PRIVATE SECTOR PRIVACY IN A CHANGING WORLD

PIPA CONFERENCE 2007: AN EDUCATIONAL FORUM FOR BUSINESSES & NON-PROFITS

3A: EMPLOYEE SURVEILLANCE: INVASIVE SPYING OR REASONABLE MONITORING

SEPTEMBER 20, 2007

Prepared by: Lorene A. Novakowski
Fasken Martineau DuMoulin
Barristers & Solicitors
Patent & Trademark Agents
2100, 1075 West Georgia Street
Vancouver BC V6E 3G2
Phone: 604-631-3216
Fax: 604-632-3216

PIPA CONFERENCE MATERIALS

Surveillance Issues – Network Use Monitoring and Other Modern Technology Issues

The issue regarding employer monitoring of e-mails has been a live issue for many years, given the availability of this technology in the workplace. A useful decision is an arbitration decision of Arbitrator Germaine: *Camosun College v. Canadian Union of Public Employees, Local 2081* [1999] B.C.C.A.A.A No. 490. In that case, Mr. Metcalfe, the Grievor, had forwarded a lengthy e-mail to a Union user group on his employer's computer network. Contained in the e-mail were allegations against faculty members, the College and the College's administration. The message was then circulated beyond the user group. The Grievor was terminated from employment.

The Employer's position was that the e-mail was a breach of the Grievor's duty of fidelity, as well as insubordination. The Union's position was that, as the e-mail had been sent originally to a user group composed only of Union members, it was confidential and privileged. As the message was intended only for the Union members, the Grievor was making legitimate use of a list. The Union argued that, because the College had allowed the Union to establish a user group for Union members only, the College could not then take the position that Union members were prohibited from communicating using that internal list to send Union messages.

The Arbitrator found that the nature of the medium could not support a claim for confidentiality, relying on *Smyth v. Pillsbury Company.* 914 F. Supp. 97 (E.D.P. 1996). The Arbitrator also relied on *Insurance Company of British Columbia* (January 27, 1994); in that case the arbitrator found that there was not the same reasonable expectations of personal privacy for employees using an e-mail system belonging to the employer, as there would be for other forms of communications, such as a private letter mail system.

Standard e-mail and computer use policies will typically state that there is no reasonable expectation of privacy over the use of the e-mail system. In addition, Privacy Commissioners have told us that if an organization is going to monitor e-mail usage by employees, at a minimum employees should be notified as to how their personal information will be collected, used and disclosed, as well as being notified if they might be subject to random or continuous surveillance. With respect to the latter, organizations should have reasonable cause to conduct

specific surveillance of an employee. See, for example, the answer to an FAQ on the Office of the Information and Privacy Commissioner of Alberta's website: *http://www.oipc.ab.ca/Search/DetailsPage.cfm?ID=1580.*

This approach was also referred to an Investigation Report from the Alberta Commissioner in 2006: *Alberta Regional Council of Carpenters, Investigation P2006-IR-004*. In that case, the Commissioner explored the due diligence required by an organization to ensure that it properly protected personal information. The Commissioner stated at paragraph 42:

> I hesitate to recommend that, in this case, more should have been done to protect against this type of threat by a trusted member of the staff who had legitimate access to the system. I considered whether every organization holding personal information in a computer system could reasonably be expected to proactively monitor all employee activity with respect to every database. Such monitoring could include installation of surveillance cameras at every days, keystroke logging software and audit capacity activated and monitored 24-7, and review of all internet activity and email. The International Union had all of these tools available to them and implemented their use immediately upon suspicion of unusual activity. I find this to be a reasonable response. Implementing all of these measures for all employees has significant privacy and resource implications. I believe that expecting these measures in every case would be too onerous. I find that there was no reason for putting this individual under surveillance until unusual activity was detected by the system administrators. They acted reasonably in trusting him to abide by policies.

A more specific analysis of the use of keystroke logging software to monitor an employee: *Parkland Regional Library Order F2005-003*. This case involved the public sector employer, Parkland Library, which had installed keystroke logging software on the computer of an employee who worked in the Information Technology area. The issue turned on whether the public body had the right and the authority to collect the information. Under public sector legislation, public bodies can collect, use and disclose information generally, as provided for by statutory authority or where it relates directly to, and is necessary, for an operating program or activity of a public body. In this case, the public body relied on the latter provision for collecting the information, saying that the information was necessary to manage the employee. In analyzing the issue, the evidence came to light that the public body had concerns about this

particular employee's use of the computer system. On one occasion, the supervisor had passed by the employee and noted that the employee's personal website was called up on his screen at a time that the supervisor thought that he was supposed to be working. The supervisor also said that the employee appeared to be spending more time on work-related tasks which had a lower priority than the tasks the supervisor thought the employee should be working on.

