

# Monitoring employee e-mail: a privacy primer

Brian Bowman  
Partner, Pitblado LLP

Andrew Buck  
Articling Student-at-Law, Pitblado LLP

## Introduction

Privacy law does not offer a black and white answer to the legal issues that are raised by e-mail monitoring practices. Instead, and like most other privacy law issues, the standard of "reasonableness" rules the day.<sup>1</sup>

## Defining 'reasonable'

The [Personal Information Protection and Electronic Documents Act](#) ("**PIPEDA**") governs federally regulated private sector organizations, as well as businesses that collect, use or disclose personal information in the course of commercial activities.<sup>2</sup> Business e-mail addresses (as well as the contents contained therein) have been held to fall within the meaning of "personal information", as that term is defined in PIPEDA.<sup>3</sup>

According to the Office of the Privacy Commissioner's ("**OPC**") 2001-2002 Annual Report to Parliament, then-Privacy Commissioner George Radwanski stated that he "accept[ed] that there may be occasions that would justify an employer's decision to review an employee's Internet network account and then use that information in a disciplinary process."<sup>4</sup>

In what situations is e-mail monitoring justified? And what tests can we use to answer this question? Neither the courts nor the OPC have given us a definitive answer to date.

## The "video surveillance test"

This four-point test was initially set out by the OPC to evaluate the reasonableness of employee video surveillance.<sup>5</sup> The employer must be able to show the surveillance was necessary to meet a specific need; the surveillance was likely to be effective in meeting the need; the loss of

---

<sup>1</sup> This standard is enshrined in s. 5(3) of the [Personal Information Protection and Electronic Documents Act](#), S.C. 2000, c. 5, which states that organizations "may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

<sup>2</sup> Depending on its location, an employer may be subject to "substantially similar" provincial privacy laws rather than PIPEDA. Currently, the provinces of [Quebec](#), [Ontario](#) (for personal health information), [Alberta](#) and [British Columbia](#) have such laws.

<sup>3</sup> Office of the Privacy Commissioner of Canada, "Interpretations (Personal Information)", online: <[http://www.priv.gc.ca/leg\\_c/interpretations\\_02\\_e.cfm](http://www.priv.gc.ca/leg_c/interpretations_02_e.cfm)>.

<sup>4</sup> *Annual Report to Parliament, 2001-2002*, online: <[http://www.priv.gc.ca/information/ar/02\\_04\\_10\\_e.pdf](http://www.priv.gc.ca/information/ar/02_04_10_e.pdf)> at 29. The OPC's comments about discipline allude to a number of issues that arise vis-à-vis e-mail monitoring and labour law. These issues are outside the scope of this article, but counsel should consider the labour and employment law aspects of e-mail monitoring in relation to privacy law implications.

<sup>5</sup> See [PIPEDA Case Summary #2003-114](#), "Employee objects to company's use of digital video surveillance cameras", later adopted by the Federal Court in [Eastmond v. Canadian Pacific Railway](#), 2004 FC 852.

privacy was proportional to the benefit gained; and no reasonable, less privacy-invasive ways to meet the need were available.

#### The "reasonable expectation of privacy test"

This test imported American case law and focused on whether an employee has a reasonable expectation of privacy in the workplace. This test was often favoured by employers since it could often be said that employees had a low expectation of privacy since they were at work and the employer owned the computer.<sup>6</sup>

The OPC has cast doubt on the continuing validity of this test in Canada, noting that "People expect to have some privacy at work, even if they are on their employer's premises and using the employer's equipment."<sup>7</sup>

#### The "objective reasonableness test"

This test looks broadly at the circumstances of each case to determine whether a reasonable person would have found monitoring to be justified in the circumstances. Relevant factors under this test have included: the nature of the monitoring; the employee's awareness of the monitoring; whether the monitored activity is classified as "business" or "private"; and the egregiousness of the monitoring.<sup>8</sup>

As stated above, courts and the OPC have yet to definitively endorse any of these tests. Consequently, it is advisable to consider them in aggregate, focusing on factors that are common to all (or at least some) of these tests.

### **Practical points for employers**

The cornerstone of federal privacy law is the requirement of informed consent before personal information can be collected, used or disclosed. PIPEDA contains narrowly defined exceptions where consent is not required before personal information is collected, the most common of which applies when an employer can prove it has reason to believe a law (or an "agreement", such as an employment contract) is being broken.<sup>9</sup> Since these exemptions are strictly construed, employers will usually be required to obtain consent from employees before e-mail monitoring practices are implemented.

