COMMERCIAL LITIGATION REVIEW

Volume 9 • Number 2 May 2011

IN THIS ISSUE:

LexisNexis®

LITIGATION: PRIVACY IN THE PRIVATE SECTOR WORKPLACE

Lisa K. Talbot
Partner, Torys LLP

… it is best for employers to have a clear privacy and computer-use policy that is consistently enforced to prevent an expectation of privacy from arising.

The Ontario Court of Appeal's Decision in R. v. Cole: Implications on Workplace Privacy

Counsel who draft and seek to enforce privacy and computer-use policies must determine whether the employer is subject to the *Charter* and, if so, whether that employer has a statutory duty to seize evidence from the computer and turn it over to the police. In these factual circumstances, we gain insight into the scope and limits of private sector workplace privacy.

The Court of Appeal for Ontario recently ruled that employees have a reasonable expectation of privacy regarding information stored on work-issued computers and other devices where the employer has not implemented a privacy policy that indicates otherwise. It was on these grounds that, in *R. v. Cole*,[1] the Court of Appeal found that the police infringed the *Canadian Charter of Rights and Freedoms* by searching a teacher's work-issued laptop without a warrant.

The *Cole* case has drawn much attention since the reasons were released on March 22, 2011. The press has referred to it as a "landmark decision" and a "seismic shift" in workplace privacy.[2] While *Cole* is certainly a significant case, its impact on private sector workplaces is likely to be more limited than the headlines suggest. *Cole* is a criminal case that was decided in the context of the *Charter*, to which private sector employers are not subject. The employer in the case — a school board — did not have a clear policy to monitor, search or police the teacher's laptop use, which was a key factor in the Court's analysis. In any event, it was the search and seizure by the police, not the actions of the employer, that were censured by the Court. Although the Court's analysis has limited application to private sector employers, it does provide insight into the Court's views on workplace privacy and underscores the importance of having clear and unambiguous privacy and computer-use policies.

Commercial Litigation Review

The **Commercial Litigation Review** is published quarterly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-44288-3 ISSN 1705-7027

ISBN 0-433-44300-6 (print & PDF)

ISBN 0-433-44660-9 (PDF)

Subscription rates: $250.00 (print or PDF)
$380.00 (print & PDF)

This article reviews the *Cole* decision, addresses the application of the case to private sector workplaces, and suggests best practices for employers to minimize privacy expectations over information stored on work-issued computers and other devices.

Facts of the Case

The *Cole* case involved a high school teacher who was charged with possession of child pornography and unauthorized use of a computer contrary to the *Criminal Code*.[3]

The teacher and his colleagues were provided with laptop computers by their employer, a school board. The laptops were for work-related uses, but personal use of the laptops was also permitted under the school board's policy manual. Teachers regularly used the laptops at home, on weekends and while on vacation. There was also evidence that teachers stored personal information and financial data on the laptops.

Under the school board's policy, sexually explicit material is not allowed to be stored on the laptops, and all data and messages generated on or handled by school board-issued equipment are considered to be the school board's property. The policy provides that teachers' email accounts may be accessed, but only for the purposes of network maintenance and investigating cases that generate a suspicion of inappropriate use.

In the process of conducting maintenance on the school's server, a computer technician accessed the contents of the teacher's laptop and found sexually explicit images of an underage female student. These were copied onto a disc. The technician reported his findings to the principal, who then asked the teacher to hand over the laptop. A school board official then searched the laptop and copied temporary Internet files from the teacher's surfing history onto another disc. The two discs and the laptop were then turned over to the police, who searched them without a warrant and subsequently charged the teacher under the *Criminal Code*.

Court of Appeal's Decision

In a unanimous decision, the Court of Appeal determined that the police search violated the teacher's *Charter* rights since he had a reasonable expectation of privacy that personal material on his work-issued computer would not be subject to search by police.

In coming to this conclusion, the Court noted that although the laptop was a work computer owned by the school board and issued for employment purposes, the following facts specific to the case supported the expectation of privacy:

1. The school board had given the teacher exclusive possession of the laptop and explicit permission to use the laptop for personal use. The school board also allowed teachers to take the laptops home on evenings, weekends and holidays. These facts suggested to the Court that the teacher had *de facto* possession or control of the laptop, militating in favour of a reasonable expectation of privacy.
2. The teacher and his colleagues used their computers to store sensitive personal information. The conventions and customary personal use of the laptop by other teachers suggested to the Court that the expectation of privacy held by the teacher was reasonable.
3. The school board had no clear policy permitting it to monitor, search or police the teacher's laptop use. In particular, the policy did not specify that the contents of the work-issued laptops were subject to search and provided only that email may be accessed for the purposes of network maintenance and investigating suspicions of inappropriate use. The Court found that the school's policy did not create the expectation that teachers' laptops would be searched and monitored by the police. The fact that the teacher knew that the school board could access the hard drive of the laptop under its policy did not displace his reasonable expectation of privacy against a search by the state. However, this expectation was limited by the right of access of his employer's technicians in performing work-related functions.

The Court compared the school board's ability to access the laptop to a hotel's cleaning staff's ability to enter a hotel room with a master key: if a hotel guest knows that cleaning staff will enter the room, it does not remove the reasonable expectation of privacy in "areas that do not require daily maintenance," but the hotel guest's reasonable expectation of privacy is modified to the extent she knows that someone will be entering and cleaning the room.

