Employer access to employee e-mails in Canada

By Dan Michaluk, Hicks Morley[1]

It wasn't too long ago that a work computer was a thing used for work alone. Desktop computers stayed in the office, cellular telephones were used for telephone calls and employees engaged in limited personal use of business computer systems. In this context, employees who attempted to assert a personal privacy interest after being caught engaging in computer misuse were met with rebuke. Canadian arbitrators and courts recognized that employers owned and controlled their systems and consistently adopted a "no expectation of privacy" approach.

The rise of mobile computing has changed business computing, and has arguably changed employers' expectations about personal use of business computer systems. To suggest that an office worker should wait to get home before e-mailing a spouse would earn a proponent scoffs if that same officer worker is expected to be reachable by work e-mail after hours. The latter, however, now represents the new norm for business systems use. Has this change made a difference? Given the change, what should employers do to protect their ability to access and use information on their systems?

This is my attempt at addressing these questions. I briefly (1) identify the specific interests an employer has in accessing information stored on its computer systems, (2) identify the bases for claims by employees that information stored on business computer systems is "private," (3) describe the "no expectation of privacy" approach adopted by Canadian labour arbitrators and courts, (4) identify cases that might demonstrate this approach is changing, and (5) discuss what the jurisprudence should mean to employers. I argue that there are signs that the traditional "no expectation of privacy" approach is waning, leaving employers with a choice between giving clearer notice to employees or, alternatively, implementing purpose-based controls to protect employee privacy.

---

[1] I am a lawyer at Hicks Morley and provide our management clients with information and privacy advocacy and advice and employment and human rights advocacy and advice. I'd like to thank John Gregory, Paul Broad and Nadine Zacks for their valued input. Please note that the views reflected in this paper are my own and not the views of Hicks Morley or its clients.

Why employers need access

Let's start by examining why employers need access to information stored on their computer systems. Consider the following five purpose statements that might be part of a computer use policy:

> We access information stored on our computer system:
>
> (a) To engage in technical maintenance, repair and management
>
> (b) To meet a legal requirement to produce records
>
> (c) To ensure continuity of business processes
>
> (d) To improve our business processes
>
> (e) To maintain control over our business processes, including preventing misconduct and ensuring compliance with the law

I intend these broad statements to capture the full range of legitimate reasons that an employer might need to access stored data and information.

Purposes "a" and "b" are self-explanatory. Although they are not the most controversial purposes, we can expect disputes about non-party privacy and mandatory production to become more prevalent. *Datatreasury v. Royal Bank of Canada*,[2] for example, dealt with a group of banks with concerns about producing customer information to an opposing party with plans to process it outside of Canada. And in the criminal context, the British Columbia Court of Appeal recently dismissed[3] an argument that various non-parties whose private communications had been intercepted by the RCMP should be given notice of a motion brought to compel the production of the intercepts. The British Columbia Court of Appeal expressly raised the conflict between protecting non-party privacy and securing the "just, speedy and inexpensive

[2] 205 FC 955 (CanLII).

[3] See *British Columbia (Director of Civil Forfeiture) v. Angel Acres Recreation and Festival Property Ltd.*, 2009 BCCA 124 (CanLII).

determination of every proceeding on its merits."[4] For employers faced with the cost of reviewing large volumes of unstructured electronically stored information (mostly e-mail) in order to meet a production requirement, the recognition of an employee privacy interest in that information is cause for concern.

Purposes "c," "d" and "e" are broader in scope and embody the following idea: if most businesses' processes are conducted electronically and recorded in electronically stored information, then process continuity, control and improvement can be established by using that electronically stored information. Ensuring continuity can be about something as simple as providing one employee's correspondence on a work project to another so that work can be completed. Control and improvement can either be about improving process quality and integrity or about reducing or eliminating misconduct. Process control and improvement can be achieved through (reactive) investigations or (proactive) audits or surveillance. For example, routinely auditing departing employees' computer use to assess whether they have misappropriated confidential information is a type of control.

The basis for employee privacy claims

Few would quarrel with the legitimacy of the purposes listed above, but privacy advocates raise their impact on employee privacy. They have argued that there is a privacy interest in information of a private nature that employees chose to place on their employers' systems – e.g. personal e-mails. Former Privacy Commissioner George Radwanski, for example, has said :

> "…just the potential for problems doesn't justify wholesale monitoring. Most of us would agree that an employer would have no business randomly or routinely pawing through the desk drawers of employees, and examining whatever happens to be there. What makes the contents of a computer any different?"[5]

[4] *Ibid.*, at para. 18.

