

Personal and Ethical Use of Work Computers

December 3, 2012

By John Wilkinson, Albert Formosa

Computers dominate the workplace. And, with increasing use comes increasing computer-related workplace issues. Recent case-law in Canada suggests that employers should be reviewing or instituting a number of policies to address these issues.

Policies for Personal Use

Does your workplace have a policy regarding the personal use of work computers? The recent case of *R. v. Cole* suggests that such a policy should be in place and should address the extent to which an employee can reasonably expect privacy of personal information stored on a work computer. The *Cole* case involved a teacher who stored inappropriate material on his work laptop computer. This material was discovered during a school board check of his saved computer files, and was then the subject of a police search of the computer.

In the Supreme Court of Canada's consideration of the validity of the police search and of the teacher's reasonable expectation of privacy of files on the work computer, the Court determined that a factor (albeit not a determinative factor) to be considered was the existence of a workplace policy regarding employer monitoring of the employee's work computer. The Court provided that workplace policies may diminish an employee's expectation of privacy in the work computer, but that they do not remove them entirely. The employee may still have a reasonable but "diminished" expectation of privacy.

The Court concluded that the totality of the circumstances, including the policies, practices, customs and "operational realities" of the workplace, must be considered in order to determine whether privacy is a reasonable expectation in the particular situation. Accordingly, an employer may wish to review the policies, practices and operational realities regarding personal use of work computers to ensure that they are consistent with the employer's goals.

Intrusion Upon Seclusion

Another recent case has highlighted the need for employers to consider the implementation or review of a 'Code of Conduct' or a 'Systems Use Policy'. Specifically, *Jones v. Tsige* involved a bank employee who, against her employer's 'Code of Business Conduct and Ethics', looked at the banking information for her ex-husband's partner 174 times. In its decision, the Ontario Court of Appeal determined that the employee's surreptitious viewing of that information amounted to a legal wrong which the Court dubbed "intrusion upon seclusion". The Court specifically mentioned the employer's 'Code of Business Conduct and Ethics' and that the employee had admitted that her actions were contrary to it. The Court also noted (as an aside) that the "rogue" employee's actions contrary to the bank's Code might have provided the bank with a complete answer to a complaint made under the federal privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA).

Given these two cases, employers should introduce, or review existing, policies, codes, practices and operational realities concerning both the personal use of work computers and proper and ethical conduct related to work computers and systems. In this context, care

For more information or inquiries:



Toronto
416.947.5010

Email: jwilkinson@weirfoulds.com

John Wilkinson practises corporate and commercial law for universities, not-for-profit organizations, charities, self-regulatory bodies, owner-managed businesses, and associations (including industry associations and sport organizations).



Toronto
416.947.5012

Email:
aformosa@weirfoulds.com

Al Formosa is a litigator with extensive experience dealing with complex commercial litigation.

www.weirfoulds.com

Toronto Office

4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office

1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035