid harassing, discriminatory or otherwise inappropriate use of email and state that discipline will result if the policy is breached.

As noted above, one of the more difficult issues for local governments is the extent to which they can monitor an employee's emails and use of the internet. Any monitoring should be addressed in an internet use policy. Local governments will need to justify any monitoring or surveillance and be able to show that less intrusive alternatives have been considered and why such measures are not adequate. Employees must be made aware of the potential for monitoring and informed of what types of activities will be monitored. As well, the actual monitoring must be conducted in a reasonable manner.

Local governments should also consult with their IT staff or service provider to discuss issues related to virus detection systems and ways to block access to certain internet sites. For example, local governments could simply block access to problematic sites such as those for social networking and instant messaging, as well as other highly accessed sites that are not appropriate for the workplace. This type of review should be done on a fairly regular basis given the proliferation of the types of internet sites that local governments may wish to block.

The following is a list of considerations for local governments regarding internet use policies:

1. The policy must be in writing and provided to all staff;

2. Have employees sign acknowledgements that they have received and that they understand the policy;

3. It should explicitly set out what activities are permitted and forbidden;

4. Confidentiality issues should be expressly addressed;

5. Prohibit conduct that could be construed as discriminatory, harassing, derogatory, obscene or otherwise inappropriate;

6. Prohibit use of social networking, instant messaging and personal websites while at work;

7. Set out circumstances, if any, under which employees may use business email and internet for personal use;

8. Explicitly set out any monitoring of employees' work emails or internet use;

9. Explain the security concerns of improper use of email or accidental downloading of viruses from the internet;

10. Be clear that a breach of the policy may be the subject of discipline, up to and including dismissal;

11. Set out to what extent the policy regulates off-duty conduct (ie, personal blogging); and

12. Review the policy on a regular basis and updated as needed.

While policies cannot prevent employee misuse of the internet and email, they are proactive measures to mitigate against the harmful effects of such misuse and will be the basis for any discipline. Local governments need to keep in mind that these policies must be reasonable, particularly any contemplated surveillance, and provided to all employees. As well, local governments need to consistently enforce the policies. Otherwise, they risk an employee successfully arguing that the local government has condoned breaches of the policy.

VI. GPS UNITS

Many employers, including local governments, have implemented GPS units in their vehicle fleets. The units are generally used to monitor the whereabouts and the operational aspects of the vehicles. This information can assist local governments in improving the efficiency and effectiveness of their vehicle fleets. The information gathered by GPS units also allows employers to monitor the performance of their employees as the units monitor various operational functions of a vehicle as well as where it has been driven each day and at what speed. Not surprisingly, unions and employees have concerns about the surveillance aspects of GPS units. Local governments must consider privacy issues in the implementation and use of GPS units both under labour law and FOIPOPA.

Arbitrators attempt to balance employee privacy issues against management's legitimate business interests with respect to the introduction of surveillance technologies. We are not aware of a successful arbitral challenge to the introduction of GPS units but in a recent arbitration, the Union raised a preliminary objection to the admissibility of data from the GPS unit in the grievor's vehicle, citing concerns about privacy and accuracy of the system (*Vaughn (City)*, [2009] O.L.A.A. No. 276). The Union then decided not to rely on its privacy arguments and focused solely on the accuracy of the system.

There is no discussion in this case as to why the Union chose to not pursue its privacy challenge but it may be an indication that the Union felt it would not be successful. The Union was aware of the implementation of the GPS vehicle tracking system and had previously raised concerns that it would be used for disciplinary purposes. The employer assured the Union it would not go on fishing expeditions but if an issue came to management's attention, they would review the GPS data. With respect to the challenge to the accuracy of the GPS information, the employer called the co-founder of the company that supplied the GPS units to testify about the system and the Arbitrator accepted his testimony and considered the evidence gathered from the GPS unit.

Even though it does not appear that there has been a successful challenge to a unionized employer's ability to introduce GPS units, cases involving the introduction of biometric scanning illustrate the difficulties employers can face with challenges by unions to the introduction of new technologies in the workplace. In two separate cases by the same arbitrator, the Union successfully challenged the introduction of biometric scanning for timekeeping and payroll purposes (*IKO Industries Ltd.* (2005), 140 L.A.C. (4th) 393 (Tims); *Dominion Colour Corp*., [2003] O.L.A.A. No. 785 (Tims)). In both of these cases, the Arbitrator concluded that the purposes of the biometric scanning did not justify the invasion of the employees' privacy.

In contrast, two other arbitrators have come to the opposite conclusion regarding similar technology. In *Canada Safeway Ltd.* (2005), 145 L.A.C. (4th) 1 (Ponak), the Arbitrator felt that the level of privacy intrusion of a hand scanner system was relatively low. He accepted the employer's reasons for introducing such a system, which were improving its time and attendance systems. The Arbitrator specifically acknowledged that he was coming to a different conclusion than Arbitrator Tims above.

