technology

by Ryan Treleaven

MOBILE DEVICE MANAGEMENT

Three important questions your municipality needs to answer

Ask employees the one item they cannot not live without even for a day and they'll likely answer, "my smartphone." Canadians have fallen in love with their mobile devices and, with more than 27 million users, represent the third highest level of smartphone penetration in the world.

Not surprisingly, mobile devices are increasingly used in support of Canadians' personal *and* work lives. A recent study found that more than three quarters of Canadian employers actively support the use of employee-purchased smartphones and tablets in the workplace – a practice known as Bring Your Own Device (BYOD).[1] Unfortunately, the corollary to BYOD is that more corporate data is lost through employee-operated devices in Canada than virtually anywhere else on earth.[2]

This presents an obvious challenge for Canadian municipalities: *how to strike an appropriate balance between the benefits gained by allowing employees to make effective use of their mobile devices, while complying with the legal obligation to protect the private information these employees routinely access.*

The solution to this challenge lies in the implementation of a comprehensive Mobile Device Management Program (MDMP).

Given the rate at which mobile devices have infiltrated the workplace, many employers have struggled to stay ahead of the mobile device management curve. Regardless of your municipality's approach to date, it is important to

[1] Nestor E. Arellano, 05 Apr 2013, "Canadian firms leading world in BYOD: Study," Computing Canada, accessed at <www.itworldcanada.com/article/canadian-firms-leading-world-in-byod-study/47616>.

[2] Nestor E. Arellano, 19 March 2012, "Canada, Italy lead in mobile data loss," IT Business, accessed at <www.itbusiness.ca/news/canada-italy-lead-in-mobile-data-loss/17158>.

RYAN TRELEAVEN is a lawyer with Sherrard Kuzz LLP, one of Canada's leading employment and labour law firms, representing management. Ryan can be reached at 416-603-0700 (main), 416-420-0738 (24-hour), or via <www.sherrardkuzz.com>.

assess the mobile technology needs of your workplace and design an appropriate MDMP. To this end, a municipality will need to answer the following three questions:

1. Whose device is it?

The answer to this question is critical because it impacts the ease with which an employer can protect corporate information, and the scope of an employee's reasonable expectation of privacy over information stored on the mobile device.

Three principal models exist:

- Bring Your Own Device (BYOD);
- Here's Your Own Device (HYOD); and
- Choose Your Own Device (CYOD).

A municipality may choose to implement one or a combination of these three approaches.

BYOD – In a BYOD program, an employee purchases the mobile device of their choosing and contracts directly with the mobile service provider. Mobile data costs can be the responsibility of the employee, municipality, or shared pursuant to an approved formula. The mobile device is used to manage personal affairs as well as organizational data.

While attractive from a short-term cost perspective, a BYOD program gives rise to several security concerns, including control and access to the corporate information that resides on the device. Employee devices run on a multitude of different operating systems, thus the implementation of software security programs can be difficult if not impossible. Furthermore, since the device is owned by the individual employee and used in their personal life, a policy that seeks to restrict the use of the device may be unpopular and difficult to enforce. Bottom line: many Canadian employers have experienced significant data loss and increased malware infections in their networks as a consequence of BYOD programs.

HYOD – In a HYOD program, an employer assigns a specific mobile device to its employee based on the mobile technology requirements of the position. Ownership of the device and mobile service contract rests with the employer. Mobile data costs are paid by the employer, or shared with the employee pursuant to an approved formula. Municipalities employing a HYOD will have significantly more control over how data is accessed and secured, and may achieve greater efficiencies by utilizing software on compatible or homogenous operating systems.

However, this added control comes at the cost of purchasing the mobile devices, and the potential for employees to be frustrated at not being able to utilize their own devices for work purposes. It is also important to remember that even where the employer owns the device, if personal use is permitted, an employee will retain a limited expectation of privacy over the personal information stored within.[3] The scope of this privacy expectation will be informed by the workplace policies and procedures, meaning a municipality's policies, including how and when it will monitor the use of workplace technology, should be well drafted, clearly communicated, and restricted to legitimate business objectives.

