FTR Now

Court of Appeal Recognizes Employee Privacy Rights in Work Computer Subject to Employer Policy and Procedure

Date: March 29, 2011

One week ago, the Ontario Court of Appeal issued a judgement that is very significant for its consideration of an employee's expectation of privacy in personal information stored on a work computer. In *R. v. Cole*, the Court recognized an expectation of privacy in the specific circumstances of the case, but also demonstrated a willingness to allow employers to govern system information, and impliedly restrict employees' expectations of privacy, through clearly articulated policy and procedure. In this *FTR Now*, we discuss the implications of this decision for employers.

BACKGROUND FACTS

A school board investigated a teacher after noticing he had an abnormally high level of activity between his board-issued laptop and the board's server. A member of the board's IT staff accessed his laptop remotely in order to perform a virus scan and to verify the integrity of the computer system. While performing this administrative work, the IT technician found nude photographs of a 16-year-old Grade 10 student.

The technician took a screen shot of the laptop to preserve a record of what he had found, and reported the matter to the school principal. At the direction of the principal, the technician copied the screen shot that he had taken, along with copies of the photographs, onto a disc for preservation. Soon after, the board obtained the laptop from the teacher (who refused to provide his password), and made a copy of the computer's temporary internet files, which were copied onto a second disc.

The board then provided both discs and the laptop computer to the police. The police proceeded to perform a search of the entire computer, and created a mirror image of the complete hard drive. This was all performed without first obtaining a search warrant.

The police charged the teacher with possession of child pornography and unauthorized use of a computer. In his defence, the teacher applied to exclude the evidence based on a breach of his right to be free from unreasonable search and seizure under section 8 of the *Canadian Charter of Rights and Freedoms* ("*Charter*").

REASONABLE EXPECTATION OF PRIVACY

Justice Karakatsanis wrote the decision on behalf of the Court of Appeal. In the course of her analysis, she assumed that the *Charter* applied to the actions of the school board, but did not make a specific finding in this regard (presumably, in part because she found that the board did not violate the *Charter* in any event, as discussed below).

While the board owned the laptop computer and had provided it for a work purpose, the Court of Appeal found the teacher had a reasonable expectation of privacy in the contents of his laptop computer based on the following factors:

- the teacher had exclusive possession of the laptop;
- he had permission to use it for personal use;
- he had permission to take it home on evenings, weekends and summer vacation;
- there was no evidence the board actively monitored teachers' use of laptops; and
- the board did not have a clear and unambiguous policy to monitor, search or otherwise police the teacher's use of his laptop.

This last factor is unique and somewhat limits the significance of the reasonable expectation finding. The board had a computer use policy that contained a warning regarding searches of e-mail communications, but did not contain a similar warning for other information stored on the board's network or on laptop computers. The Court relied on this limitation rather notably, but nonetheless recognized a reduced expectation of privacy based on a general finding about system administrator privileges:

Business and other institutions commonly engage technicians to service and maintain their networks. Users understand that a technician can access computers connected to the network to ensure the integrity of the system.

Because the school board's technician stayed within an "implied right of access" corresponding to this privilege, the Court held that the school board did not violate section 8 by its initial inspection of the laptop. It rejected the defence argument that, without a clear and unambiguous policy authorizing random searches, a government employer must meet either a reasonable and probable ground or reasonable suspicion standard to conduct a search. Instead, the Court suggested that the only question in determining whether a search is properly authorized in the absence of specific authorizing policy language is whether the search is conducted for a purpose consistent with proper systems administration.

The Court of Appeal also found that the board did not violate section 8 of the *Charter* when, upon the direction of the principal, the technician made copies of the screen shot he had created and of the images that he had initially discovered. In coming to this conclusion, the Court upheld the reasonableness of these actions on the basis of the principal's overriding obligation to ensure the health and safety of students in the school. The further search by the school board (when the copy was made of the temporary internet files) was also found to be reasonable.

THE POLICE SEARCHES

In contrast to its findings with respect to the searches performed by the technician, principal and board, the Court of Appeal found that the police search did amount to an unreasonable search and seizure under section 8 of the *Charter*. Key to this finding was the earlier finding that the teacher enjoyed a reasonable expectation of privacy in the contents of the laptop, and that a search of a computer is a highly invasive search. The Court went on to exclude all of the evidence uncovered by the police search, and conditionally excluded the disc containing the copy of the temporary internet files. However, the original screen shot and copies of the images originally discovered by the technician were not excluded, and will be considered by the trial court when the case proceeds to a trial.

LESSONS FOR EMPLOYERS

This case highlights for employers the growing recognition of employee privacy expectations associated with the personal use of employer computer systems. Moreover, the case also highlights that courts and other decision-makers will give legal recognition to those expectations where an employer has created objective conditions that enhance the employees' subjective expectations of privacy. Given that most employers permit some personal use of computers, this trend can be expected to continue.

However, the case does not go so far as to say that employee expectations of privacy are absolute. Even in the absence of a clear policy statement, the Court still limited the privacy expectation to permit routine system administration activities. Moreover, there is a strong suggestion throughout the judgement that employers can shape and limit their employees' expectation of privacy through the articulation and enforcement of a clear computer use policy and procedure that provides to the employer a clear right to monitor and control employee personal content and places clear limits on their employees' privacy interests. Such a policy is especially important if an employer is going to permit reasonable personal use of its IT systems by its employees.

If you would like to discuss the implications of this decision for your organization or would like a lawyer from our firm to assist you to review your organisation's existing computer use policies, please contact Paul Broad at 519.931.5604, Scott Williams

at 416.864.7325, any other member of our firm's Information and Privacy Group or your regular Hicks Morley Lawyer.