CARTERS.ca

CHARITY LAW BULLETIN NO. 160

Carters Professional Corporation / Société professionnelle Carters
Barristers, Solicitors & Trade-mark Agents / Avocats et agents de marques de commerce

MARCH 26, 2009
Editor: Terrance S. Carter

MONITORING EMPLOYEE COMPUTER USE RAISES PRIVACY CONCERNS

By U. Shen Goh, LL.B., LL.M. & Trade-mark Agent

A. INTRODUCTION

Back in the days when employees spent time at the water fountain socializing with colleagues while neglecting work, it was easy for management to see and address the problem immediately. These days, however, if employees spend time on the computer surfing the internet or sending personal emails while neglecting work, it is difficult for management to ascertain and handle the problems in a timely fashion. While the answer may appear simple enough (*e.g.,* monitor the computers), the question is how to do so in a respectful and legal manner.

There is a delicate balance between an employee's expectation of privacy and an employer's expectation of accountability. This balance becomes even more challenging for charities and non-profit organizations, especially churches and other religious organizations that may hold their employees to a higher moral and ethical standard than is expected in the rest of society. Where this balance should lie and how it should be implemented is the focus of this *Charity Law Bulletin*.

B. PRIVACY: CAN EMPLOYERS MONITOR COMPUTERS?

The employee's expectation of privacy is justified and finds support in privacy law. With respect to the public sector (*e.g.*, government institutions), the applicable privacy legislation would generally be the federal *Privacy Act*, the provincial *Freedom of Information and Protection of Privacy Act,* and, in some cases, the *Municipal Freedom of Information and Protection of Privacy Act*. With respect to the private sector (*e.g.*, charities and

non-profit organizations), the applicable privacy legislation would generally be the federal *Personal Information Protection and Electronic Documents Act,* as well as the provincial *Personal Information Protection Act*. Which privacy legislation actually applies in a specific situation, and in a particular province, needs to be reviewed carefully on a case-by-case basis, as federal privacy legislation may not apply in all situations (*e.g.*, provincial employees) and provincial privacy legislation may not exist in all provinces (*e.g.*, Ontario has the *Personal Health Information Protection Act* instead).

For the purpose of this *Charity Law Bulletin*, we will focus on the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") to address the privacy concerns that are raised when charities and non-profit organizations monitor their employees' computers. It is recognized that PIPEDA will likely apply only where the charities and non-profit organizations (1) engage in commercial activities, and (2) are federal employers. However, this bulletin focuses on PIPEDA because (1) charities and non-profit organizations are engaging increasingly in commercial activities, (2) provincial privacy legislation is generally substantially similar to PIPEDA, and (3) in cases where no privacy legislation applies, charities and non-profit organizations should still voluntarily adhere to the underlying privacy principles of PIPEDA, as this is in keeping with the reasonable expectation of the employees that the charities and non-profit organizations they work for will recognize their right to privacy as an essential issue.

For example, section 3 of PIPEDA sets out the underlying privacy principle to be considered regarding the question of whether employers can monitor computers:

- Section 3 of PIPEDA:

  3 – Purpose
  The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

As such, PIPEDA suggests that the expectation of privacy must be balanced with the need to collect personal information and, therefore, the employee's expectation of privacy is not unequivocal. In this regard, the legislation makes it clear that personal information may be collected under reasonable circumstances. For example, section 5(3) of PIPEDA and section 4.4 of Schedule I of PIPEDA state:

- Section 5(3) of PIPEDA:

  5(3) – Protection of Personal Information
  An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

- Section 4.4 of Schedule I of PIPEDA:

  4.4 Principle 4 - Limiting Collection
  The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
  4.4.1
  Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).
  4.4.2
  The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.
  4.4.3
  This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

The challenge for employers is showing that they meet the test of reasonableness implied by the above sections of PIPEDA. The courts have provided some guidelines in this regard, stating that employers can monitor computers if it is done in a reasonable manner with regards to the following:

1. <u>The Notice/Warning Given To the Employee:</u>

   Examples of a reasonable notice/warning would be a computer use policy outlining terms of use and monitoring, a sign on the computer warning of monitoring, or a computer pop-up when employees log onto a computer reminding them that their use is being monitored. See *Re Treasury Board (Solicitor General Canada – Correction Service) and Briar*, [2003] C.P.S.S.R.B. No. 3, 116 L.A.C. (4th) 418. Having said that, no notice/warning is required where the employee's computer use is unprofessional, offensive or illegal (*e.g.,* racism or sexual harassment); where the employee's computer use is not private in that it is publicly available (*e.g.*, chat group); or where common sense should have made it self-evident to any employee that the computer use was inappropriate (*e.g.*, pornography). This will need to be determined on a case-by-case basis, depending on the specific facts of the situation.

