Ontario Court of Appeal Considers Employee Expectations of Privacy in Information Stored On Work Computers

By Barry Kwasniewski*

A. INTRODUCTION

Many employees have access to a computer that is provided to them by their employer. Many charities and not-for-profits allow for the personal use of these work computers, for activities such as downloading, storing information, or browsing the Internet. However, when employees use work computers for personal use, the boundaries become blurred between what information can and cannot be protected by an individual's reasonable expectation of privacy. In *R. v. Cole,*[1] a recent decision of the Ontario Court of Appeal, the court discussed an employee's expectation of privacy in information stored on a work computer. This *Charity Law Bulletin* summarizes this decision and discusses the privacy implications for employers/employees.

B. BACKGROUND TO THE DECISION

The Case

Richard Cole, a teacher employed by the Rainbow District School Board, was criminally charged with possession of child pornography after the school board's IT staff found nude photographs of a 16 year old Grade 10 student on his school-owned laptop computer. In his defence, Mr. Cole applied to exclude evidence based on an alleged breach of his right from unreasonable search and seizure, pursuant to section 8 of the *Canadian Charter of Rights and Freedoms.* The decision deals with the factual and legal issues arising on the application to exclude evidence obtained as a result of the seizure.

The Facts

* Barry W. Kwasniewski, B.B.A., LL.B., practices employment and risk management law with Carters Ottawa office and would like to thank Kate Robertson, B.A. LL.B., Student-At-Law, for her assistance in the preparation of this article. This article is reproduced with permission from *Charity Law Bulletin* No. 250, April 18, 2011.

[1] [2011] O.J. No. 1213 (Ont. Court of Appeal).

The teacher was provided with a laptop by the school for use in teaching communication technology and supervising a laptop program for students. As a supervisor, he was able to remotely access the data stored on student computers within the school network. At some point during his employment, he accessed a student's email account and copied nude photographs of one of the students onto the hard drive of his work laptop. As computer technicians for the school board have the responsibility of monitoring and maintaining the integrity and stability of the school network, one of the computer technicians observed an unusual amount of activity between the teacher's laptop and the school's server, which sparked a search of the contents of the teacher's hard drive. In this search, the computer technician came across a hidden folder on this hard drive, which exposed the nude photographs of a 16-year-old student. The computer technician reported the images to the principal of the school. The teacher was asked to return his laptop to the school and provide his password for access. The teacher refused to provide his password, but the computer technician accessed the computer again and obtained several compact discs of relevant information. The laptop was then handed over to the police, along with compact discs of scanned information from the teacher's computer.

The police then conducted a warrantless search of the laptop and a disc with temporary internet files, which showed the teacher's internet browsing history. The teacher was eventually charged with possession of child pornography and unauthorized use of a computer contrary to ss.163.1(4) and 342.1(1) of the *Criminal Code*. In the Ontario Court of Justice, the evidence was excluded under s. 24(2) of the *Charter*, as the judge determined that the teacher had a reasonable expectation of privacy in the contents of his laptop hard drive, and the warrantless search and seizure of the material by the police officer constituted a breach of his Section 8 *Charter* rights. On appeal to the Superior Court of Justice, the trial judge's decision was overturned and sent back for retrial, since the appeal judge found that there was no reasonable expectation of privacy in the contents of the laptop's hard drive. The teacher appealed this decision to the Ontario Court of Appeal, which for the reasons described, allowed the appeal in part, and sent the matter back for trial.

C. ISSUES

There were several issues raised in the Ontario Court of Appeal decision:

- Did the teacher have a reasonable expectation of privacy in the contents of the laptop?
- If so, did (a) the technician or (b) the principal or (c) the school board breach s.8 of the Charter?
- Did the police breach s.8 of the Charter by searching the laptop and the compact discs without a warrant?
- If so, did the trial judge err in excluding the evidence?

The focus of this *Charity Law Bulletin* is whether the high-school teacher had a reasonable expectation of privacy in the contents of a work computer on which he was entitled to store personal information.

D. COMMENTARY

1. Reasonable Expectation of Privacy

Ontario Court of Appeal Justice Karakatsanis discussed whether or not the teacher had a reasonable expectation of privacy in the contents of the laptop. The reasoning of the judge involved an analysis of the factors identified in the leading Supreme Court of Canada decision in *R. v. Edwards,*[2] which include:

- Whether the accused was present at the time of the search;
- Whether the accused had possession or control of the property or place searched;
- Whether the accused owned the property or place searched;
- The historical use of the property or item;
- The ability to regulate access, including the right to admit or exclude others from the place;
- The existence of a subjective expectation of privacy; and
- The objective reasonableness of the expectation.[3]

[2] [1996] 1 S.C.R. 128.
[3] *Ibid* at para 45.

Applying these tests, the Ontario Court of Appeal concluded that the teacher had a reasonable expectation of privacy in the contents of the laptop because:

- While the teacher did not own the laptop, the teachers at the school were granted exclusive possession of the laptops;
- The accused was given access to the computer on weekends and during vacations for personal use;
- Access to the computer was protected by a password;
- It was the norm for other teachers on the board to store sensitive personal information on their work laptops as well; and
- The policy provisions dealing with the monitoring or search of teacher laptops were found to be vague.[4]

Although the teacher was aware of the school board policies regarding the search of email communications specifically, there were no clear policies that mentioned the monitoring or policing of teachers using their laptops for personal use.[5]

It is important to note that while the court held that the teacher had a reasonable expectation of privacy, the actions of the board in copying data and searching the laptop in support of an investigation of a serious allegation of teacher misconduct did not violate the teacher's rights. The court stated, "…the school board had an ongoing obligation to take steps to ensure a safe and secure learning environment for its students and to protect the students' privacy rights. The search of the laptop and preservation of the evidence for an internal discipline procedure was an obvious means to do so."[6] Further, the court held that the principal's decision to copy images onto a disc and seize the laptop was implicitly authorized by the *Education Act*[7], as part of the principal's duty to ensure a safe school environment. While the principal and school board's actions were deemed appropriate by the Court, the warrantless seizure of the laptop by the police was found to constitute a violation of section 8 of the *Charter*. While it is beyond the scope of this Bulletin to analyze the details of this part of the decision, the Court did permit the disc with the screen shot and the images of the student to remain as prosecution evidence.

---

[4] *Supra* note 1 at para 36-39.
[5] *Ibid* at para 41.
[6] *Ibid* at para 64.
[7] R.S.O. 1990, c. E.2, s. 265.

E. CONCLUSION

Employers have the right to govern the terms of the use of work computers by their employers. With the number of employees that now require computers as part of their daily activities in the workplace, the conflicts that could potentially arise will undoubtedly continue. While decided in the criminal law context, *R. v. Cole* illustrates the importance of having a policy relating to personal use of work computers. Such a policy will determine the extent to which an employee has any expectations of privacy of materials stored on work computers. As with all policies, it is important that they be clearly communicated to employees to ensure adherence and provide a basis for discipline in the event of a breach. The law changes over time, and may differ according to the jurisdiction where you operate. Therefore, it is advisable to have any new policies reviewed by a lawyer before you implement them.