BULLETIN
The HR Space

FASKEN MARTINEAU
www.fasken.com

March 24, 2011

Special Bulletin - Workplace Computer Pornography Ruling: Police Need Search Warrant; Employer Has Latitude

By: Maria Giagilitsis and Brian Smeenk | Toronto

In a decision released this week, the Ontario Court of Appeal issued a surprising ruling affecting privacy rights in the workplace. The case, *R. v. Cole* (PDF), involved criminal charges against a teacher involving possession of child pornography. The court said the employee has a reasonable expectation of privacy regarding the contents of his workplace computer. This meant that he was protected against computer searches by the police absent a search warrant. The employer was given more latitude, but not free reign. While this decision certainly muddies the waters, it may not be as damaging as first appears for employers' ability to control how their computer equipment is used.

Until now, the general rule was that personal information stored by employees on workplace computers would be treated as the employer's property, with full access by the employer. Employers could clearly investigate suspected mis-use of equipment, and take action against employees who violated their policies. It was assumed that this might include handing over to the police material that might lead to criminal charges. But in this week's decision, the employee's reasonable expectation of privacy meant that prosecutors will be unable to use many of the images police obtained from the workplace computer, at the teacher's criminal trial. However, the Court said that different considerations apply to employers. This raises new questions about what employers can do to ensure their equipment is not mis-used by employees.

The Basic Facts

A Sudbury high school teacher was provided a laptop by his school. He used the laptop to teach communication technology. He was also responsible for supervising a laptop program for students.

The teacher had the authority to remotely access data stored on the students' laptops. He did this regularly. While reviewing one student's computer files, he discovered nude photos of another student. The teacher copied the nude photos onto the hard drive of his (school-issued) laptop, rather than reporting the incident.

The school's computer technician discovered the nude photos in a 'hidden' folder on the teacher's computer. He found them while doing a routine data scan. Upon identifying the girl as a student, the technician notified the principal. The principal instructed him to copy the images, along with the teacher's internet surfing history, onto a disc. That surfing history included a large number of pornographic sites. The employer gave that, along with the nude photos, to the police. The police viewed both the disc and the laptop without a warrant.

The teacher was charged with possession of child pornography and criminal use of computer systems. In court, the teacher's lawyer argued that the teacher had a reasonable expectation of privacy in the contents of his laptop. The issue was appealed to Ontario's highest court.

Interesting Twists

The Court of Appeal emphasized that the teacher had exclusive use of the laptop and that the laptop was protected by a personal password. The Court also noted that teachers were generally permitted personal use of school computers.

But the evidence also was that the school's Policy and Procedures Manual prohibited having sexually explicit content on school computers. The Manual also said that all data and messages are considered the property of the school board. The Manual further advised teachers that the school would access private emails if inappropriate use is suspected. And users were advised that they should not assume that files stored on the network or hardrives were private.

The Court of Appeal Decision

The Court found that the teacher did have a reasonable expectation of privacy in the contents of his laptop, at least vis a vis the police. The police therefore violated the teacher's right against unreasonable search and seizure under the *Charter of Rights and Freedoms* when they seized the laptop and searched it without a warrant.

The Court looked beyond the strict wording of the school's computer use policies. It focused instead on the actual practice and customs of the workplace. While the policy was that computers were meant to be used for business purposes, staff routinely used computers to store intimately personal information, such as financial and banking data. All the circumstances satisfied the Court that the teacher had a reasonable expectation of privacy in the contents of his laptop. This gave him protection against police seizures and searches.

The Court, however, gave the employer more leeway than it gave police. Although the Court assumed that the *Charter* could apply to the school board [note that this is contentious – the *Charter* does not apply to most employers], it found that the employer did not violate the teacher's *Charter* rights. The employer did not act improperly when it accessed the teacher's laptop and copied the photos to disc. The employer found these photos while performing normal computer maintenance – an activity that the Court acknowledged was within the employer's right to carry out on its own equipment.

Similarly, the teacher's principal acted properly in viewing some of the images found by the technician, directing him to copy the photographs onto a disc, and requiring the teacher to hand over the laptop. Even though this was a "search and seizure", it was consistent with the principal's duty to ensure the health and safety of students. The principal could not be held to the same standard as the police.

As for the employer itself, the school board, it did not violate the teacher's *Charter* rights either. This, even though it searched the laptop and secured further evidence regarding the teacher's computer and internet use before handing it over to the police. The search and the preservation of evidence for internal discipline procedure was in accordance with the employer's obligation to ensure a safe and secure environment for its students.

Quick Assessment

This case will be analyzed and commented upon by many. An early assessment is that it may not be as bad for employers as first appears.

First, it must be emphasized that the expectation of privacy only operated against the police's search and seizure in this case. Secondly, note that this decision was based on *Charter* rights. Those rights do not apply to most employment relationships. Certainly not those in the private sector.

One might argue that the Court's decision places individual privacy rights over other rights. This might be true with respect to police searches and seizures. However, the decision supports employers who maintain well drafted policies that make it clear the employee has no privacy rights on the employer's computers. It also favours employers who actively maintain, monitor and enforce their own computer use policies.

The decision acknowledges that employers may access data stored by employees on workplace computers in appropriate circumstances. It also acknowledges that such data can be used in internal investigations and later disciplinary proceedings. This is clearly the case with respect to situations that are found as a result of regular monitoring and maintenance.

The decision highlights the importance of well-written computer use policies. It also highlights the importance of ensuring that workplace practices are consistent with those policies.

For more information on the subject of this bulletin, please contact the authors:

Maria Giagilitsis
416 868 3544
mgiagilitsis@fasken.com

Brian P. Smeenk
416 868 3438
bsmeenk@fasken.com

FASKEN MARTINEAU
www.fasken.com

Contacts

VANCOUVER

Kevin P. O'Neill
604 631 3147
koneill@fasken.com

Charles G. Harrison
604 631 3132
charrison@fasken.com

CALGARY

Katie Clayton
403 261 5376
kclayton@fasken.com

TORONTO

Karen M. Sargeant
416 868 3475
ksargeant@fasken.com

Brian P. Smeenk
416 868 3438
bsmeenk@fasken.com

OTTAWA

Stephen B. Acker
613 236 3882
sacker@fasken.com

OTTAWA / MONTRÉAL

Dominique Monet
514 397 7425
dmonet@fasken.com

MONTRÉAL

Dominique Launay
514 397 5240
dlaunay@fasken.com

QUÉBEC CITY

Jasmin Marcotte
418 640 2030
jmarcotte@fasken.com

LONDON

Cerys Williams
+ 44 207 917 8955
cwilliams@fasken.co.uk

PARIS

Judith Beckhard-Cardoso
+33 1 44 94 96 98
jbeckhard@fasken.com