In *Agropur* (2008), 180 L.A.C. (4th) 252 (Slotnick), the Arbitrator also accepted the employer's introduction of a time management system that involved mandatory finger tip scans. The Arbitrator recognized that employees have some privacy rights but that these rights are not absolute and that the greater the intrusion on privacy, the greater the business rationale that must be demonstrated. The Arbitrator in this case concluded that the infringement on privacy was at the low end of the spectrum and stated the following (para. 37):

> How great is the infringement on privacy of employees? In my view, the evidence reveals it to be extremely small, almost negligible. In fact, labeling this as an "invasion" of privacy strikes me as linguistic excess.

Again, the Arbitrator specifically noted the above cases decided by Arbitrator Tims and did not even attempt to distinguish the facts before him. He simply stated that he preferred the analysis in the *Canada Safeway* case.

These cases illustrate the different approach arbitrators can take regarding similar technologies. Regardless of who the arbitrator is, employers must ensure that they clearly articulate the purposes of the GPS units, the type of information that will be collected, the uses for that information, the safeguards for protecting any personal information collected as well as the business reasons for introducing the GPS units. We are of the view that the invasion of employees' privacy is lower than other surveillance technologies, such as video surveillance. Local governments need to ensure the Union and its employees are aware of the introduction of any GPS units, the purpose for the installation and the uses for the information is collected, which may include performance management. With respect to performance management, employers will have an easier time justifying the introduction of GPS units where they are not using the information as a surveillance method, but rather to gather evidence only if a specific issue comes to light.

As noted above, the introduction of GPS units raises issues under FOIPOPA. Although the Information and Privacy Commissioner for British Columbia has not issued a decision regarding GPS, the Federal Privacy Commissioner has urged caution with respect to the installation of GPS units. In a case summary under the federal private-sector privacy legislation (PIPEDA Case Summary #2006-351), the Assistant Federal Commissioner raised concerns about the use of GPS information for performance management purposes. In this case, employees complained when they learned their employer was going to install GPS units in their vehicles. The employer had notified affected employees, told them the rationale for implementing GPS, held meetings with the employees, and provided a copy of its GPS Policy.

The Assistant Federal Commissioner did not accept the employer's argument that the information collected by the GPS units was not the personal information of the employees as it tracked the movement and operation of vehicles. She determined this information falls within the scope of personal information for the following reason:

> As the information can be linked to specific employees driving the vehicles, they are *identifiable* even if they are not identified at all times to all users of the system.

The Assistant Federal Commissioner also stated her view that while using GPS to track a vehicle is not overly invasive of employees' privacy, the use of that information to routinely evaluate work performance based on assumptions drawn from GPS information does impact individual privacy. The company in this case had taken measures to limit the use of GPS as a general employee surveillance method. The company was clear that managers would not be monitoring employees via GPS but that the information may be used if an issue is raised with respect to a particular employee. As well, the company had instituted a policy that outlined what information was being collected and for what purposes. It also set out the safeguards for the protection of personal information and covered disclosure and retention of information collected via GPS.

The Assistant Federal Commissioner accepted the company's reason for installing GPS units and found no violation of the privacy legislation. However, the Assistant Federal Commissioner warned against "function creep" as follows:

> In other words, the purposes and uses of a particular technology should be precisely specified, and that technology should be restricted to its intended purposes.

Given the reasoning in the federal case regarding GPS, local governments will need to be prepared to justify the introduction of GPS units under FOIPOPA, particularly if the information will be used for performance management purposes. Under the Act, local governments have obligations regarding the collection, use, disclosure, protection and storage, and retention of personal information. Local governments need to clearly set out the legitimate business reasons for installing GPS units and how the information collected will be used for performance management. As in the labour law context, the less the information is being used for general employee surveillance, the more likely a local government will be able to successfully justify the introduction and use of GPS units for performance management.

Given the requirements under labour law and FOIPOPA, we recommend developing a policy regarding the collection, use and disclosure of personal information collected by GPS units that addresses the following issues:

1. the type of information that will be collected;
2. the purposes for which the information will be used;
3. contact information of the manager(s) who can answer questions about the collection of the personal information;
4. who will be authorized to access any personal information;
5. training that will be provided to managers with respect to the use and disclosure of personal information;
6. how the personal information will be stored;
7. security arrangements in place to protect the personal information; and
8. a retention and destruction schedule.

VII. CONCLUSION

While new technology and applications of these technologies is ever and fast changing, arbitrators seem to be applying traditional labour relations principles in their analysis of whether discipline is warranted. Arbitrators have been clear that discipline, including dismissal, will be justified, even for off-duty conduct, where an employee has made inappropriate use of the

internet or their business email address. Like any other policy, internet use policies in unionized workplaces must be reasonable and consistent with the collective agreement. As noted above, a well drafted and consistently enforced internet policy will assist employers in justifying any disciplinary action.

Privacy adjudicators will also review the reasonableness of an employer's use of technology that constitutes a form of surveillance, whether it is the use of GPS units for performance management or installing keystroke software. When employers wish to use technology to monitor employee performance, an employer must be prepared to justify the privacy intrusion and demonstrate that less invasive measures would be ineffective.

New issues will no doubt arise in the coming years that will continue to challenge both local governments and decision makers. By implementing and enforcing internet use policies, local government will be taking the necessary steps to ensure employees are aware of their obligations and of the consequences should they breach the policy or otherwise make inappropriate use of new technologies.