The Court found that the teacher's *Charter* rights were not breached by his employer as a result of the technician's search, since it occurred during routine maintenance of the system; nor were his rights breached as a result of the principal's and school board's actions, which constituted proper follow-up — especially given that the images found depicted an underage student in their care. The Court noted that once the principal and school board were aware of the images, the *Education Act*[4] implicitly authorized seizing the evidence and turning it over to the police. The Court found that the school board 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 breach of the teacher's *Charter* rights resulted not from the employer's actions, but from the police's warrantless search and seizure of the laptop and of a disc containing temporary Internet files. It was lawful for the police to look at the disc on which the images of the student were copied, but copying the entire hard drive of the laptop and searching the disc containing the temporary Internet files was unreasonable. The Court found that the lack of exigency, the privacy interest that the teacher had in his browsing history and the broad nature of the search contributed to the unreasonableness and unlawfulness of the police conduct under s. 8 of the *Charter*.

The Court ordered that the evidence be excluded and a new trial conducted.

Application of the Case to Private Sector Employers

Before the Court of Appeal's decision in *Cole*, there had been a dearth of clear appellate authority regarding workplace privacy. Since the release of the decision, many have concluded that *Cole* has revolutionized the area. However, it must be noted that the Court's analysis has only limited application to private sector employers, for the following reasons:

1. The decision in *Cole* arose out of a criminal proceeding. For many employers, privacy is a serious concern because they are worried about their own liability. In *Cole*, the police — not the employer — were found to have breached the *Charter*. This case creates a helpful precedent for employees whose workplace computers are searched and seized by police and who are subsequently prosecuted; however, it does not necessarily create new sources of liability for employers, especially those who have clear privacy and computer-use policies.
2. The case was decided in the context of the *Charter.* The issue before the court was whether the school board and/or the police breached the teacher's right, under s. 8 of the *Charter,* to be free from

unreasonable search and seizure. The Court assumed that the *Charter* applied to the school board. The Court's analysis, then, applies directly to parties who are subject to the *Charter*: private sector employers are not.

3. The employer in *Cole* had a statutory duty under the *Education Act* to seize the evidence and turn it over to the police. The Court's approach to the conduct of the school board and its personnel was predicated on the statutory duty of the school board to protect its students. While this approach likely resulted in a more favourable finding with respect to the employer in this case, it also narrows the reach of the Court's analysis.

Although the Court's reasoning has limited direct application to private sector employers, it is an important case for them nonetheless. The Court's decision provides insight into its views on privacy rights in the workplace. These views will certainly be taken into consideration by courts, arbitrators and tribunals when assessing the scope and limits of private sector workplace privacy in the future and should form the basis of counsel's advice to employers with respect to best practices in future.

Advising Employers after *Cole*

The most important lesson that emerges from *Cole* for private sector employers is that an employee's privacy interests are not negated simply because a device on which private information is stored is owned by the employer. In the past, ownership of property had been of central importance in determining whether a reasonable expectation of privacy exists. From now on, relying solely on mere ownership of property is not likely to serve as sufficient insulation from claims that employees have a reasonable expectation of privacy over information stored on work-issued computers and other devices.

Cole also underscores the importance of having clear policies that minimize employees' privacy expectations in their work-issued computers and other devices. Many employers already have such policies (another reason why *Cole* is not as revolutionary as some have suggested). Out of an abundance of caution, employers should consider turning the following best practices into standard practices:

- Have a clear policy that expressly sets out any prohibited use of work-issued computers, laptops and other devices. The policy can be a stand-alone document or part of an employee code of conduct. For new employees, incorporate the privacy policy or code of conduct into the employment contract by explicit reference. The privacy policy should
    - include a clear statement that use of work-issued computers, laptops and other devices for any unlawful or inappropriate purpose or for a purpose contrary to the employer's policies is prohibited;
    - explicitly reserve the employer's right to broadly access, monitor, search, review, track and store any communication or information that is stored on work-issued computers, laptops and other devices, to report any unlawful use to the police and to take any and all appropriate action, including disciplinary action if a violation of the policy is found;
    - clearly state the reasons why the employer might access, monitor, search or review any communication or information that is stored on work-issued computers, laptops and other devices, including to ensure compliance with its policies and to protect
        - the integrity of data;
        - the efficient and proper operation of its systems;
        - the confidentiality of information and data belonging to the company, its employees, clients, suppliers, etc.;
        - the company's compliance with applicable laws; and
        - employees and the workplace environment from harassment and discrimination.

    - expressly advise employees that as a result of the employer's broad rights (as mentioned above) regarding communications and information stored on work-issued other devices, they should not expect their communications to be private and should use good judgment and discretion when sending or storing personal, confidential or sensitive information or messages.

- Ensure that employees regularly acknowledge that they have read, understood and agreed to abide by the privacy policy. This can be done electronically or by initialling each page of a paper copy of the policy and signing it. Keep the employees' acknowledgements or signed policies in their employee files.
- Enforce the policy consistently to avoid allowing customary use to create an environment in which expectations of privacy can emerge. Do not condone breaches of the policy.
- Review and update the policy regularly and have employees sign off on the policy every time it is revised.

Cole confirms what many lawyers have been advising for years: it is best for employers to have a clear privacy and computer-use policy that is consistently enforced to prevent an expectation of privacy from arising.

[*Editor's note*: The author wishes to thank Steven Slavens, student-at-law, for his assistance in the preparation of this article.]

---

1 [2011] O.J. No. 1213, 2011 ONCA 218.

2 Wallace Immen, "Computer ruling seen as landmark workplace decision," *The Globe and Mail*, March 25, 2011 online: <http://www.theglobeandmail.com/report-on-business/managing/on-the-job/computer-ruling-seen-as-landmark-workplace-decision/article1957321/>. See also: Kirk Makin, "Material on work computer private, court rules," *The Globe and Mail*, March 22, 2011 online: <http://www.theglobeandmail.com/news/national/ontario/material-on-work-computer-private-court-rules/article952239/>.

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

4 R.S.O. 1990, c. E.2.