[5] G. Radwanski, "The New Era of Privacy Protection," (Toronto: Treasury Management Association of Canada, 19th Annual Finance and Treasury Management Conference, October 2001) at 8.

They may also argue that there is a privacy interest in electronically stored information that reveals how employees work – e.g. websites visited, time spent on certain websites and so on. This latter type of information, of course, is collected automatically in the course of work.[6]

The prevailing approach in Canada

The striking feature of the prevailing Canadian jurisprudence is that it does not illustrate an attempt to reconcile the employer and employee interests described above. Most labour arbitrators and courts have said that employees have no expectation of privacy in private information recorded on an employer's system and have not required employers to justify access to such information as being necessary and legitimate.

The prevailing view was well-expressed by Arbitrator Peltz in *Naylor Publications*,[7] a case in which she rejected a union argument that offensive e-mails sent by the grievor to her spouse and several friends were "private" and therefore less culpable. She said:

> Like it or not, the technology creates real limitations on privacy and security of an e-mail message. In *Camosun College* and *Telus Mobility*, cited above, arbitrators took note of the potential for uncontrolled dissemination. The Union in the present case analogized to writing a letter for venting purposes and leaving it at your desk, or taking your troubles home to a spouse or friend. However, e-mail users ought to know that when they put out sensitive or offensive material into cyberspace, they can never be sure where the message will ultimately come to rest. Today, if a person needs or desires a private conversation, she must carefully consider how to ensure true privacy. Expressing deeply personal thoughts over an employer's computer system is surely not a good choice. At times,

---

[6] Employers have generally failed in arguing that video camera installation does not affect employee privacy because employees are still subject to human supervision: see e.g. *PIPEDA Case Summary #279*, [2004] C.P.CS. F. No. 24 (QL). Computer monitoring is different, in that behavioural information is collected automatically; the privacy issue is about an employer's right of use. For more on workplace surveillance, see D. Michaluk, "Walking the Tightrope – Recent Developments in Employee Surveillance" online: Hicks Morley <http://www.hicksmorley.com/images/SurveilancePaper_May07_DJM.pdf>.

[7] *Naylor Publications Co. (Canada) and Media Union of Manitoba, Local 191 (Re)*, [2003] M.G.A.D. No. 21 (Peltz) (QL).

> notwithstanding the inconvenience, it may be preferable to wait until there is an opportunity for face to face communication.[8]

Ms. Peltz's finding that the grievor lacked a reasonable expectation of privacy is based on the nature of the technology at issue and not any specific policy that warned the grievor about the monitoring. Other leading Canadian cases also reflect this permissive view. [9] In *Camosun College*, for example, Arbitrator Germaine noted that employer control over e-mails is one factor that ought to limit employee privacy claims, and that the potential for wide dissemination of e-mails is another.[10] And in the only reported Canadian court case in which a court has considered a request to suppress e-mail evidence based on a privacy claim, the Court stated, "Where there is no e-mail policy in place, an employee has no reasonable expectation of privacy in relation to e-mails received and sent in the workplace on an employer's time and equipment."[11]

Whether this is the right approach may be debated, but it does appear that Canadian courts and arbitrators have seized upon the key difference between monitoring employee computer use and implementing other forms of employee monitoring like video surveillance and GPS monitoring: the collection of "private" information is incidental to a legitimate collection of work-related information and the information is stored on a medium that employers have many proper reasons to access. They also appear to have accepted that any negative affect on employee dignity that is caused by this incidental collection is reasonable in the modern Canadian workplace.[12]

---

[8] *Ibid*., at para. 140.

[9] *Insurance Corporation of British Columbia (Re)* (27 January 1993, unreported, Weiler), *International Association of Bridge, Local Union No. 97 and Structural and Ornamental Ironworkers and Office Technical Employees Union, Local 15 (Re)*, [1997] B.C.C.A.A.A. No. 630 (Bruce) (QL) and *Camosun College and Canadian Union of Public Employees, Local 2081 (Re)*, [1999] B.C.C.A.A.A. No. 490 (Germaine) (QL).

