LAWSON LUNDELL LLP
www.lawsonlundell.com

April 29, 2011

Labour & Employment Law Bulletin

Company Computers and the Employee's Expectation of Privacy – Do your Employees have a Reasonable Expectation of Privacy over their Computer Data?

In *R. v. Cole,* 2011 ONCA 218 ["*Cole*"] a high school teacher obtained pornographic pictures of a grade 10 student via the school computer network. He was able to obtain the pictures because he was a network administrator with remote access to student computers. He stored copies of these pictures on a laptop that was provided to him by his employer. The employer's computer policy specifically permitted personal computer use and it did not generally address the employee's expectation of privacy over data stored on the school network.

One of the school's computer technicians discovered the pictures while scanning the computer remotely for viruses. The technician saved the digital pictures and screen shots on a disk and provided them to the school principal. Eventually, school board computer technicians copied temporary internet files from the laptop onto another disk. At the request of the principal, the teacher handed over the laptop but did not provide his password. The police were then informed, and the disk containing the pictures was provided to the police. The police searched the laptop and seized the disk containing temporary internet files without a warrant. The teacher was charged with possession of child pornography and unauthorized use of a computer.

On March 22, 2011, the Ontario Court of Appeal released a decision holding that the teacher had a reasonable expectation of privacy over the personal contents of the laptop hard drive. The reasonable expectation of privacy was, however, limited to the extent that the teacher expected the "technician could and would access the laptop as part of [the technician's] role in maintaining the technical integrity of the…information network". Consequently, it was ordered that only the information that was initially obtained by the technician was admissible. Information obtained by the police from the laptop and the disk containing temporary internet files was found to be inadmissible.

Although this decision is primarily concerned with whether the police obtained the evidence in a constitutionally acceptable manner, the case has important implications for employers:

1. Where employees are provided with exclusive access to a computer and personal use is permitted, a reasonable expectation of privacy may arise.

2. An employee's reasonable expectation of privacy over data stored on an employer's computer is limited to the extent that technicians would be expected to access the information in maintaining the technical integrity of the network.

3. The employer's computer policy will significantly impact whether an employee has a reasonable expectation of privacy over the data stored on computers provided by the employer.

In *Cole*, information initially found by the employer's computer technician was found to be admissible in a criminal trial. This does not, however, mean that computer network administrators can simply access and store any employee data they find in the course of their duties. Privacy legislation may limit the collection, use, and disclosure of information that employees store on their employers computers.

The limits set by privacy legislation upon monitoring employee computer use were carefully examined in a 2007 adjudication under British Columbia's *Freedom of Information and Protection of Privacy Act* ("*FIPPA*"). In that case, an employee at the University of British Columbia ("UBC") was terminated in part due to his internet use at work.

UBC monitored the employee's internet use by examining computer log files which recorded the internet sites that were visited by the employee. In examining the log files, the employer suspected internet use was reducing productivity, and the employer began to more closely monitor the employee using computer monitoring software. The employee was not informed that his computer use was being monitored until the monitoring reports were examined and a decision was made to discipline the employee. The employee was informed of the investigation during disciplinary meetings, and he was eventually terminated for cause.

The employee filed a complaint against UBC alleging improper collection of information. Adjudicator Catherine Parker determined that the employer had breached *FIPPA*. She found it was not reasonable to "initiate surreptitious surveillance" before taking other steps to address the issue. As such, the collection of information regarding the employee's internet use was not reasonably necessary for "the management of the employment relationship".

Employers should review their computer policies and practises to ensure they are accurately describing the extent to which an employee can expect their data to be accessed by others. *Cole* suggests the policy will significantly impact the court's assessment of the employee's reasonable expectation of privacy. Where access is permitted, it is important to ensure that the collection, use, and disclosure of an employee's computer data is reasonable and necessary. Where an employer suspects an employee is engaging in improper computer use, legal advice can assist the employer in determining how to address the issue without breaching privacy legislation.

For more information please contact a member of our Labour & Employment Group.

Key Contacts

- **Patricia Gallivan, Q.C.**
  P: 604.631.6718
  E: pgallivan@lawsonlundell.com
- **Rob Sider**
  P: 604.631.6722
  E: rsider@lawsonlundell.com

Team Members

Name	Phone	Email
Patricia Gallivan, Q.C.	604.631.6718	pgallivan@lawsonlundell.com
Jordan Kirkness	604.631.9172	jkirkness@lawsonlundell.com
(M.J.) Peggy O'Brien	604.631.9201	pobrien@lawsonlundell.com
Walter Rilkoff	604.631.6719	wrilkoff@lawsonlundell.com
Rob Sider	604.631.6722	rsider@lawsonlundell.com
Nicole Skuggedal	604.631.6795	nskuggedal@lawsonlundell.com
Clara Ferguson	403.218.7532	cferguson@lawsonlundell.com
Paul Smith	867.669.5532	psmith@lawsonlundell.com

©2011, Lawson Lundell LLP. All rights reserved. The information provided in this publication is for general information purposes only and should not be relied on as legal advice or opinion. For more information, please contact one of the lawyers listed above. To be removed from this mailing list please send an e-mail to genmail@lawsonlundlell.com or phone the Marketing Department at 604.685.3456.