Forbidden Images on a Teacher's Laptop - A Lesson Well Learned

By Teresa Haykowsky, Partner

In the recent Ontario decision *R.* v. *Cole*, the Ontario Court of Appeal was called upon to determine whether employees have a reasonable expectation of privacy in their personal use of work computers or laptops and whether the computer/laptop searches conducted by the School District and the police in that case were reasonable under the *Charter*.[1]

Facts

A high school teacher used an employer-owned laptop to teach communication technology and supervise a student laptop program. The teacher had domain administration rights to the network so he could monitor and police the network. As part of his job, the teacher regularly accessed data stored on student computers connected to the school network. The teacher found nude photos of one student on another student's email account. The teacher copied the photos to his school-issued laptop.

Noting a large amount of activity between the teacher's laptop and the school's server, a computer technician for the School District did a virus scan on the teacher's computer and discovered nude, sexually explicit photos of a girl who appeared to be underage.

The technician advised the school's principal who directed him to copy the images to a disc. The School District also searched the laptop and copied the teacher's surfing history onto another disc. It gave the police two discs: one with a copy of the photos and another with a copy of the teacher's surfing history.

The School District provided the investigating officer with copies of its Acceptable Technology Use Policy which allowed employees to store personal information on work laptops. The policy did not expressly state that sexually explicit material was not allowed on the computers. While students were required to sign an Acceptable Use Agreement, teachers were not.

The police officer determined that notwithstanding this policy, the computer data did not belong to the teacher. As a result, he reviewed the discs to determine whether the photographs constituted child pornography, all without the benefit of a search warrant.

The teacher was then charged with possession of child pornography and unauthorized computer use.

The Court of Appeal found that the School District did not breach the teacher's right to an unreasonable search and seizure under the *Charter* by having School District officials search the content of the work computer. The employee had no expectation of privacy with respect to access to

[1] This decision did not deal with private sector employers, which are not subject to the *Charter*. The Court of Appeal assumed that the *Charter* applied to the School District, as a government entity.

his hard drive by a technician (of the School District) for the limited purpose of maintaining the technical integrity of the school's information network and the laptop:

> "The technician was acting within the scope of his functions when he came across the student photographs and thus did not violate the appellant's [teacher's] modified privacy interests. The principal and school board officials acted reasonably under the authority of the *Education Act* to protect students and a safe learning environment."

On the other hand, the Court found that the teacher had a reasonable expectation of privacy with regard to the review of his personal files on the School District's hard drive by the police.

As part of its investigation into the matter (given the allegation of teacher misconduct and the threat to the school environment), before handing over the laptop to the police, the School District searched the laptop, obtained data relating to the teacher's internet browsing and saved the 'temporary internet files' onto a disc.

The Court found that the School District's search and seizure of the laptop was authorized and reasonable - there was no *Charter* breach. While there was no longer any immediate threat to the school, students or the school's computer network, the School District had an ongoing obligation to take steps to ensure a safe and secure learning environment for its students and to protect their privacy rights. The employer's laptop search and preservation of the evidence for an internal discipline procedure was an obvious means to do so.

Again, however, the police laptop search and the police seizure (of the disc containing temporary Internet files from the teacher's browsing history) violated the teacher's right to be secure against unreasonable search and seizure under the *Charter*. The Court of Appeal ruled that this evidence should be excluded at the teacher's trial.

This case suggests that employees may, in certain circumstances, have a reasonable expectation of privacy in relation to their personal use of work-related technology. However, whether an employee has an expectation of privacy depends on the specifics in each case. Factors upon which the Court relied in this case included:

- whether the policy permitted employees to use the work technology systems for personal matters;
- whether the policy clearly stated the employer could monitor or search the laptops used by employees;
- whether the employer regularly monitored employee computer/laptop usage;
- whether an employee was the sole user of the computer/laptop and whether s/he had password protected the computer access; and
- whether employees could take the computer/laptop home.

In consideration of these factors, the Court made the following findings:

- That the teacher's reasonable expectation of privacy in the laptop had been modified because the teacher knew the technician could access the computer to maintain the technical integrity of the school's information network.
- That the Technology Use Policy had been modified by practice.
- That the laptop search by the School District was authorized and reasonable based on its obligation to ensure student health and safety under the *Education Act*.
- Because the photographs were taken from the school's network using the school's computer and were the subject of the student privacy, the teacher had no personal privacy interest in this data.

Employers should take steps to ensure their Internet/Acceptable Technology Use policies are clear in terms of searching and monitoring hard drives, internet and e-mail, computers, laptops and other computer devices used by employees for work-related purposes.

Employers should regularly update these policies to keep up with the law, particularly in the area of employee privacy. As part of this review, employers should implement a clear and comprehensive policy which addresses the following:

- A clear definition of acceptable and unacceptable technology usage.
- The extent (or limits) to which, if at all, employees may use the employer's technology for personal use and whether employees may take laptops and electronic devices home for personal use.
- Whether there is a reasonable expectation of privacy with regard to the employee's usage of the employer's electronic technology.
- The employer's right to search and monitor its employees' technology use and the reasons for the same.
- Statement that the employer will search/monitor an employee's inappropriate use of the employer's technology and that this type of search/monitoring is considered reasonable.
- Statement that all employees (including supervisors, managers and directors) will be held to the same standard and violations will be dealt with in a consistent manner.
- Notice regarding the consequences to employees who fail to act in accordance with the policy.
- Appropriate policy training and written confirmation from employees that the policy has been read, understood and that each employee agrees to and will abide by the same.

As a result, if a company has condoned personal usage of its electronic technology, an employee may be able to argue that s/he has a reasonable expectation of privacy in that usage. A well-written policy, that is enforced consistently, goes a long way to address the concerns raised by the Ontario Court of Appeal in *R.* v. *Cole*.