[10] *Camosun College*, *ibid*., at para 21. For similar reasoning, see *Briar and Treasury Board (Solicitor General Canada – Correction Service) (Re)*, [2003] C.P.S.S.R.B. No. 3 at para. 59 (Taylor) (QL).

[11] *Milsom v. Corporate Computers Inc.*, [2003] A.J. No. 516 at para. 41 (Atla. Q.B.) (QL). See also *Consumers Gas and Communications, Energy and Paperworkers Union (Re)*, [1999] O.L.A.A. No. 649 at para. 71 (Kirkwood) (QL).

[12] The reasonable expectation of privacy concept is meant to establish acceptable norms: *R. v. Tessling*, [2004] 3 S.C.R. 432.

Note that the permissive analysis described above does not apply in circumstances in which employees enjoy statutory privacy rights.[13] The "expectation of privacy" concept is featured in some Canadian privacy statutes as a means of establishing a flexible standard of protection,[14] but Canadian privacy statutes generally protect all "personal information." And while information about work and work life is not personal information,[15] information that reveals intimate things about how one goes about work has been held to be personal information.[16] Canadian information and privacy commissioners have therefore demanded justification from employers for accessing employee personal information stored on their computer systems. In 2005, for example, the Alberta Information and Privacy Commissioner held that an employer 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.[17] More recently, the Office of the Information and Privacy Commissioner for British Columbia held that the University of British Columbia violated the British Columbia *Freedom of Information and Protection of Privacy Act* by conducting a "reasonable grounds investigation" of an employee's personal computer use by using technology that captured screen images.[18]

There is some evidence of change

The prevailing view on employee privacy is well established by a series of cases leading up to 2003.[19] After 2003, there was little activity until Arbitrator Ponak's 2007 decision in *Lethbridge*

---

[13] For a description of the various sources of employee privacy rights in Canada See D. Michaluk, "The Limits of The Application Game – Why Employee Privacy Matters" online: Hicks Morley <http://www.hicks.com/images/pdf/2008/TheApplicationGameEmployeePrivacyRights.pdf>.

[14] See e.g. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1, Principle 4.3.5. and *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, s. 43.

[15] *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 at para. 94.

[16] See e.g. *Order M-720*, [1996] O.I.P.C. No. 84 (QL) (information about performance of job duties challenged as inadequate is personal information), *Order P-1124*, [1996] O.I.P.C. No. 65 (QL) (information about attendance at a training course is personal information) and *Order P-1384*, [1997] O.I.P.C. No. 112 (QL) (records of overtime hours worked contain personal information).

[17] *Parkland Regional Library (Re)*, [2005] A.I.P.C.D. No. 23 (QL).

[18] *University of British Columbia (Re)*, 2007 CanLII 42407 (BC I.P.C.).

[19] In addition to the cases cited above, see *Owens-Corning Canada Inc. and Communications, Energy and Paperworkers Union of Canada, Local 728 (Re)*, [2002] A.G.A.A. No. 74 at para. 74 (Price) (QL) (though the arbitrator does note that the employer put employees on notice through policy), *407 ETR Concession Co. and C.A.W., Local 414 (Re)*, 2003 CLB 12468 (Randall) and *British Columbia Ferry Services Inc. and British Columbia Ferry and Marine Workers' Union (Re)*, [2003] B.C.C.A.A.A. No. 383 at para. 116 (Blasina) (QL). But see *CT and*

College, in which he held that e-mails that an employee had sent and received through his Microsoft Hotmail account (produced from a forensic analysis of his work computer) were admissible into evidence.[20]

The college retained a forensic IT specialist to conduct the analysis after terminating the grievor (a college professor) for engaging in inappropriate relationships with at least three students. When it conducted the search, the college already had received a complaint from one student, had found corroborative evidence in the grievor's e-mails sent and received on its own e-mail system (the admissibility of which was not challenged) and had received a corroborative report from another individual. The college claimed that conducting word searches by the names of the grievor's former students was the most effective way of determining whether he had engaged in additional inappropriate relationships.