At paragraph 15, the Commissioner notes that the one time event of seeing the employee's personal website called up on the screen did not constitute evidence establishing a concern about the employee's use of his computer, that was sufficiently serious to warrant collecting all future keystroke entries. With respect to the other concerns about the work being performed, the Commissioner noted that the supervisor sat just a few feet away and could have handled the employment management issue through other means such as a discussion with the employee, coupled with a warning if necessary. The Commissioner found that the public body had failed to demonstrate its authority to collect personal information, as it had not demonstrated that the information was necessary for the management of the employment relationship. The Commissioner said at paragraph 30:

> 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.

The Commissioner went on to note that information could be necessary in a case where, for example, speed and accuracy were agreed to performance measures. However, if an employer thought that the employee was using office equipment for improper purposes, keystroke, logging software could become "necessary" but only after the employer had notified employees of the computer use policy. The Commissioner went on to note that in order for information to be collected surreptitiously, the employer would have to show that had considered all other options to obtain the information before proceeding.

Another source of monitoring activity has arisen as a result of the explosion in the use of blogs and social networking. A blog is a site where entries are made by individuals. Social network services are online forms of communities of people, usually conducted online. Some of the most popular social networks today include MySpace, and Facebook. In these kinds of services, users can create a profile that allows the user to control who would have access to that site. There are risks, however, of information being removed from the user's site and passed on by third parties. Users should also take note of the Terms of Use. Facebook's Terms of Use state (*inter alia*) that "by posting User Content to any part of the Site, you automatically grant… to the Company, an irrevocable, perpetual, non-exclusive, transferable, fully paid worldwide license… to use, copy, publicly perform, publicly display… and distribute such User Content…" Some users have realized that while you can erase posts, user content can remain available on the Web.

More and more organizations are monitoring these social networking sites to see what their employees are up to. A number of schools, both in the US and Canada, have used Facebook to the detriment of the users. In the case of user groups, for example, which might include an entire college campus, college administration usually signs up for the service as well.

In one arbitration involving an employee who was terminated for disclosing personal information on her blog which was accessible to the public, about the residents in a care home in which she worked, the arbitrator dismissed the Grievor's evidence that she thought she had set up a private blog: *Chatham-Kent –and- CAW Canada, Local 127* 159 LAC (4^{th}) 321. The Grievor's evidence was that she was not computer literate and that she relied on her fellow workers who had told her how to set up the permission screen so that only a few co-workers would be able to view the blog. However, the Grievor did not make any changes to the permission setting on the screen, thereby creating a public setting for her blog. The Arbitrator found that at best she was careless in ignoring the message given to her when setting up her blog. She had set it up in a way that was not outside her control and not accidental and could have been avoided by the exercise of due care.

The privacy issues, more generally, with respect to organizations' reviewing their employees' social networking or blogging sites have yet to be explored in detail in any decision. Clearly what is being placed on these sites includes personal information. Where the site is public as in

the *Chatham-Kent* decision noted above, arguably the individual has no reasonable expectation of privacy over the personal information that they have posted on the site. In fact, an argument can be made under B.C. PIPA Regulation 6(e) that the personal information is printed in an electronic publication that is available to the public such that no consent is required to collect, use or disclose the information. Similarly, Section 7(e) of the Alberta Regulations defines publicly available information as personal information contained in *inter alia* an electronic publication, if the publication is available to the public and it is reasonable to assume that the individual that the information is about, provided the information.

Where users have set preferences to limit who has access to their information arguably these definitions may not apply, i.e. the information is not "available to the public". But what about the Terms of Use – should the user be taken to know that the information they post is owned irrevocably and subject to distribution by the website host?

If the information is not publicly available, an organization would have to rely on an exception to consent for collection of the information, such as for purposes of an investigation into a breach of an employment agreement, or relying on the framework for dealing with employee personal information, i.e. on the basis that the collection is reasonable for the purposes of managing the employment relationship, having notified employees in advance of the purposes of the collection. Public sector employers have to consider whether they have the right to collect the information.

While this new area of the law is developing, some organizations might want to take note of the practices of other organizations which is to not encourage blogging, but to accept that it will occur and establish extensive policies for the rules for employee blogging. One example is Sun Microsystems, which does encourage employees to blog, but gives employees rules about their expectations. Other companies include IBM and Yahoo! Different considerations arise, for example, for public sector employers or large publicly traded private sector employers who may need to set guidelines about what employees can and cannot say on blogs, particularly to remind employees that the concept of "free speech" has limits in the employment context.