September 2014

mcmillan Employment and Labour Bulletin

Bring Your Own Device (BYOD) – A Primer for Employers

Introduction

The development of portable technology has dramatically altered the relationship between professional and personal life. On a morning commute to the office, it is not uncommon for an individual to pull out a single smartphone both to read and respond to a client email and confirm dinner plans with a friend over text message. Some individuals on their morning commute pull out a work-issued smartphone and others pull out a personally-purchased device. The focus of this article is on managing the use of personally-purchased devices for professional tasks.

In what follows, we explore the increasingly popular Bring Your Own Device ("BYOD") model that permits employees to use their personally-owned devices to access confidential company systems and information and highlight some key legal issues for employers to consider before implementing a BYOD policy. Specifically, this article addresses ownership of and access to the device, related employment issues, and privacy and data security. The article also considers these issues and proposes solutions for employers to build into their BYOD policies to address the relevant legal concerns. While the BYOD model is attractive, a carefully constructed policy and related management practices are critical to ensuring compliance with data management obligations and to avoid related legal liability.

Property and Access to Device

Payment for Device

If an employee is required to have a device that meets a particular standard of quality there may be a question about whether an employer is obligated to subsidize the cost of that device. Where an employee must use a mobile device in the course of employment, the employer may have to pay for the cost of operating the device. Employers must be aware of any applicable laws in their jurisdiction that may impose obligations on employers to pay for their employees' devices. It is important to clearly address the issue of payment for the device in the BYOD policy.

Ownership

The very nature of the BYOD model is that employees use their own devices. While an employee retains ownership of their cell phone, an employer retains ownership and control of its email system and the professional work product produced on the device. Employers should ensure that the BYOD policy explicitly defines the relationship between the employee, employer, and the device. The policy should specifically address scenarios where the employer requires and is permitted access to the device for legitimate work purposes.

Related Employment Issues

Acceptable Use Policies

While the BYOD model permits employees to perform work tasks on their personal devices, employers have legitimate reasons to order that use of the device complies with certain standards. Organizations have the right to set operational and other standards for the workplace, because an employee's misuse of computer systems to access, receive, or disseminate inappropriate materials could damage the employer's reputation, adversely impact the work environment, diminish productivity, and expose the employer to liability. Despite using their own devices, employees continue to represent the company in their professional interactions using the device. Accordingly, an employer's interest in regulating employee use of personal devices for professional purposes is a legitimate one.

The BYOD policy should set explicit acceptable use guidelines for employees to follow while performing work functions on their personal devices. The acceptable use component of the BYOD policy should be consistent with the company's existing policies.

Overtime Obligations for After-hours Work on Device

An employee who performs work tasks on their personal device has access to the device throughout the day. Employers must consider the possibility that an employee may claim to be entitled to overtime pay for work tasks performed during non-work hours. It is important that employers consider relevant legislation and regulations, and for those who are over-time-eligible, develop a system for tracking their working hours on personal devices.

Employers who wish to limit the number of hours that employees work should include in the BYOD policy restrictions on working during non-work hours. For instance, the BYOD policy may prohibit sending work emails during evenings or weekends. Alternatively, employers could restrict remote access to the company network during non-work hours.

Privacy Issues

Security of Privileged Company Information

While a BYOD model allows an employee to perform work tasks from virtually anywhere, an organization must take steps to ensure the security of privileged and confidential information. Use of a personal device to perform work functions may compromise security in a variety of instances, including access to documents or emails over an unsecured WiFi network, performance of tasks in public, or upon termination of the employment relationship if company data remains on an employee-owned device.

The BYOD policy should be clear with regard to how employees may perform work tasks on their own devices. For instance, a BYOD policy should prohibit accessing the company network through unsecured WiFi connections. The policy should also provide for destruction of work product information on the device upon termination of the working relationship. In certain cases, appropriate transfer of data to the company may be necessary.

Security of company information on an employee's personal device may also be protected by requiring the use of security software through which to access the company network. Such software should require username and password credentials in order to gain access to company documents. This system could prevent third-party access to confidential company information even in the event an employee's device is lost or stolen. A company should keep a list of devices that employees use in order to ensure compatibility with the selected software. If necessary, employers may restrict participation in the BYOD policy to certain devices.

Employee Privacy

While a BYOD model enables an employee to conveniently organize its personal and professional life on a single device, the blending of personal and professional information creates the potential for significant employee privacy concerns. While an employer may have a legitimate reason to access business information on an employee's personal device, an employee may have a concern that an employer will also access its personal information without authorization.

It is important to understand the risk that accessing work data on an employee's device may still result in the collection of personal information for the purposes of *PIPEDA* and similar privacy legislation. In the BYOD model, the distinction between work product information and personal information becomes blurred. A single device that an employee uses professionally and personally is more likely to have work product information and personal information

intermingled. Accordingly, an employer runs a risk of inadvertently collecting personal information while accessing the device for the purpose of collecting work product information. This risk can often be mitigated through an appropriate employee consent.

The BYOD policy should ensure that employees understand the risks of using a single device for both professional and personal use. The policy should therefore inform employees of the various reasons why an employer may collect information from an employee's device and of the possibility that personal information may be made available to the employer. Employees should also be asked to confirm receipt of the BYOD policy and agree to be bound by it.

Conclusions

Portable technology has altered the division between professional and personal life. Organizations are increasingly showing a preference to permit employees to perform work functions on their personal devices. This article surveyed several issues that an employer must consider before implementing such a BYOD program and proposed solutions for employers to follow to mitigate against the risks outlined above. Companies must ensure that they have a clear BYOD policy in place that addresses employment issues, privacy concerns and data security. Implementing such a policy establishes a guideline with which employees must comply. Companies should further examine whether it is appropriate to acquire remote access software in order to strengthen control over the security of company data and employee monitoring. Of course, many of the issues arising from a BYOD program are dependent on the unique circumstances of the organization implementing it and the relevant data being handled. The issues highlighted above therefore are key considerations when an organization develops a BYOD policy customized to business needs.

by George Waggott and Mitch Koczerginski, Student-at-Law

For more information on this topic please contact:

Toronto George Waggott 416.307.4221 george.waggott@mcmillan.ca

a cautionary note