CANADIAN
Employment Law Today

Published by Canadian HR Reporter, a Thomson Reuters business ■ www.employmentlawtoday.com

CURRENT NEWS AND PRACTICAL ADVICE FOR EMPLOYERS JUNE 15, 2011

CASE IN POINT: PRIVACY

Whose hard drive is it anyway?

Ontario court ups the ante for employees' right to privacy on work computers against employer searches and monitoring

BACKGROUND

Work computers a private affair

IN THE May 18, 2011, issue of *Canadian Employment Law Today*, Alberta employment lawyers Tina Giesbrecht and Toni Eckes discussed how far employers can expect to be able to keep an eye on what employees are doing on the employer's own computer equipment. Based on a prominent Alberta Court of Appeal decision, it appeared there were definite limits on how much expectation of privacy employees could have regarding work computers.

However, a sidebar to that story noted a recent Ontario Court of Appeal decision that may muddy the waters and raise the bar with regards to employees' privacy rights on work computers and other electronic equipment. Ontario lawyer Adrian Jakibchuk takes an in-depth look at this recent decision and what it means for employee privacy rights and employers' rights to check their own equipment.

| BY ADRIAN JAKIBCHUK |

IN THE technological workplace, more and more employers are permitting — even encouraging — employees to use company-owned devices beyond the workplace and outside of working hours. While this may lead to an improved ability to respond to customer demands and increased flexibility in employee scheduling, it inevitably also leads to a heightened risk of computer misuse and abuse.

One of the ramifications of an increased reliance on portable technology is a more focused conflict between the privacy interests of employees in the personal, non-work-related information stored on "their" computers and the interests of employers in ensuring the technology they provide to employees is not misused. This conflict was recently considered by the Ontario Court of Appeal in its decision in *R. v. Cole*, released in March.

The defendant was a high school teacher charged with possession of child pornography after the school's computer technician found nude, sexually explicit images of a grade 10 student on the hard drive of the teacher's laptop computer. The teacher, who was a member of the school's technology committee and, consequently, able to monitor the school's network, was believed to have obtained the images by accessing a student's email account.

The computer technician came across the images while conducting routine maintenance. Upon finding the images, the technician took a screen shot of the laptop and reported it to the principal. The principal asked the technician to copy the photos onto a disk and to provide it to him. The next morning, the principal asked the teacher to hand over the computer. The laptop and disks, as well as temporary internet files from the laptop's browsing history, were provided to the police, who searched them without a warrant.

The teacher challenged the searches of his laptop by the technician, principal, school board and police, arguing they breached his charter right to be free from unreasonable search and seizure.

The Ontario Court of Appeal wades in

The Court of Appeal held that the teacher had a reasonable expectation of privacy in the personal use of his work laptop. Even though the laptop was a work computer owned by the school board and issued for employment purposes, a number of factors pointed towards a reasonable expectation of privacy in its contents. In particular, the court noted the school board gave teachers possession of laptops and granted them explicit permission (set out in the board's Policy and Procedures Manual) to use them for personal use and to take them home on evenings, weekends and summer vacations. The court likewise noted that teachers invariably used their computers for personal use, stored personal information on their hard drives and used passwords to prevent others from accessing their laptops. Finally, and perhaps most importantly, the court noted there was no "clear and unambiguous policy to monitor, search or police the teachers' use of their laptops."

That having been said, the court found the teacher's privacy interest was subject to the limited right of access by the school's technicians performing work-related functions. According to the court, the teacher had no expectation of privacy with respect to this limited type of access.

Based on this finding and in consideration of the school board's statutory obligations under the Ontario Education Act to ensure a safe school environment, the court determined neither

Continued on page 5

CASE IN POINT: PRIVACY

Owner of equipment is not the only privacy interest

...continued from page 4

the technician, principal, nor school board, had violated the teacher's charter rights as they concern search and seizure. However, the same could not be said for the police investigation. The court found the warrantless police search and seizure of the laptop and the additional disk containing the temporary internet files breached the teacher's privacy rights under the charter. In this regard, the court went so far as to specifically note the teacher had "a privacy interest in his personal Internet browsing history and what it revealed about his personal predilections and choices."

Lessons for employers

As *R. v. Cole* demonstrates, employers should not assume that since they own the equipment, the only privacy interest in play is their own. As the Ontario Court of Appeal has confirmed, there may be legitimate, competing interests which should be defined in a "clear and unambiguous" information technology (IT) use policy.

A carefully crafted IT policy should outline an employer's right and ability to monitor an employee's computer, cell phone, or other electronic device provided by the employer and put employees on notice of the fact that they should have no expectation of privacy when using company IT equipment and systems.

The specific content and implementation of the policy will depend on the work environment. In most non-unionized workplaces, an employer will be able to unilaterally implement an IT use policy. In that case, courts would be expected to uphold and enforce it provided it is reasonable, employees have received sufficient notice of its implementation and implementation would not be so significant as to constitute a change to a fundamental term of employment.

In a unionized workplace, the provisions of an existing collective agreement may place additional obligations on an employer, such as a requirement to consult, or reach an agreement, with the union prior to implementation. It should also be noted that a majority of arbitrators have already recognized the existence of a "reasonable expectation" of privacy on the part of employees which must be "balanced" against the employer's legitimate interests in managing the workplace.

Regardless of the nature of the work environment, every employer should consider these tips in drafting and implementing an IT use policy:

- **Explain the purpose** —– Employers, especially those in Canadian jurisdictions subject to comprehensive privacy legislation, should explain to employees the rationale behind the policy. This is also important in ensuring employee buy-in and acceptance.
- **Explain how the policy will apply** — Spell out for employees what types of technology and what specific IT applications will be covered, how the policy will apply, when it will take effect, the use that may be made of any information collected, and the potential consequences for a breach of the policy.
- **Ensure sufficient notice** — This means more than just posting a copy of the policy in the lunchroom. Ideally, to ensure enforceability, each employee should not only personally receive a copy of the policy but also confirm she has read, understood and agrees to be bound by it.
- **Confirm there should be "no expectation of privacy"** — Any IT use policy should confirm the IT equipment at issue belongs to the employer and employees should have no expectation of privacy as it relates to its use.
- **Provide clear guidance on acceptable personal use** — Where personal use of IT equipment is to be permitted, an employer should specifically set out in the IT policy what types of personal use might be acceptable and what is off-limits.
- **Ensure consistent enforcement** — If an employer fails to consistently enforce an IT use policy or turn a blind eye to misconduct, it will become much harder for IT policy-related discipline to "stick" in the future.
- **Obtain legal advice** — While it is important to have an IT use policy, it is even more important the policy be done right. Before implementing a policy, consult with experienced counsel to assist you to better understand your rights and obligations as an employer. CELT

ABOUT THE AUTHOR

Adrian Jakibchuk

Adrian Jakibchuk is a lawyer with Sherrard Kuzz LLP, a management-side employment and labour law firm in Toronto. He can be reached at (416) 603-0700 (Main), (416) 420-0738 (24 Hour) or by visiting www.sherrardkuzz.com.

Employment law blog

Canadian Employment Law Today invites you to check out its employment law blog. Recent topics include the effectiveness of health and safety fines, working from home, what employees can say on social media sites, appropriate job interview conversation and employee privacy on company computers.

You can get to the blog by visiting www.employmentlawtoday.com and clicking on the employment law blog banner.