Blaney McMurtry LLP

PUBLICATION

Blurred Lines: Mobile Devices in the Workplace

Date: April 21, 2015
Lawyers You Should Know: Christopher McClelland

Original Newsletter(s) this article was published in: Employment Update: April 2015

As smartphones become increasingly common in the workplace, many employers are recognizing the difficulty of attempting to draw a clear line between a “work device” and a “personal device.” Employers have adapted to this issue in different ways. Some employers permit employees to use their own mobile device to access the employer’s corporate networks and systems (commonly referred to as “Bring Your Own Device” or “BYOD”). Other employers provide employees with mobile devices that contain pre-installed software allowing for the creation of a “personal” profile that is kept separate from the “work” profile. Even in cases where an employer does not specifically address the issue, it is often implicitly recognized that an employee who is carrying a mobile device with them for work purposes will engage in some personal activities on that device, whether that means surfing the internet, checking personal email accounts or using the map function.

The blending of work and personal use on a single device raises a number of employment and privacy related issues. For many employees, their mobile device is one of the primary tools they use to interact with their colleagues and to perform their work. At the same time, personal use of a mobile device will almost inevitably result in the device containing personal information, some of which may be very sensitive. Employers should therefore regularly review their existing policies to ensure that employees have a clear understanding of the employer’s expectations regarding the use of mobile devices. The following is a list of topics that employers may wish to address in their policies:

PERSONAL USE

It is possible for an employer to prohibit any personal use of corporate-owned mobile devices. However, doing so would require that the employer take specific steps to enforce the policy (including by potentially imposing discipline) and do so consistently. In most cases, the employer will permit limited personal use so long as it does not interfere with the employee’s duties and responsibilities or result in the violation of any other policies. In cases where the

employee provides their own personal device the employer retains even less control, making it even more important to have policies in place.

ACCEPTABLE USE

Employers should impose explicit acceptable use guidelines that distinguish between using a mobile device for work purposes and personal purposes.

OFF-THE-CLOCK WORK

Employees that use mobile devices for work are much more likely to review work-related emails and perform work outside of normal office hours. This can create potential difficulties if the employee is eligible for overtime or performs work when they are on a leave of absence. The employer's policies should specifically address these situations.

INFORMATION SECURITY CONCERNS

Employers should provide clear instructions to employees about how they may perform work tasks on their mobile device to ensure that company data, networks and systems are protected. Employers should also explain what will happen to the work information and the personal information on the mobile device if it is lost or stolen (i.e. the employer's IT department may need to reset or wipe the device).

EMPLOYEE PRIVACY

By allowing an employee to use their corporate mobile device for non-work-related purposes, an employer is implicitly acknowledging that an employee has a reasonable expectation of privacy with respect to the personal information contained or stored on the mobile device. It is therefore important for the employer to specifically set out under what circumstances it will monitor or access the information stored on the mobile device.

If the mobile device has a "work profile" and a "personal profile," the presumption is that the employer will not monitor or inspect the information contained or stored within the personal profile. At the same time, the employer should clarify the extent to which it will monitor or inspect the information contained or stored within the work profile, both during and at the end of the employment relationship.

TERMINATION

Employers should clarify what happens to the information contained or stored on the mobile device when employees are terminated or resign their employment. If the mobile device belongs to the employer, the employee may wish to be given an opportunity to back-up or remove any personal information stored within the personal profile. If the mobile device belongs to the employee, the employer will likely want to ensure that it has the ability and the right to access the device in order to remove any work-related information.

Given the myriad of issues that are unique to the use of mobile devices in the workplace, employers may consider developing a stand-alone mobile device policy. Doing so would make it easier for the employer to respond to the changes in technology that are likely to continue blurring the line between work devices and personal devices.