

Feature

Employee Privacy Breach: A Quick Glance Can Lead to Just Cause

Privacy breaches and proactive steps for employers

With technology developing as it has, being able to dig into someone's personal information can be as easy as a click of a button. We have celebrity pictures being hacked from the Cloud and customer credit card numbers stolen over the internet. But not all breaches are so public, nor do they require high tech hacker ability. One employee can breach the privacy of another and a termination for just cause can be upheld if the employer has taken the right proactive steps.

In *Steel v. Coast Capital Savings Credit Union*, (2013 BCSC 527) an IT employee at the credit union accessed a confidential document in another employee's personal folder without permission. Normally access was restricted to the employee assigned to the folder, but as IT Ms. Steel had access in case there were ever any technical difficulties. Even then, there was a protocol she had to follow to access it.

In addition to the protocol for access, there were also policies in place regarding access to information that were regularly brought to the attention of Ms. Steel. Her job description stated she had to "Respect the privacy and confidentiality of all customer and staff information at all times."

Despite her 20 years of service to the employer, the Court upheld her termination for just cause. This case, instead of showing what the employer did wrong, enforced what the employer did right. As an employer, be proactive when it comes to privacy matters in the workplace.

1. Ensure you have policies and procedures in place regarding privacy and access to personal documents.

Clear, concise policies that outline the seriousness of a breach of privacy and examples of what constitutes a breach of privacy are key. Do not rely on just common sense. Be explicit. Be clear. Be definite. Ensure you have a protocol in place like the credit union for employees who by the nature of their position have access to the personal information of other employees. State in the policy that privacy breaches can or will result in discipline up to and including termination of employment.

2. An unknown policy is no policy at all

A policy only has weight if an employee knows of it. Do not rely on an employee reading a privacy policy in a binder of policies on their own time after hire. Bring it specifically to their attention. Have them sign off that they have read it. Reaffirm their review and signature at yearly performance reviews like the employer did here. It does not have to be administratively burdensome. If the policy hasn't changed, have them sign the same one each year with the date beside it.



*Sarah Manning
Senior Associate
Lawyer
Taylor MacLellan
Cochrane*

Members Quarterly

Spring 2015 Edition

Feature

3. Follow the policy in place

A policy applied arbitrarily loses its strength and weakens your ability to rely on it to support strong disciplinary action. The point of a policy is that an employee knows the employer's expectations. If the expectations are applied differently depending on the employee, then will the next employee really know what is expected of him or her? If you are consistent with its application for similar behaviour similar consequence it can weaken a claim against you that this was personal, or unfair. If there are extenuating circumstances to warrant treating a situation differently, make sure to note why so you can defend it later if challenged.

4. State it in the job description

Put privacy expectations in the job description. Don't just limit it to employees in confidential positions. An employee can come across private information of another employee in a number of ways. For example, a janitor cleaning an office or an employee dropping something off sees confidential information on the desk. Employees working in an industry where trust, privacy and confidentiality are key will be held to a higher standard and a termination for just cause will be easier to support. This does not mean however that discipline will not be upheld for breaches of employee privacy in other types of workplace.

Follow these proactive steps and most importantly, ensure that every single employee regardless of their position is aware of them and reviewing them on a regular basis. Employees will think twice about peeking into files and documents knowing that this could now lead to termination.

*Sarah Manning is a Senior Associate Lawyer with
Taylor MacLellan Cochrane and can be reached via email at manning@tmclaw.com.*