



Is your employer monitoring your Net use?

Monday, March 7th, 2005

On the cutting edge - Brian T. D. Bowman

YOU are at work today and decide to send a personal e-mail to your spouse about how you are upset at your boss for not giving you a well-earned raise. You then do some Internet surfing for available job postings on a competitor's website.

Did you know your boss might be reading your e-mail and viewing your Internet activities? More importantly, did you know it may be perfectly legal for your boss to do so?

Too many employees are either naive or in denial about whether their boss has the right or capability to monitor their e-mail and Internet activities. Employee monitoring is much more common than you may think.

So, why would an employer want to monitor his or her employees?

According to a 2003 Ipsos-Reid study, Canadian employees spend 4.5 hours a week surfing the Internet for personal reasons. For an organization with, say, 20 employees that each work 50 weeks a year, that amounts to 4,500 hours of lost productivity annually. The employer might as well hire only 18 employees, because 4,500 hours is more than the number of hours that two employees will typically work in a year.

In certain circumstances, employers have legitimate reasons to monitor their employees' e-mail and Internet activities. Workplace productivity is one obvious reason. Employees who spend time at work surfing the Internet to shop, read e-mail jokes or play games do not contribute to the employer's bottom line. But there are many other circumstances where employers may face adverse business or even legal repercussions for the e-mail and Internet activities of their employees. Employers may be liable when their employees violate someone else's privacy. For example, if an employee distributes a customer's personal information or e-mail message without consent, that customer's privacy may be violated. In fact, forwarding a customer's, or other third party's e-mail message without consent may amount to copyright infringement under Canada's Copyright Act.

Employees' distribution of derogatory comments or inappropriate jokes of a sexual, racial or other nature via e-mail is another common source of employer liability, which in Manitoba could give rise to employee and employer liability under The Human Rights Code. By deriding a fellow employee or customer in an e-mail, an employee and their employer could also be exposed to liability for defamation.

Too often, disgruntled employees leak to competitors or other third parties the employer's confidential commercial information. With just a few clicks of a mouse a competitor may

have access to sensitive company data, with devastating impacts to the employer's business.

In most cases, however, employees do not intentionally try to embarrass or hurt their employer's business. Nonetheless, it is all too easy to make mistakes when sending e-mail or surfing the Internet. Reading the news on a daily basis will provide repeated examples of situations where employees have embarrassed or subjected themselves and their employers to liability.

Sending e-mail messages from a work e-mail address is comparable to sending letters on your employer's letterhead. Correspondences that originate from a workplace -- whether in electronic or paper form -- have the ability to tarnish the reputation of the employer and expose it to liability.

But wholesale monitoring of all employees' Internet and e-mail activities is not the answer. Employees have legitimate rights to their privacy. New privacy laws and heightened sensitivities regarding privacy should necessitate openness and transparency in the workplace. Employers should balance the interests of their employees' right to privacy and their need to be protected from liability with the implementation of thorough computer-use policies and privacy policies. Such policies provide the ground rules for Internet and e-mail use by employees and monitoring by employers.

If you do not know whether your boss is reading your e-mails or viewing your Internet activities, you should find out. And, if you are a boss who does not have a computer-use policy and privacy policy, you should think twice before acting like Big Brother.

Brian T. D. Bowman is a lawyer with the privacy law group of PITBLADO LLP, Barristers & Solicitors. He can be reached at (204) 956-3520 or via bowman@pitblado.com

© 2005 Winnipeg Free Press. All Rights Reserved.