November 2017

Prying Eyes: Risk of Employee 'Snooping' and How to Reduce it

Privacy is an area of increased focus for many companies, given the media attention and class action lawsuits that can arise from significant privacy breaches. Although many companies focus their attention on preventing data breaches from malicious outsiders, such as hackers, organizations also have a duty to protect the information that they process and store from unauthorized access, use and disclosures by their own employees.

Such obligations arise under the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and substantially similar provincial legislation in Alberta, British Columbia and Quebec. Some health sector employers may also have obligations under provincial personal health information legislation across Canada.

For example, under PIPEDA, organizations must implement physical, organizational and technological safeguards to protect personal information, which must be appropriate based upon the sensitivity of the information. Organizational safeguards include limiting access to personal information on a "need to know" basis, and providing appropriate privacy training to employees.

In addition to statutory obligations, employers that condone or do not take steps to protect against privacy breaches by their employees could potentially be held vicariously liable under the common law for the improper actions of such employees.

In 2012, the Court of Appeal for Ontario in *Jones v. Tsige* 2012 ONCA 32 recognized a new tort of "intrusion upon seclusion," pursuant to which an individual can claim damages on the basis of a person intentionally or recklessly intruding upon the individual's private affairs or concerns, if the invasion would be highly offensive to a reasonable person.

The risks associated with employers failing to take steps to address employee "snooping" (i.e., accessing personal information held by the organization without a reasonable business purpose for doing so), are illustrated by two class action lawsuits filed in Ontario in recent years.

First, in *Hopkins v. Kay* 2015 ONCA 112, hospital employees accessed hundreds of patient medical records without any legitimate work-related reason. The Court of Appeal for Ontario allowed a class action to proceed against the employer (the Peterborough Regional Health Centre) despite the fact that the Information and Privacy Commissioner of Ontario had already investigated the matter as a breach of the Ontario *Personal Health Information Protection Act*, 2004 (SO 2004, c 3, Sch A).

Second, in *Evans v. Wilson* 2014 ONSC 2135, the court held that there was a sufficient basis to permit a class action to proceed against the employer for the unlawful activities of its employee. In this case, the employee stole information about the Bank of Nova Scotia's customers and gave it to his girlfriend who then sold that information to third parties for fraudulent purposes.

The Bank of Nova Scotia eventually settled the case on the basis that it would pay $1,155,000 in damages, to be divided among the approximately 165 plaintiffs who suffered identity theft as a result of the employee's misconduct, and $444,000 in legal fees to the plaintiffs' counsel.

In addition to the risks of non-compliance with applicable legislation and/or being held vicariously liable for tortious actions of employees, employers whose employees wrongfully access, use or disclose private third party information run the risk of having their reputations tarnished. Individuals, including customers, increasingly

expect that organizations will protect the data that they collect or process, and may be less likely to do business with a company that does not take appropriate steps to prevent both internal and external privacy breaches.

To reduce the risk of employee snooping, and show due diligence in the event that the employer's practices are scrutinized (e.g., in the context of litigation or an investigation by the applicable privacy commissioner), employers must take active steps to limit unauthorized access to personal information and train employees on appropriate information handling practices. In this regard, the Office of the Privacy Commissioner of Canada has set out these helpful tips for preventing employee snooping:

Educate

- Foster a culture of privacy, including by having clear and comprehensive policies and procedures for handling personal information as well as a proactive and empowered privacy officer;
- Have periodic and/or "just in time" training and reminders of privacy and anti-snooping policies;
- Ensure employees know that policies will be enforced and breaches will have consequences.

Protect

- Ensure each employee's access is restricted to information that s/he requires to perform authorized job duties;
- Allow individuals to block specific employees from accessing their personal information, where there is a reasonable basis for doing so;
- Have access logs and/or other oversight tools.

Monitor

- Proactively monitor and/or audit access logs and other oversight tools;
- Understand “normal” access, to better detect inappropriate access.

Respond

- Investigate all snooping reports;
- Respond where proactive measures fail, including by imposing appropriate disciplinary action up to and including termination of employment for cause in the event of serious misconduct.

Following the OPC’s recommended steps will not guarantee protection against employee snooping. However, by having clear and understood policies, and acting swiftly to respond to any breach, an employer can show evidence that the employee’s activities were not done in the “ordinary course” of his/her job, which can reduce the risk of successful vicarious liability claims.

by Lyndsay Wasser and Kyle Lambert

This article originally appeared at the Lawyer’s Daily and has been reprinted with permission.

For more information on this topic, please contact:

Toronto	Lyndsay Wasser	416.865.7083	lyndsay.wasser@mcmillan.ca
Ottawa	Kyle Lambert	613.691.6117	kyle.lambert@mcmillan.ca