SHERRARD KUZZ LLP
Employment & Labour Lawyers

Newsblast: October 25, 2012

It *Isn't* Time to Throw Away Your Workplace Computer Policies!
…despite the Supreme Court of Canada's recent decision in *R. v. Cole*

As you may have heard, the Supreme Court of Canada recently released its decision in *R.* v. *Cole*, a case involving a school employee who accessed and stored child pornography on his work computer. The case is frequently described as one which has created a 'reasonable expectation of privacy' with respect to information an employee accesses or stores on his or her workplace computer. However, this description isn't a complete (or completely accurate) summary of the impact of the case, particularly on employers.

What many legal commentators have failed to highlight is that the crux of *R.* v. *Cole* wasn't about whether Cole's *employer* had the right to access the material contained on his computer; it was whether the *police* had the right to do so. The case focused on whether the police, having searched Cole's computer without a warrant, violated his right to be secure from an unreasonable search and seizure under the *Charter of Rights and Freedoms*.

Charter rights only come into play when an individual is affected by the actions of *government*. This *may* include an employer but only if the employer is considered *government* or a *government* actor. The vast majority of employers in Ontario are *not* government, and therefore *Charter* rights do not apply to their day to day relationships with their employees. **The Supreme Court's decision in *R.* v. *Cole* therefore does <u>not</u> directly affect the way non-governmental employers must deal with workplace computer systems and their employees' expectations of privacy.**

However, the story does not end here. We know from experience, adjudicators will often apply '*Charter* principles' even when the *Charter* itself does not apply. Accordingly, it is a good reminder for all employers to ensure they are using best practices when it comes to employee use of workplace computers and related technology. For instance:

- Ensure you have a written Policy in place to which employees have acknowledged in writing they are bound.

…2

- The Policy should include not only the fact the employer owns the equipment and related technology, but employees have no expectation of privacy in anything they view, access or store on the workplace system (including computer histories or cookies).

- Although your Policy may contemplate limited personal use of workplace technology, expressly prohibit employees from storing vital personal information on their company computer, such as banking information. This prohibition will undermine the potential for an employee to later claim he or she truly believed their information would be private, despite the Policy.

- Do not permit the use of passwords other than ones provided by the employer.

- Unless it is necessary for work purposes, employees should not be permitted to take a work computer home or in any way treat it as their 'personal' computer.

- The Policy should expressly contemplate 'spot checks' or 'periodic audits' of the system, including individual employee computers. But that's not enough – be sure your IT professional actually *performs* the audits, records having done so and you act promptly in respect of anything improper found (including requiring the removal of the information and potential discipline for the employee).

These are among the best ways to ensure an employee cannot persuasively argue he or she had a 'reasonable expectation of privacy' in respect of workplace technology, and attack an employer's ability to access files or act on information it may find.

If you would like assistance designing an effective internet and computer use policy for your organization please contact a member of the team at Sherrard Kuzz LLP.

SHERRARD KUZZ LLP
Employment & Labour Lawyers

250 Yonge Street, Suite 3300
Toronto, Ontario, Canada M5B 2L7
416.603.0700 Phone
416.603.6035 Fax
416.420.0738 24 Hour
www.sherrardkuzz.com