Arbitrator Ponak admitted the evidence on a rather unremarkable application of the classic "balancing of interests" tests applied by Canadian labour arbitrators, but the application of the test itself is very significant. At the outset, however, Mr. Ponak commented on the expectation of privacy the grievor had in information sent and received through a web-based e-mail account but on a computer owned by the college:

> We start from the premise that employees have some expectation of privacy in the receipt and transmission of emails from an internet provider that is not their employer's (Weir; McIsaac et al.). Thus, it was reasonable for the Grievor to believe that emails on his hotmail account were beyond the reach of the College. In the Board's view, if the Grievor's hotmail was exclusively located on the Grievor's own private computer it would be inadmissible without the Grievor's consent. The Grievor, however, used the computer provided to him from the College for some of his hotmail email, changing the circumstances. The College computer was intended primarily for College work and it belongs to the College, factors which give the College some rights to access that computer. The Grievor's

---

Bank of Montreal (Re), [2005] C.L.A.D. No. 74 (Newman) (where the adjudicator applies a balancing of interests approach based on the employer's policy, which invited such balancing).

[20] *Lethbridge College and Lethbridge College Faculty Assn. (Bird Grievance) (Re)*, [2007] A.G.A.A. No. 67 (Ponak) (QL).

> right to privacy for the contents of the College computer is not absolute. At the same time, recognizing that the policy against using the College computer for non-College matters has not been rigidly enforced (if enforced at all), the Employer's access to the contents of the computers it provides its employees is not unfettered either. The Employer's right to search the contents of an employee's computer must be balanced against an employee's expectation of privacy and is subject to a test of reasonableness.[21]

This is hardly a forceful argument for change, but might suggest that employers who allow personal use must reckon with an employee privacy interest in information stored on their business systems.

The next case that shows a potential indication of change is *Johnson v. Bell Canada*, in which the Federal Court held that the *Personal Information Protection and Electronic Documents Act* does not give employees of federally-regulated employers a right of access to e-mails concerning them that are sent between co-workers in their personal capacity and stored on the employers e-mail system.[22]

The applicant, a former employee, filed a request for all e-mails "concerning" him. At the Federal Court, the primary issue in dispute was about whether "personal" (i.e. non-work related) e-mails about the applicant were subject to the right of access in PIPEDA.

PIPEDA does not include a traditional "custody or control" standard for access. Though the access principle refers to personal information "held" by an organization, the existence of a right of access turns on whether a request is for personal information that is collected, used or disclosed by an employer "in connection with the operation of a federal work or undertaking."[23] PIPEDA also expressly excludes information that an individual collects, uses or discloses for exclusively "personal or domestic purposes."[24]

---

[21] *Ibid*., at para. 31.
[22] 2008 FC 1086 (CanLII).
[23] PIPEDA, *supra* note 14, s. 4(1)(b).
[24] *Ibid*., s. 4(2)(b).

Mr. Justice Russel Zinn held that the personal e-mails sought were not collected in connection with the operation of a federal work or undertaking and were also excluded as e-mails collected, used and disclosed for personal or domestic purposes. The core of his reasoning is captured in the following excerpt:

> First, in my view, the information is not being "handled" by Bell Canada. Like the bycatch of the cod fisherman, personal e-mail is the bycatch of the commercially valuable information that is being handled by Bell Canada. Secondly, to be information collected in connection with the operation of the business, requires that there be a business purpose for the information. There is none with respect to personal e-mails. In fact, from the viewpoint of organizations like Bell Canada, personal e-mails are refuse that take up valuable space and time. It is for this reason, among others, that organizations discourage or limit employee utilization of their computer systems for personal reasons.[25]

Zinn J. also appears to have been influenced by the rights of the co-workers who sent and received the impugned e-mails and their interest in what has otherwise been called "mixed personal information." He suggests that these individuals would be deprived of the personal and domestic purposes exclusion if PIPEDA was held to apply to their e-mails, hence framing the exclusion as a form of right.

Like Mr. Ponak's *Lethbridge College* decision, Zinn J.'s decision in *Johnson v. Bell Canada* does not advocate for change. He also was not making a decision about Bell Canada employees' expectation of privacy nor did he consider whether Bell had reserved a strong right of control over "personal" e-mails in its corporate computer use policy.[26] *Johnson v. Bell Canada* is worth noting, however, for how different an approach the Court takes than that articulated by Arbitrator

---

[25] *Johnson v. Bell*, *supra*, para. 35.

