AML
ARMSTRONG MITCHELL
LAWYERS

# Employee Privacy in a Work Computer
# The Supreme Court Has Its Say

On October 19, the Supreme Court of Canada rendered its decision in *R. v. Cole*, a case with major implications regarding an employer's ability to monitor and access information stored on its employees' work devices. We are writing you today to outline what we see as the main practical lessons to take from this case.

The accused high school teacher was criminally charged with possession of child pornography after the school's IT department discovered nude photographs of a student in a hidden folder on his hard drive. The technician found the photos while performing system maintenance and notified the principal, who contacted the police. The main issue in the case was whether the police had the right to seize the pictures without a warrant and use them as a basis for criminal charges. Of greater concern to employers are the Court's comments on a side issue – the school's right to analyze the teacher's hard drive.

The Court found that the principal's search was allowed because the teacher's expectation of privacy in a work computer was diminished in the circumstances. The principal had a legal duty to maintain a safe school environment and therefore a reasonable power to seize and search a laptop issued by the school-board. It is also worth noting that the technician found the pictures while analyzing the hard drive for a legitimate purpose as opposed to searching without reasonable suspicion simply trying to catch the teacher doing something wrong.

The Court qualified its ruling by stating that workplace policies cannot completely remove an employee's privacy expectations. An employee has a reasonable expectation of privacy in a work computer where personal use is permitted and reasonably expected. All of the circumstances must be considered to define the employee's expectation of privacy. Furthermore, the employee never objected to the search by the school and its information technologists. Consequently, the Court reserved its detailed analysis of an employer's right to monitor computers it issues to its employees for a future case.

120, 4838 RICHARD ROAD SW
CALGARY, ALBERTA, T3E 6L1
T 403.233.0050 | F 403.266.1238
AMLLAWYERS.COM

Nonetheless, there are lessons to take away from this case. The most obvious one is that there is no substitute for a sound workplace policy on the use of technology, including reminding employees that their expectation of privacy is diminished with respect to workplace devices and the employer's network. As the Court stated, employees can reasonably expect some level of privacy. It is usually too difficult to prevent employees from engaging in some personal use of the employer's devices. More to the point, it is probably unwise to outright ban personal usage unless such a restriction can be enforced. Look at it the same way you would an employee's office telephone. An employee will probably use it on occasion for personal calls.

In the usual office setting, it is better for morale and more realistic from an enforcement standpoint to insist that personal use be limited and to inform employees that the system and network is monitored. Inform employees that they are expected to refrain from accessing content inappropriate for work, engaging in more than incidental personal use, or misusing company information or software.

Just having a policy is not enough, of course. It must be communicated to your employees. The traditional ways to do this are to send each employee the written policy or post it in a central place, physically or electronically. Some employers go one step further by having employees sign a document stating that they have read and understood the policy. An even better way is to remind your employees every time they log onto the network with a prompt, or "pop-up," referencing the policy and reinforcing that the employee is agreeing to its terms by signing in.

The Court's insistence that employees have some expectation of privacy in work devices places employer monitoring under scrutiny; however, a sound policy effectively communicated to employees gives the employer a leg up in the event such monitoring is challenged. If you have any questions about this issue, do not hesitate to contact our firm for advice.

William J. Armstrong, Q.C.
Direct: 403-260-6754
w.armstrong@amllawyers.com

Timothy D. Mitchell
Direct: 403-260-6751
t.mitchell@amllawyers.com