Labour and Employment in the News

Off Limits? Maybe Not: Supreme Court Addresses Employee Privacy on Company Computer

By: Christina Hall and Andrew Carricato

On October 19, 2012, the Supreme Court of Canada released its eagerly awaited decision in ***R. v. Cole, 2012 SCC 53***. In this criminal case, the accused (a high school teacher), argued that his right under section 8 of the *Canadian Charter of Rights and Freedoms* (the "*Charter*") to be free from unreasonable search and seizure had been violated when police reviewed the contents of his work-issued laptop without first obtaining a search warrant. As a result, he argued that the evidence obtained from his laptop should be excluded from consideration in his criminal case.

In its decision, the Supreme Court held that where employees are permitted or reasonably expected to make personal use of work-issued computers or devices, they may have a reasonable, though diminished, expectation of privacy in the personal information they have stored on those devices. This reasonable expectation of privacy is protected by the *Charter* such that any inspection and taking of an employee's work-issued device by the state will constitute a "search and seizure", requiring an assessment as to whether the search and seizure was reasonable in accordance with *Charter* principles.

R. v. Cole received a significant amount of attention in both the mainstream and legal media as it navigated its way through the courts up to the Supreme Court of Canada. There was concern expressed along the way that a decision in the case could create a new law with respect to the privacy rights of employees *vis à vis* their employers – for example, a pronouncement on the scope of an employer's right to monitor the computers and other devices issued to its employees. However, these concerns have been alleviated as the Supreme Court confirmed in *R. v. Cole* that the privacy rights recognized in the decision apply only to the rights of employees *vis à vis* the state and the right of an individual to be free from unreasonable search and seizure**.** The Court specifically stated that it would leave for another day "the finer points" of an employer's right to monitor computers and devices issued to employees.

THE FACTS

Richard Cole was an Ontario high school teacher. In addition to his regular teaching duties, he was responsible for policing the use by students of their networked laptops. To this end, he was supplied with a laptop owned by the school board and he was given domain administration rights on the school's network. This allowed him to access the hard drives of students' laptops. Mr. Cole was also permitted to use his laptop for incidental personal purposes, which he did. He often browsed the Internet and stored personal information on the laptop's hard drive.

Mr. Cole's difficulties began when a school technician, performing maintenance activities on the school's network, found a hidden folder on Mr. Cole's laptop that contained nude photographs of a high school student. The technician copied the photographs to a CD and reported his findings to the school principal. The school principal seized the laptop and school board technicians copied its temporary Internet files onto a second CD. The laptop and both CDs were handed over to the police who reviewed all the information without first obtaining a search warrant. Mr. Cole was then charged with possession of child pornography and unauthorized use of a computer contrary to ss. 163.1(4) and s. 342.1(1) of the *Criminal Code*[1] and was prosecuted by way of summary conviction.

THE *CHARTER* ISSUE

At the outset of his criminal case, Mr. Cole brought a pre-trial motion challenging the admissibility of the evidence obtained by the police from his laptop. He argued that his right to be free from unreasonable search and seizure, enshrined in section 8 of the *Charter*, had been infringed when the police reviewed the evidence from his laptop without having first obtained a search warrant and therefore that the evidence seized should be excluded pursuant to section 24(2) of the *Charter*. A threshold issue thus became whether Mr. Cole had a reasonable expectation of privacy in the contents of his work-issued laptop such that he was entitled to the protection of the *Charter*.

PRIOR PROCEEDINGS

The trial judge found that Mr. Cole had a reasonable expectation of privacy in his work-issued laptop and that the police had breached his rights under section 8 of the *Charter* by searching and seizing the laptop without first obtaining a search warrant. The trial judge excluded all of the computer evidence obtained as a result of the search, on the basis that the admission of the evidence would bring the administration of justice into disrepute. As the Crown offered no further evidence, the charges against Mr. Cole were dismissed.

On appeal, the summary conviction appeal court reversed the initial decision and admitted the computer evidence. It found that Mr. Cole did not have a reasonable expectation of privacy in his work-issued laptop and therefore that there had been no breach of his *Charter* rights.

On further appeal to the Court of Appeal for Ontario, the decision of the summary conviction appeal court was set aside. The Court found that Mr. Cole had a reasonable expectation of privacy in his work-issued laptop such that the warrantless search and seizure of the laptop by the police breached Mr. Cole's rights under section 8 of the *Charter*. It excluded most of the evidence seized and sent the matter back for a new trial.

THE DECISION OF THE SUPREME COURT OF CANADA

The Supreme Court confirmed that in order to determine whether Mr. Cole had a reasonable expectation of privacy in his work-issued laptop, the Court was required to apply the following four lines of inquiry:

1. An examination of the subject matter of the alleged search;
2. A determination as to whether the claimant had a direct interest in the subject matter;
3. An inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and
4. An assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.[2]

After considering these lines of inquiry, the Court concluded that the subject matter of the police search was the informational content of the laptop's hard drive and Internet files. The Court further commented that Mr. Cole's direct interest and subjective expectation of privacy in this informational content could be inferred from his use of the laptop to browse the Internet and to store personal information on the hard drive. Thus, the remaining question was whether Mr. Cole's subjective expectation of privacy was objectively reasonable.

