Is A Workplace Computer Private?



Most businesses, and many employees, regularly use computers in the workplace. Often, employers assume that since they own the computer, they own all the information on it. When it comes to information put on a workplace computer by an employee, however, the answer may not be so simple. There were two significant decisions on computer privacy in 2012. Although neither case was an employment law decision, they both have important implications for computers in the workplace.

The first case is *R. v. Cole*. Mr. Cole was a high school teacher who used a laptop issued by the school board. When a technician for the board ran a routine check, he found that there were photographs of a naked student on Mr. Cole's computer. The board seized the computer and searched it, then called the police and gave them the laptop, as well as discs with Mr. Cole's internet browsing history. A long legal battle ensued over whether the police should have obtained a search warrant for the computer. In the end, the Supreme Court of Canada ruled that Mr. Cole had a reasonable expectation of privacy in the computer and the police should have obtained a search warrant.

R. v. Cole was a criminal law case, and the Supreme Court in its decision said it would "leave for another day the finer points of an employer's right to monitor computers issued to employees". Nonetheless, the Court's comments provide some important insights. The Supreme Court looked closely at the workplace policies and practices at the board, which the Court said diminished Mr. Cole's expectation of privacy, including:

- the board's computer policy was up-to-date, and asserted ownership of both the hardware and the information on the computer and network;
- the board reminded the employees every year of the policy; and
- the policy provided that email could be monitored and that "users should NOT assume that files stored on network servers or hard drives of individual computers will be private."

Even with all of these helpful factors, the Supreme Court still concluded that the police should have obtained a search warrant. But that wasn't the school board's problem. The Supreme Court did not have any issue with the *board's* search of the computer. As the employer, the board was within its legal rights to review the contents of the computer's drive.

In a criminal case, the available remedy for an unreasonable search is to throw out the evidence. That doesn't normally happen in employment law cases. What is the

consequence of an unreasonable search? There are a few possibilities. One possibility is a claim for constructive dismissal. If the employer destroys the employee's trust, the employee can quit and demand a severance package. The second possible remedy for an employee comes from another case last year.

The second important computer privacy case from 2012 was *Tsige v. Jones*. In this case, a bank employee, Winnie Tsige, snooped the bank records of Sandra Jones, one of the bank's customers. Ms. Tsige was in a relationship with Ms. Jones' former common law husband. She wanted to know if Ms. Jones' ex-husband – now Ms. Tsige's partner – was really paying child support to Ms. Jones like he said he was. So, she looked at Ms. Jones' bank account 174 times over 4 years. When Ms. Jones found out, she was understandably upset. Although the bank suspended Ms. Tsige for a week, that didn't do anything to help Ms. Jones. She sued for damages.

The Ontario Court of Appeal ultimately decided to recognize a new cause of action for cases like this, called "intrusion upon seclusion". The Court identified three required elements for this new claim: (1) the defendant's conduct must be intentional (which includes recklessness); (2) the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and (3) a reasonable person must regard the invasion as highly offensive, causing distress, humiliation or anguish. The Court specifically stated that no loss of money was necessary. The Court suggested that ordinarily damages would not exceed $20,000 in such cases, and it awarded Ms. Jones $10,000.

In the wake of *R. v. Cole* and *Tsige v. Jones*, employees – and recently terminated employees – have already begun to assert that employer searches of their workplace computers are an "intrusion upon seclusion". How can an employer monitor and search the computers that it puts in the hands of its employees? The key is to manage expectations. Employers can minimize their employees' expectation of privacy in their workplace computers by considering the follow

- Adopt a proper computer use policy, outlining what employees are allowed to do and the monitoring and searching the employer may do;
- Ensure the policy is signed by the employees and they are regularly reminded of it; and
- Implement the policy and follow through so that the reality of how employees use their computers and how the employer monitors that use matches the policy.