[26] Notably, several weeks after Zinn J.'s judgement was released, the Federal Court issued a judgement in which it dismissed a PIPEDA application that alleged an executive had unlawfully collected personal information by sending an e-mail to members of his firm to inquire about the applicant: *Waxer v. J.J. Barnicke Limited*, 2009 FC 168 (CanLII). Though a jurisdictional objection does not appear to have been made, given the e-mail sent by the executive was arguably "personal" (he sent it because the complainant was allegedly harassing his sister) it might have been outside the scope of the Act on Zinn J.'s analysis.

Peltz five years earlier in *Naylor Publications*. The "by-catch" simile employed by Zinn J. shows that he saw Bell Canada as having a limited interest its employee's non work-related e-mails.

Conclusion – Two responses to uncertainty

The tension demonstrated in the above noted cases is likely to take some time to be resolved.[27] The uncertainly alone, however, is good reason for employers to re-think their approach to managing employee computer use. It is less clear what to do.

One approach is to give employees clearer notice.[28] If more permissive rules on personal use are the basis for changed expectations, employers may work harder to ensure employees are making informed choices about the sacrifice of privacy associated with personal use. Under this approach, computer use policies need not change much at all; the solution lies more in their implementation and, more specifically, in communication measures such as periodic acknowledgements, log-in notices and the like.

While the "clearer notice" approach is appealing in its simplicity, it is also somewhat risky given the relationship between permissive personal use rules and acceptable workplace privacy norms. For one, managers sensitive to the type of "private" content generated by personal use might resist and send inconsistent messages about policy. This practical risk is well-illustrated by a much-discussed case in which a California court held that a public employer violated several employees' privacy rights by auditing their text messages.[29] This outcome was based on a finding that a supervisor had implemented an informal process of allowing employees to pay for "overage" charges as a means of avoiding text message audits.[30] But even if managers can be suitably controlled, a court or labour arbitrator may still reject a policy that permits personal use

---

[27] Shortly before this paper was completed, the Ontario Superior Court of Justice issued *R. v. Cole*, 2009 CanLII 20699 (ON S.C.). The Court adopts the position traditionally adopted by Canadian labour arbitrators and Courts in finding that a teacher had no expectation of privacy in a laptop issued to him by his school board, but does stress the extraordinary facts on which its decision was based, including the fact that the board had assigned the teacher the responsibility for supervising system use by students.

[28] Some might argue that clear notice is required to protect against potential criminal liability for breach of the Criminal Code wiretap prohibitions, though at least one court has held that one does not "intercept" a private communication (a prerequisite for criminal liability) by searching stored communications: see *R. v. Giles*, [2007] B.C.J. No. 2918 at para. 7 (S.C.) (QL).

[29] *Quon v. Arch Wireless*, 2008 WL 2440559, rehearing en banc denied, 9th Cir., 27 January 2009. Note Arbitrator Ponak's comment about condonement in *Lethbridge College*, *supra* note 21.

[30] *Ibid*. at 7021, 7022.

and relies strictly on notice. Personal use and zero privacy don't sit well together, so a clear "no privacy" notice might not always convince an adjudicator that an expectation of privacy is unreasonable.

The more cautious employer will implement a new form of computer use policy that reserves the right to meet all legitimate purposes identified above, but also includes privacy controls to ensure that use of more sensitive types of information on its system (e.g. the content of e-mails and information revealing of keystrokes) is based on reasonable necessity.[31] I am not suggesting that management fetter its rights in a manner that sacrifices management interests. If an employer, for example, feels that investigations based on "reasonable suspicion" instead of "reasonable grounds" are justified, then it should promulgate policy that contemplates investigations based on a reasonable suspicion. Likewise, if an employer feels that routine and/or random audits are justified, it should promulgate a policy that contemplates routine and/or random audits. In some circumstances – where employment privacy legislation applies for example – proof of business justification might be required, but an employer faced with a policy challenge should be well-positioned to argue that the chosen approach is measured and moderate compared to the traditional type of policy that has met with arbitral and court approval.

[31] American e-discovery commentator Ralph Losey argues that senior executives should be wary of facing the consequences of their own aggressive computer use policies in R. Losey, "IT Workers Read Your Personal Email and U.S. Law is Generally OK with That." online: e-Discovery Team <http://ralphlosey.wordpress.com/2009/02/09/it-workers-read-your-personal-email-and-us-law-is-generally-ok-with-that/>.