1 R.S.C. 1985, c. C-46

2 *R. v. Tessling* [2004] 3 S.C.R. 432 at para. 32; *R. v. Patrick* [2009] 1 S.C.R. 579 at para 27

In order to answer this question, the Court first considered the nature of the information in issue and stated that the closer that information lies to the biographical core of personal information, the more likely it is that there will be a reasonable expectation of privacy in relation to that information. Here, Mr. Cole's computer was used to browse the Internet which has been recognized to reveal a person's specific interests, likes and propensities, which are all recorded and stored in the browsing history and cache files. As a result, the Court held that this highly revealing and meaningful information about Mr. Cole's personal life went to the very heart of the "biographical core" of personal information protected by section 8 of the *Charter.* This weighed in favour of a reasonable expectation of privacy.

The Court then turned to examine ownership issues and operational realities. In this case, Mr. Cole's employer, the school board, had a patchwork of policies, practices and customs – all of which factored into the Court's analysis. In terms of ownership, the Court noted that the school board had a policy stating that it owned not only the hardware (i.e. the laptop itself), but also the data stored on it – a fact which weighed against a reasonable expectation of privacy. In terms of the operational realities, the Court noted that this factor weighed both for and against a reasonable expectation of privacy – *for,* because written policy and school board practice was to permit Mr. Cole to use his work-issued laptop for personal purposes, and *against* because school board policies and technological reality deprived Mr. Cole of exclusive control over – and access to – the personal information he chose to record on his laptop. That is, the contents of his hard drive were available to all other users and technicians with domain administration rights.

After considering the "totality of the circumstances", the Court concluded that although Mr. Cole's privacy interest in his laptop was diminished by ownership issues, workplace policies and various operational realities, these factors did not *eliminate* his otherwise objectively reasonable expectation of privacy in the contents of his work-issued laptop. The Court further concluded that the examination of the laptop by the police without a warrant, violated Mr. Cole's rights under section 8 of the *Charter.* However, despite these conclusions, the Court declined to exclude the evidence obtained from the police search on the basis that it was, "highly reliable and probative physical evidence" and that its admission would not bring the administration of justice into disrepute. The Court thus set aside the exclusionary order of the Court of Appeal for Ontario and ordered a new trial for Mr. Cole.

IMPLICATIONS FOR EMPLOYERS – LITTLE CAUSE FOR ALARM

While the Supreme Court has confirmed in *R. v. Cole* that employees may have a reasonable expectation of privacy in the personal information stored on their work-issued devices, particularly where personal use of those devices is permitted or reasonably expected, it is important to reiterate that this "reasonable expectation of privacy" arises in relation to an individual's *Charter*-protected right to be free from unreasonable search and seizure by the state. As a result, while the decision will no doubt be of great interest to governmental authorities, the police and public sector employers who are subject to the *Charter,* it is of limited practical relevance to private sector employers.

That said, the decision in *R. v. Cole* does provide insight into how the Court will approach claims of individual privacy rights in an era in which an ever-increasing amount of personal information is created and stored in electronic form – often on portable devices such as laptops and smartphones that move easily, and blur the lines, between home and work and the personal and professional. Although, in this case, the Court specifically declined to address the issue of an employer's right to monitor the computers and devices it issues to its employees, there will surely be a time in the not-too-distant future when the Court will be called upon to address this issue.

Taking guidance from the Court's decision in *R. v. Cole*, employers would be well-advised to implement workplace policies that govern employees' use of the employer's technology. Such policies should:

- Address ownership issues in the technology and any data stored on the technology;
- Outline the permitted use of the technology (including any permitted personal use), as well as a list of prohibited conduct in relation to the technology;
- Confirm the employer's right to access and monitor the technology and the reasons for which the employer may do so, such that an employee should not have an expectation of privacy when using the technology; and
- State that any use of the technology in contravention of the policy may result in disciplinary action up to and including termination of employment, and that any possible criminal use of the employer's technology will be reported to the appropriate authorities.

As with all workplace policies, employers should ensure that any policy governing employee use of the employer's technology is provided to employees for review at the time of hiring and that the employee agrees that he or she has read, understood, and will abide by its contents by signing off on the policy. Similarly, it is critical that any such policy be well-understood by those within the organization who will be responsible for enforcing it and that the policy is, in fact, consistently enforced. Lastly, employers must remember to review and update the policy as necessary in order to ensure that the policy remains compliant with any legal requirements and that it takes into account any changes in technology. Of course, any updates must also be clearly communicated to employees.

While the above measures may not preclude a court from finding, in a future case, that employees have some measure of privacy rights *vis à vis* their employer in the information they store on a work-issued computer or device, employers who adopt these measures will be in a stronger position to defend against any such claims and argue against the employees' "reasonable expectation of privacy".

ABOUT HEENAN BLAIKIE

Heenan Blaikie is recognized as one of Canada's leading law firms. We focus on six practice areas: business law, labour and employment, taxation, litigation, intellectual property and entertainment law. We deliver comprehensive legal advice and innovative business solutions to clients across Canada and abroad from our nine offices in Quebec, Ontario, Alberta and British Columbia, and our Paris office and Singapore representative office.

Today, the firm is over 575 lawyers and professionals strong and still growing. We strive to become partners in our clients' businesses, ensuring that our legal advice addresses their preoccupations and priorities. We seek to constantly adjust the scope of our services to better serve our clients' legal needs.

Our clients range in size and sophistication from start-ups to the largest public companies, as well as health care and social services institutions, schools and universities, and numerous government entities. We also represent international clients seeking to protect and expand their interests in Canada.

Seminars & Training for Employers
www.managingtheworkplace.com

Workplace Wire Blog
www.workplacewire.ca