WORKWISE
CURRENT EMPLOYMENT AND LABOUR LAW ISSUES

WORKWISE ISSUE# 45 WINTER 2012

TERRI SUSAN ZURBRIGG

DRAWING LINES IN THE VIRTUAL SAND: A CONSIDERATION OF *R. v. COLE* AND TIPS YOU CAN USE FOR DEVELOPING EFFECTIVE COMPUTER USE POLICIES IN THE WORKPLACE

Although a criminal case, the Ontario Court of Appeal's recent decision in ***R. v. Cole***, 2011 ONCA 218 **[*Cole*]** has significant implications for employers with respect to establishing expectations of privacy in the workplace in relation to employee computer use.

Traditionally, the law in this area was fairly straightforward and firmly rooted in the overarching principle that workplace computers were employer property, and, as such, any information stored on them was also employer property. Accordingly, the employee did not have any expectation of privacy in this data, and employers could monitor an employee's use of computers in order to ensure they were being used for work-related purposes.

Not surprisingly, as this technology has developed, so has the law. Indeed, computer technology in the workplace is no longer limited to desktop computers owned by the employer and provided to employees for their use during working hours. With the seemingly ubiquitous use of laptops and smart phones, the lines surrounding appropriate use of these portable and popular technologies in the workplace have become more difficult to draw.

In ***Cole***, a high school teacher used a laptop that his employer provided to store nude photographs of a student. As a result of a laptop program that he supervised at the school, he had access to data stored on students' laptops. Upon reviewing a student's computer files and discovering nude photos of another student, he transferred these photos onto his laptop's hard drive. The school's computer technician located these photos, which Mr. Cole stored in his "hidden" folder, in the course of performing routine computer and network maintenance. The technician notified the principal, and was then instructed to copy the images and Mr. Cole's internet search history onto a disc which was in turn provided to the police. The police examined both the disk and Mr. Cole's laptop without first obtaining a search warrant.

Mr. Cole was charged with possession of child pornography and unauthorized computer use. At the criminal trial, Mr. Cole's counsel successfully argued that the data resulting from the police's search

of Mr. Cole's laptop, as well as all temporary internet files that had been recovered by the police, should be excluded from evidence on the basis that Mr. Cole had a reasonable expectation of privacy in this data. In deciding to exclude this additional evidence, the Court of Appeal highlighted the fact that Mr. Cole had exclusive use of the laptop, which was also password protected, and that, in general, teachers who had been provided with laptops by the school board used them for personal purposes, such as banking, as well as professional purposes. Consequently, the police required a search warrant in order to access Mr. Cole's laptop for further evidence of misconduct. For a more comprehensive overview of the facts and findings in ***Cole***, please see the Summer 2011 edition of Field Law's Privacy Press newsletter.

While at first glance this ruling may be concerning to employers, it is important to keep in mind that the finding that Mr. Cole's right against unreasonable search and seizure was violated arose in relation to the police's ability to conduct a search, not his employer's. In fact, the Court found that the school board properly accessed Mr. Cole's laptop and copied the data to a disk for further internal investigation, as doing so was in keeping with the principal's obligations to ensure a safe school environment and to discipline teachers engaging in inappropriate conduct.

In this regard, it is worth noting that the school board was also able to rely upon its Policy and Procedure Manual, which prohibited storage of sexually explicit content on computers. The Manual further stipulated that all data and messages stored on computers were considered to be property of the school board, and made it clear that in cases where inappropriate use was suspected, the school would access private emails and data so teachers should not consider files stored on the network or hard drives to be private.

Finally, the photos in question were located by the computer technician in the course of carrying out routine computer maintenance, in the regular course of his duties. As such, the school board did not access the photos as a result of an arbitrary search.

Consequently, ***Cole*** should not be interpreted as holding that employers have a broad right to access employee's computer data in any and all circumstances. Rather, the lesson to be learned from ***Cole*** is that employers should establish policies clearly articulating their expectations regarding computer use in the workplace, and under what circumstances an employer may access computer data stored on its technology or networks by an employee. The arbitration decision in ***Re Lethbridge College and Lethbridge College Faculty Assn***[1] provides assistance in this regard as it emphasizes that an employer's ability to search the contents of an employee's computer "must be balanced against an employee's expectation of privacy and is subject to a test of reasonableness." While clearly-worded policies are an ideal way to establish the contours of reasonableness, evidence of suspicious behavior or anomalous network activity (for example, transferring or storing large amounts of data) are also factors that will affect the reasonableness of accessing data stored on workplace computers by employees.

In developing effective workplace computer policies, employers should be guided by the following principles; and the policies should include the following information:

1 *Re Lethbridge College and Lethbridge College Faculty Assn. (2007) 166 L.A.C. (4th) 289.*

- Parameters and rules regarding permissible and appropriate use (what is acceptable and what is unacceptable in the workplace);
- Whether any personal use of the technology is permitted, and if so, to what extent;
- That an employee does not have an expectation of privacy in data sent, stored or received using the employer's computer technology even if work-related information is intermingled with personal information;
- That the employer reserves the right to perform random checks or audits of an employee's computer and network use;
- Under what circumstances an employer will access an employee's computer account or monitor an employee's computer activity; and
- What discipline or consequences (including possibly termination) will flow from a contravention of the policy.

Although it is important for employers to have clear policies regarding workplace computer use, the ***Cole*** decision demonstrates that actual practices in the workplace are also relevant in determining privacy expectations. Accordingly, employers should strive for consistency in enforcing their policies and their practices.

- Where workplace computers are used by employees for personal purposes, it will be more difficult to argue that employees have no expectation of privacy whatsoever in this data, unless the policy clearly states otherwise.

Employees should be given a copy of any computer use policy. Ideally, the employer should review the policy with the employee and ask them to sign an acknowledgement that they understand its terms.

Field Law can assist with the preparation, drafting and review of workplace computer use policies. Please contact us for further information.

At the time of this publication, the Supreme Court of Canada granted leave to hear ***Cole***, which means that Canada's top court will soon weigh in on the contentious and complex issue of workplace privacy▲

EDMONTON
2000, 10235 - 101 STREET
EDMONTON AB T5J 3G1
PH 780 423 3003
FX 780 428 9329

CALGARY
400, 604 - 1 STREET
CALGARY AB T2P 1M7
PH 403 260 8500
FX 403 264 7084

YELLOWKNIFE
201, 5120 - 49 STREET
YELLOWKNIFE NT X1A 1P8
PH 867 920 4542
FX 867 873 4790

WWW.FIELDLAW.COM