Further, Privacy Commissioner findings consistently hold that — in the absence of an exemption to obtaining consent — an employer's desire to covertly monitor all employee e-mail as a matter of course simply does not justify the invasion of privacy covert monitoring represents.<sup>10</sup>

### **Collect information 'pursuant to a clearly stated purpose'**

---

<sup>6</sup> Melanie Bueckert, *The Law of Employee Monitoring in Canada* (Markham, Ont: LexisNexis Canada, 2009) at 157.

<sup>7</sup> OPC, "Fact Sheet: Privacy in the Workplace", online: <[http://www.priv.gc.ca/fs-fi/02\\_05\\_d\\_17\\_e.cfm](http://www.priv.gc.ca/fs-fi/02_05_d_17_e.cfm)>.

<sup>8</sup> *Ibid.*, citing Kris Klein & Vivian Gates, *Privacy in Employment: Control of Personal Information in the Workplace* (Toronto: Thomson Carswell, 2005) at 57.

<sup>9</sup> Ian Turnbull et. al, *Privacy in the Workplace* (Toronto: CCH Canadian Limited, 2004) at 35. See also s. 7(1)(b) of PIPEDA.

<sup>10</sup> *Ibid.* at 31 and 35: "At the very least, employees have the right to know that such monitoring is possible, or probable." See also *The Law of Employee Monitoring in Canada, supra*, at 159.

Case law and findings released by federal and provincial Privacy Commissioners hold that an employer must be able to point to specific purposes to be addressed by e-mail monitoring: it is not enough to conduct employee surveillance "just because"; no employer has an inherent right to monitor its employees in the absence of a pressing reason for doing so.<sup>11</sup> Further, employers are typically required to show that e-mail monitoring actually furthers these purposes.

There are legitimate reasons why computer use policies that include e-mail monitoring are desirable. It is fair to expect employees will further company objectives while they are at work, and excessive personal e-mails on company time can become an issue deserving of attention. Employers may also be rightfully concerned about security and the protection of valuable proprietary information. Defending corporate reputations is yet another reason why employers might want to monitor employee e-mails.<sup>12</sup>

There are many other valid reasons for monitoring employee e-mails. What is critical from an advising counsel's perspective, however, is the need to identify and document the purposes why monitoring is required.

### **Proportionality**

The benefits of e-mail monitoring must be proportional to the loss of privacy that results. Applied to e-mail monitoring, this requirement mandates employers to exhaust less privacy-invasive means of accomplishing the same purposes before resorting to e-mail monitoring. Such less intrusive measures could include: blocking websites; warning employees about prohibited computer usage; and frequently deleting the contents of employee computers to discourage them from storing personal files on corporate computer systems.<sup>13</sup> From a simple cost-benefit perspective, these less intrusive measures are also beneficial because they are far less time consuming than active, non-selective e-mail monitoring.

### **Implement a computer use policy (and keep it updated)**

At base, computer use policy should outline "when and how employee monitoring may occur".<sup>14</sup> The Alberta Office of the Information and Privacy Commissioner suggests a computer use policy should explain what personal information will be collected, used and disclosed through e-mail monitoring, and whether employees will be subject to continuous monitoring. The policy should also tell employees who will have access to their personal information and name the organization's designated privacy officer.<sup>15</sup>

It is advisable to ensure the policy remains at the forefront of employees' minds. The best computer use policy in the world will not help your client if none of its employees are aware it exists.

---

<sup>11</sup> [Colwell v. Cornerstone Properties Inc.](#), 2008 CanLII 66139 (ON S.C.).

<sup>12</sup> *Law of Privacy in Canada*, *supra*, at 2-82.4.

<sup>13</sup> *The Law of Employee Monitoring in Canada*, *supra*, at 159 and 160.

<sup>14</sup> *Ibid.* at 158.

<sup>15</sup> Office of the Information and Privacy Commissioner of Alberta, "Can a company monitor or trace computer email to and from an employee, or monitor or track phone traffic to and from an employee without their knowledge?", online: <<http://www.oipc.ab.ca/pages/PIPA/QAs.aspx?id=241>>.

## **The bottom line on e-mail monitoring in the workplace**

The key to a defensible system of e-mail monitoring is the creation of a comprehensive and communicated computer use policy. Such a policy can go a long way toward meeting the "reasonableness" standard imposed on employers who wish to collect, use or disclose their employees' personal information. Not only can it set out the way in which e-mail monitoring will be conducted, it can also be used to inform employees, thereby ensuring the employer's obligations of notification and consent are met.

*[Brian Bowman](http://www.brianbowman.ca) is a partner with the Winnipeg law firm Pitblado LLP. He is past Chair of the CBA's National Privacy and Access Law Section and writes a professional blog at [www.brianbowman.ca](http://www.brianbowman.ca).*

***Andrew Buck** is an articling-student-at-law with Pitblado LLP and the recent recipient of the University Gold Medal Law award for highest standing in his graduating class at the University of Manitoba Faculty of Law.*