The Reciprocal
Insurance, Financial & Business Solutions
April 2016

Electronic Devices & Employee Privacy Expectations

The prevalence of ***continuous connectivity*** has created an environment where your employees need internet access, not only for business purposes, but for personal reasons as well. Internet access through the company internet connection is often made possible via both company-owned and employee-owned computers, tablets and/or cell phones. Whether employees are using corporate electronic devices, or their own devices through the company network, the company has a role to play in relation to personal information, content and data collection. As a company, decisions need to be made regarding personal usage of company equipment and to what extent it is allowable. ***Do you monitor or track personal usage or content? What right to privacy do your employees expect?***

One of the basic principles of employment law in Canada is that employees have a ***reasonable expectation of privacy*** in the workplace as it relates to matters which are personal to an employee. This expectation of privacy includes written records and data created through the use of electronic equipment supplied by the company. On the other hand, companies have the right through the terms of a contract, to place limitations on an employee's privacy as long as these limitations are considered "reasonable."[1]

An employee's expectation of privacy generally arises out of two factors:

1. The employee must themselves expect privacy at some level (usually demonstrated by their actions to keep the information private).
2. The expectation of privacy must be reasonable. Recent court cases have highlighted this issue.[2]

To ensure the privacy needs of the company and the employee are both met, your company's corporate policies and procedures play a large role. Some policies which may help address employee privacy expectations include: ***Personnel Privacy Policy***, ***Email Use Policy*** and ***Internet Use Policy***. Each of these corporate policies needs to clearly specify the collection, use, accessibility and disclosure of an employee's personal information, particularly if it is being stored on company-provided electronic devices.

Regardless of the type of program, equipment or intended use of the information by the company, it is important that there be ***a clear, written corporate policy***. Each policy should be ***reviewed by legal counsel*** to ensure compliance with all applicable employment laws and standards.

Your corporate policy should also:

1. Describe the intended use of data
2. Outline the expectations of privacy employees can have
3. Require employee signoff indicating acknowledgment that the employee has read, understood and agrees to abide by the company policy

See over…

If your company plans to monitor employees' personal use of company-supplied email, internet or electronic equipment usage, ***it's best to obtain written consent from the employee through the corporate policies***. Corporate policy must be very clear, letting employees know the company has the right to monitor personal emails and personal internet use of any company-provided electronic devices.

Each policy should address potential privacy expectations employees might have related to this equipment. If, based on the company's policy, employees are to have no expectation of privacy when using company-provided equipment or networks, ***the policy must be very clear and unambiguous***. To implement the policy, any new employees would be required to sign an individual policy indicating they have read, understood and agree to abide by the terms. For existing employees, it may be a matter of agreement to the new policies with language that suggests "…your continuation of employment indicates your acceptance and agreement to abide by these various policies."

There are other types of electronic devices that may be implemented by employers specifically for the purpose of data collection for business optimization. In these cases, how can an employer "monitor" employees and not breach the employee's right to privacy?

For example, a GPS system installed in your vehicles provides a window into the operation of your fleet. In addition to vehicle location tracking, it is possible to monitor speed, starts/stops, idling and overall vehicle performance. By encouraging changes to driving habits, it may be possible to save money and reduce operating costs. However, to make employees comfortable with this data tracking, ***it is important your employees are aware of why data is being collected and how it will be used***. With the intention of improving fleet operations and cost reduction, it may not be problematic. However, some employees could view this data collection exercise as an invasion of privacy.

Many corporate wellness programs employ the use of ***wearables***, such as a fitness tracker wristbands, to encourage healthier exercise patterns. In fact, 40% to 50% of employers with a wellness program use trackers to enhance these programs, according to a recent article in The Wall Street Journal.[3] These devices offer employers ***new ways to measure productivity and safety, and potentially give insurers the ability to track workers' health indicators and habits***. Although there may be positive outcomes from the use of these devices, employees may have issues with this type of personal data collection.

To ensure the needs of the company and employee privacy are met, employers can take steps to remove themselves from the collection process of the data by ***hiring a third-party provider to maintain it and only receive anonymized data themselves***. As well, the company must always be sure it is not breaching the "personal information" of an employee. Employees' personal information (such as banking information, health data, etc.) should not be disclosed or mishandled. This information is protected under the same privacy laws as the general public.

What's next for the workplace? From security systems that include retinal scanning to wearables in the workplace, each raises potential legal and privacy issues. ***Plan now to be ready.*** The use of technology has many benefits, but all within the realm of the expectations for privacy and protection of data.

1 "WeirFoulds LLP Employment Law in Canada."Pg. 28. Fall 2011. Web. April 2016.
2 "Does Monitoring Emails Breach an Employee's Right to Privacy?" MacLeod Law Firm. 25 March 2013. Web. April 2016.
3 "As Wearables in Workplace Spread, So Do Legal Concerns." The Wall Street Journal. 13 March 2016 Web. April 2016.

Gary Durie, *Manager*
Risk Management & Underwriting Services
905.265.5355 | 1.800.668.9979
3700 Steeles Avenue West, Suite 1100
Vaughan, Ontario L4L 8K8
gdurie@mearie.ca | mearie.ca