CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY LAW BULLETIN NO. 295

NOVEMBER 29, 2012

EDITOR: TERRANCE S. CARTER

SUPREME COURT DECISION ON WORKPLACE COMPUTERS AND EMPLOYEE PRIVACY

By Barry W. Kwasniewski[*]

A. INTRODUCTION

Do employees have a reasonable expectation of privacy with respect to their personal information stored on workplace computers? This is a complex legal question, affecting the rights of charities and not-for-profits in their capacities as employers. In the recently released Supreme Court of Canada decision *R. v. Cole*,[1] Canada's highest court affirmed that employees can reasonably expect at least some privacy in the personal information they may generate on their workplace computers.[2] As explained below, the *Cole* decision arose in relation to a criminal proceeding. As such, the decision does not have direct application to private sector employees, including those of charities and not-for-profits. However, the decision does provide useful insight regarding how courts in Canada may approach the issues of workplace computer privacy. This *Charity Law Bulletin* will review the *Cole* decision, and provide guidance on how employees may address the issues of workplace computers and employee privacy concerns.

B. THE FACTS

R. v. Cole is a criminal case, but with important implications for the workplace. Richard Cole was a high school computer teacher who was charged with possession of child pornography and unauthorized use of a computer pursuant to ss.163.1(4) and 342.1(1) of the *Criminal Code*. During regular maintenance activities

[*] Barry W. Kwasniewski, B.B.A., LL.B., practices employment and risk management law with Carters' Ottawa office and would like to thank Tanya L. Carlton, OCT, B.Sc. (Hons.), B.Ed., J.D., Student-At-Law, for her assistance in the preparation of this *Bulletin.*

[1] *R v Cole*, 2012 SCC 53 (*Cole*).

[2] For background information, see Barry W. Kwasniewski "Ontario Court of Appeal Considers Employee Expectations of Privacy In Information Stored On Work Computers" in Charity Law Bulletin No. 250 (April 18, 2011) online: http://www.carters.ca/pub/bulletin/charity/2011/chylb250.htm.

by a school board computer technician, hidden files containing nude and partially nude pictures of an underage female student were discovered on Mr. Cole's computer. The laptop computer supplied to Mr. Cole by the school, and its use, was governed by the school board's Policy and Procedures Manual, which allowed for "incidental personal use of the board's information technology."[3] The policy stated that all teachers' email correspondence would remain private, but school administrators could access it if specified conditions were met. The school's Acceptable Use Policy, a student use policy which restricted laptop use and warned users to not expect privacy in their files, was also applicable to the teachers.

Following the search of the computer by the technician and school administrators, the police then performed a warrantless search. The warrantless search by police of the laptop and photographs copied onto compact discs by the technician was found by the trial judge to be in violation of ss.8[4] and 24(2)[5] of the *Canadian Charter of Rights and Freedoms*.[6] The summary conviction appeal court overturned the trial judge's decision and found that Mr. Cole's section 8 rights were not violated.[7] The Court of Appeal for Ontario however, held that the police did infringe his section 8 rights[8] and the Supreme Court of Canada upheld this finding, stating that Mr. Cole "expected a measure of privacy in his personal information on the laptop."[9] However, the Supreme Court also held that the evidence which the police obtained as a result of the search should not be excluded from the trial, as its admission "would not bring the administration of justice into disrepute".[10]

C. RIGHT TO PRIVACY: WORKPLACE COMPUTERS

As noted by the Supreme Court of Canada, personal information stored on computers can be "meaningful, intimate, and touch(es) on the user's biographical core".[11] Where a workplace permits personal use of computers, stored information "exposes the likes, interests, thoughts, activities, ideas and searches for

[3] *Cole, supra* note 1 at 16.
[4] Section 8 of the *Charter* provides that "Everyone has the right to be secure from unreasonable search and seizure".
[5] Section 24(2) provides that evidence obtained in a manner that infringes or denies any *Charter* rights will be excluded from evidence in a criminal trial, if the admission of that evidence would bring the administration of justice into disrepute.
[6] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c.11 (*Charter*).
[7] .*R v Cole*, 2009 CanLII 20699 (ONSC).
[8] *R v Cole*, 2011 ONCA 218.
[9] *Cole, supra* note 1 at 8.
[10] *Ibid* at 97.
[11] *Ibid*, at 2.

information" of an individual employee.[12] Accordingly, the Supreme Court held that employees would have a reasonable expectation of privacy concerning the personal information, where personal use is either expressly permitted or reasonably expected. This finding has important implications for employers, in terms of managing employee expectations of privacy, and protecting the employer from the abuse of workplace computers.

D. WORKPLACE COMPUTER POLICIES

The Supreme Court of Canada noted that "workplace policies and practices may diminish an employee's expectations of privacy in a work computer."[13] Therefore, practices and policies of the workplace will be relevant, and the "operational realities" of the office may decrease the reasonable expectation of privacy an employee might otherwise have.[14] Employers though, cannot rely on written policies alone in the determination of their employee's expectation of privacy – in the end it will be the "totality of the circumstances" that will determine whether privacy is to be expected.[15]

In the *Cole* case, the school board stated in their policy that they owned "all data and messages generated on or handled by board equipment" and the Student Acceptable Use Policy (also applicable to teachers) stated that email and work saved on hard drives would be monitored and users were warned that they "should NOT assume that files stored on network servers or hard drives of individual computers will be private."[16] The operational realities of the workplace in this situation therefore limited the privacy that Mr. Cole and other teachers should have expected in their computer files. Even so, the Supreme Court of Canada, looking at the "totality of the circumstances" still recognized a constitutionally protected privacy interest, as the information that was generated on the work computer from Mr. Cole's personal use was "meaningful, intimate, and organically connected to his biographical core."[17] Although workplace policies and procedures were in place, and the computer was owned by the school board, it still did not completely eliminate his privacy rights.

[12] *Cole*, *supra* note 1 at 3.
[13] *Ibid*.
[14] *Ibid* at 52.
[15] *Ibid* at 53.
[16] *Ibid* at 55.
[17] *Ibid* at 57-8.

E. CONCLUSION

The *Cole* decision highlights the importance of employers, including charities and not-for-profits, developing workplace computer policies governing employee use of work computers, Smartphones and other mobile communication devices. Although the Supreme Court of Canada has not commented on the right of an employer to monitor an employee's computer use, employers should be aware that some employees may still attempt to rely on *Cole* to limit their employer's monitoring rights, claiming an invasion of privacy.

Employers obviously have a legitimate interest in how their computers are used by employees. Employers need to protect confidential information and the integrity of their equipment and software. They also may require monitoring of computer use in order to assess employee performance issues, or to investigate harassment, workplace violence or human rights complaints. In light of the *Cole* decision, employers will need to take proactive steps to manage their employees' expectations for the privacy of any work related computer use. Employers should be clear that work computers are for work only, and that any personal communications must be limited, and/or transactions should be done on their own computers or devices. By implementing and adhering to these policies, employers can limit an employee's privacy expectations, by making it clear that the employee's work computer use is <u>not</u> private and may be monitored.