

Employee computer monitoring – Wither the most certain management right of all?¹

Good morning.

In this segment on workplace privacy I've chosen to describe the prevailing rule on employee computer monitoring and explain how that rule might be giving way. I'll do this in three parts.

- First, I'll describe why courts and arbitrators have consistently said that employees have no expectation of privacy in using their employers' computer systems.
- Second, I'll identify an early sign that this prevailing view may one day be replaced with a view that requires a balancing of management and employee interests.
- Third, I'll identify two recent and very radical cases that I believe go too far in recognizing employee privacy interests because they suggest an employer has no right of control over employees' non work-related communications.

My thesis is that new patterns of computer use are engendering employee privacy expectations that employers must immediately reckon with. I'll end with a short discussion of what steps employers should take immediately.

No expectation of privacy view

Few rules are certain in law, but one of the most certain rules for management lawyers in the last ten years was one which said that employers could do a full examination of an employee's computer with no justification at all.

This view rests on three factors:

- First, it rests on notification. Most employers advise employees that they will audit or investigate computer use, and in a reasonable expectation of privacy analysis, this type of notice does count.
- Second, it rests on the fact that the employer owns the medium. Decision-makers recognize that employers, as system owners, have too many legitimate reasons to examine their systems for employees to expect privacy in their computer use.
- Third, it rests on the insecure nature of e-mail communications. In a case last month an arbitrator said that sending an e-mail is like sending a post card. This

¹ Dan Michaluk. Lawyer at Hicks Morley. A speech prepared for the OBA's "Hot Issues in Privacy Law" seminar, held in Toronto on June 9, 2009. These views are my own and neither that of Hicks Morley nor its clients.

idea has been used to find that employee e-mail communications, in particular, are not private.

So this is the view that is reflected in the majority of cases decided until recently. Under it, employees have no reasonable privacy expectation at all, so employers can access any of their stored information without any justification.

The balancing of interests view

The first Canadian decision to depart from the “no expectation of privacy” view and actually balance management versus employee interests is a case called *Lethbridge Community College* from the middle of 2007.

Lethbridge is about a college that did a forensic analysis of an instructor’s work computer and obtained e-mails from his MS Hotmail account. These e-mails contained damaging information, and the instructor’s union argued they were inadmissible in his termination arbitration. In the end, Arbitrator Allen Ponak held the e-mails were admissible because the college had reasonable grounds to conduct its forensic investigation.

Though this decision seems aggressive on employer rights because it endorsed access to an employee’s *personal* e-mail account, its significance really lies in the recognition of an employee privacy interest. The case suggests that employers should have reasonable grounds to access information stored on their own systems and, as I’ve said, this is a Canadian first.

The beyond control view

Arbitrator Ponak’s balancing of interests is new but not necessarily radical. There are, however, more recent cases that go much further and suggest that employers have no control over employee communications that are not work related.

The first is *Johnson and Bell Canada*. This was about a request for access to personal information under PIPEDA, and in particular, access to “personal” e-mails about a former employee. Mr. Justice Zinn of the Federal Court held that these “personal” e-mails were not subject to PIPEDA because they were personal rather than communicated “in connection with the operation of a federal work or undertaking.” Mr. Justice Zinn said personal e-mails on a business computer system are merely the “by-catch of commercially valuable information.” He also suggested that the employees sending and receiving these e-mails have a privacy interest that weighs against another’s right of access.

The second case is an unreported labour arbitration case involving the University of Ottawa and its faculty that was decided by arbitrator Philip Chodos in September 2008. The University was brought under public sector freedom of information legislation in 2006, and after it received its very first access request sent a collection notice to the entire faculty asking it to turn over responsive records. The association then grieved.

In the end, Arbitrator Chodos held only that the University violated its collective agreement by sending the overly-broad request. He was, however, urged by the parties to provide guidance about what types of records produced by faculty would ordinarily be in the university's custody or control.

Now custody or control is a very record specific question, so it's not surprising that Arbitrator Chodos really struggled with this task. His *dicta* is therefore not strong and the academic context for his decision is unique, but in the end, Arbitrator Chodos did make some oblique statements that suggest work e-mails not related to work duties would ordinarily be beyond the custody or control of an employer.

Now *Johnson and Bell Canada* turns on the specific language in PIPEDA and the University of Ottawa case is not particularly authoritative, but they are both very radical decisions in that they suggest an employer may not be in custody or control of stored information that is not work-related.

Wow! It's one thing to say you can't look at personal e-mails without legitimate reason, but it's rather shocking to suggest that you can't harvest and turn them over subject to a legal requirement.

The Information and Privacy Commissioner of Ontario recently addressed this very issue from the opposite perspective in an order called MO-2408, issued in April 2009. This was a case about whether several e-mails sent and received by a City of Ottawa solicitor in his personal capacity were subject to public access because they were under the custody or control of the City. The City's argument against application rested on the permission it had granted employees to use its computer system for incidental personal use. It also attempted to argue that its right of access to *all* e-mails under its computer use policy did not give it a strong enough interest in *personal e-mails* to bring them within its custody or control. The IPC disagreed, and issued a very solid award that may offend evolving expectations of privacy but is consistent with the traditional view on employer control of business systems.

Practical options for employers

So to summarize, the traditional view is still the prevailing view, but there are number of signs that this view will be challenged.

As I outline in my paper, this is because we use work computer systems differently than we did even 10 years ago. When we have access to our work systems 24 hours a day, and when we are given license to do very personal things on them, the expectation of privacy naturally rises.

In my view the response reflected in *Johnson and Bell Canada* and the University Ottawa decisions goes too far in responding to this rising expectation, but employers ought to expect to be held to a balancing of interests framework in the future.

For employers, this change does require a response. If you're unionized and you don't respond, you're going to run the risk of having evidence excluded in a discipline arbitration. If you're non-unionized, though information you collect will often go in as evidence despite an alleged privacy breach, you'll still run the risk of having to deal with privacy tort and constructive dismissal claims. So employers should do something now.

In my paper I outline the two potential responses. They are mutually exclusive options – which means you must commit to one or the other, but can't apply a mixed approach.

The first approach involves trying harder to achieve zero expectation of privacy despite permitting personal use – giving notice more often and clearer terms. This is an option, but I worry that employers choosing this option may run into difficulties associated with enforcing policy that doesn't fit with objective reality.

The second option is to abandon the effort at achieving no expectation of privacy and build privacy controls into policy.

- Set a protocol for routine audits that recognizes and respects a privacy interest.
- Set a threshold for investigations.
- Make and communicate a choice about the most invasive techniques like key logging.

My view is that you ought to be very free to set policy that protects management interests while protecting yourself by acknowledging competing employee interests.

Thank you!

Dan Michaluk, June 9, 2009