CYOD – In a CYOD program, an employee selects a mobile device from an approved list. The ownership of the device and the mobile service contract can be in the name of the employee or employer. Similarly, mobile data costs can be allocated between parties. A CYOD is a flexible option providing employees with a degree of freedom over their mobile devices, while ensuring significant consistency throughout the devices used in the workplace, thereby simplifying the implementation of critical software solutions.

2. What policies are needed to support an MDMP?

Regardless of the approach selected, all municipalities will, to varying degrees, face the same basic challenges posed by personal mobile devices accessing their secured networks. The good news is that these challenges can be effectively managed with appropriate policies and technological solutions. What follows is an outline of some of the relevant MDMP policies to consider. They do not represent an exhaustive list of relevant policies, nor could they, given the rate at which technology is evolving. As with any workplace policy, to be of greatest utility, they should be clearly written and communicated; and, employees should be expressly advised that a violation may result in discipline up to and including termination for cause and/or a civil lawsuit. Ideally, all policies should be acknowledged in writing by employees as having been received, read, and understood:

Acceptable use policy – The undisciplined use of mobile devices is one of the key information security threats facing Canadian employers. A recent study found 45 percent of organizations had at least some employees circumvent or disengage core security features installed on their devices (i.e., passwords or key locks). An acceptable use policy should clearly explain the security procedures pertaining to the use of mobile devices, including when and how those devices will lock and may be connected to secured networks.

Social media policy – Regardless of whether your municipality has an active social media presence, consider the benefits of a social media policy to protect the municipality's brand and manage the risk of liability. Some of the greatest social media blunders of the past year came as a result of employees mistakenly posting comments to the wrong account while using their personal mobile device. (To learn more about the benefits of a social media policy, see "Three Golden Rules of Social Media for Municipalities," published in the March 2014 issue of *Municipal World*.)

Privacy policy – Every municipality has an obligation to protect the personal information it receives in the course of operations, even when that information is located on the mobile devices of its employees. These privacy obligations are complicated by the fact that, in addition to the municipality's own data, mobile devices used for work purposes also contain the individual employees' personal information. An appropriate privacy policy should outline the security measures that will apply to the device and its content, and what information may be monitored or searched by the

[3] *R. v. Cole*, [2012] SCC 53.

municipality and in what circumstances. To the extent that third parties may access information on the municipality's network, steps should be taken to ensure these parties adhere to the same privacy standards.

Lost or stolen device/surrendering device policy – There should be a clear protocol for reporting lost or stolen mobile devices. Most MDM software suites include a remote data wiping feature. Employees should be advised that, in the case of a lost or stolen device, all data (both personal and work-related) may be wiped remotely. The policy should also detail the employee's obligation to temporarily surrender their mobile device in specific circumstances for data retrieval or deletion. This may be necessary to support litigation discovery obligations, workplace investigations, or upon an employee's resignation or termination.

Data classification policy – There may be certain classifications of data for which the consequences of unintended disclosure are so severe they should never be accessed through mobile devices. That type of information must be identified with precision and communicated clearly to employees.

Camera phone use policy – Virtually every smartphone has video and picture capabilities. There should be a policy governing when, and in what contexts, this technology may be used in connection with work. These restrictions can be enforced through the use of existing technologies.

3. What technology solutions are needed to support an MDMP?

Software developers have been diligently working to provide technical solutions to the various issues employers encounter as a consequence of their employees' use of mobile devices. Virtually all devices provide standard security features such as password protection, encryption for wifi and remote access, device lock, and remote wiping.

Some advanced features are also available to address the more specific issues outlined above. For example, "ring-fencing" and "sandboxing" act to segregate a mobile device's data into personal and business categories, making monitoring or searching easier to navigate. There are also software tools to prevent employees from streaming, downloading information, and installing applications that present malware risks. These software suites range in price and ease of use and should be thoroughly investigated with your IT department.

Parting Thoughts

Implementing a comprehensive MDMP is a significant undertaking; but, given the increasingly important role of mobile devices in the workplace, and the potential consequences of undisciplined use, it is an undertaking of great importance. If your municipality turns its minds to the three questions outlined above, it should be well on its way to establishing an effective MDMP. MW

This article is for general information purposes only and does not constitute legal or other professional advice.