2. The Purpose/Reason for Monitoring:

Examples of a reasonable purpose/reason would be ensuring that the employee is fulfilling his/her work responsibilities or protecting intellectual property and confidential information. However, monitoring how the employee is spending every minute at work would likely be unjustifiable, as there is jurisprudence to suggest that it is reasonable for employees to use computers for personal purposes (on a limited basis) in the same way as they can use telephones. See *Liberty Smelting Works (1962) Ltd. C. Syndicat international des travilleurs unis de l'automobile, de l'aéronautique, de l'astronautique et des instruments aratoires d'Amérique (T.V.A.) Local 1470*, (1972) 3 S.A.G. 1039 at 1044 and 1045, *Bell Canada c. Association canadienne des employés de téléphone*, [2000] R.J.D.T. 358.

3. The Scope/Intensity of Monitoring:

For example, if the purpose for monitoring an employee's computer is to ensure that an employee is not spending time on the computer surfing the internet or sending personal emails while neglecting work, then the monitoring would be limited to company time and it may not be necessary to monitor the employee during his/her personal lunch time. Or, if the purpose for monitoring an employee's computer is to ensure that an employee is not downloading illegal or offense materials from the internet or sending harassing/discriminating emails at work, then the monitoring would be limited to reviewing the website visited or the subject lines of the emails initially and it may not be necessary to review the content of every website visited or each email sent by the employee. See *Re Owens-Corning Canada Ltd. and UNITE HERE, Local 1350*, [2005] O.L.A.A. No. 442, 142 L.A.C. (4^{th}) 62.

C. EMPLOYMENT: CAN EMPLOYEES BE DISCIPLINED OR TERMINATED FOR COMPUTER USE?

Assuming that an employer's monitoring meets the test of reasonableness implied by the above sections of PIPEDA or the applicable privacy legislation, the question then becomes what the employer should do if the monitoring results in discovering that an employee's computer use is inappropriate.

Just as the employee's expectation of privacy is justified and finds support in privacy law, the employer's expectation of accountability, on the other hand, is equally justified and finds support in employment law. As such, employees can be disciplined or terminated with cause for inappropriate computer use. However, such

discipline or termination with cause must still be managed carefully and with consideration to the guidelines below, as employers can still be liable for wrongful dismissal in such situations.

1. The General Rule:

   Privacy law prevents employers from monitoring computers without consent, unless obtaining consent would have been inappropriate under the circumstances. This generally means that any monitoring without consent is an invasion of the employee's privacy and any subsequent termination is a wrongful dismissal of the employee.

2. The Exception:

   There is no invasion of privacy if the employer's monitoring meets the test of reasonableness implied by the above sections of PIPEDA and, furthermore, no wrongful dismissal with respect to any subsequent termination if the employee consented to discipline or termination with cause for inappropriate computer use. Evidence of such consent can be a computer/email/internet use agreement signed by the employee, a computer/email/internet use policy forming part of the employee's agreement/manual and brought to the attention of the employee, a notice on the computer to remind employees of such monitoring, etc. Having said that, the courts recognize that, even where there is no such evidence of consent, employees may still be disciplined or terminated with cause for inappropriate computer use under certain circumstances. This will need to be determined on a case-by-case basis, depending on the specific facts of the situation.

D. CONCLUSION

The delicate balance between an employee's expectation of privacy and an employer's expectation of accountability is best managed by ensuring that the employer's monitoring meets the test of reasonableness implied by the above sections of PIPEDA and obtaining the employee's consent to discipline or termination for inappropriate computer use. The latter is especially important for organizations that wish to hold their employees to a higher moral and ethical standard than is expected in the rest of society, as the organization's definition of "inappropriate computer use" may differ from society's definition.

Although the courts have recognized certain circumstances where it is reasonable to monitor computer use and discipline or terminate an employee subsequently for inappropriate computer use without any notice/warning to the employee, such circumstances are limited. A prudent and proactive employer should readily use agreements, policies, notices, etc., to ensure that its employees are aware of the limitations of the employee's expectation of privacy and of the employer's expectation of accountability. Not only can this assist in deterring possible claims of privacy breaches or wrongful dismissal should the employment relationship be terminated, it can also assist employers and employees in behaving appropriately so that the employment relationship need not be terminated and, instead, may continue to benefit both parties.

CARTERS.ca

Carters Professional Corporation / Société professionnelle Carters
Barristers, Solicitors & Trade-mark Agents / Avocats et agents de marques de commerce

Ottawa (613) 235-4774
Mississauga (905) 306-2791
Orangeville (519) 942-0001
Toll Free: 1-877-942-0001
www.charitylaw.ca