by Lou Milrad

# MOBILE DEVICES & YOUR MUNICIPALITY

## Avoiding Downstream Liability

It's become increasingly common for municipal staff, particularly those requiring secure access to municipal servers, to sport at least one, and in some instances, two or more mobile devices. At a recent municipal consultation, an informal "show of hands" poll evidenced that six of the 10 attendees present each sported an institutionally-issued Blackberry together with a personally acquired iPhone, Android, or Windows smartphone for their own personal and private use. The six also enjoyed restricted access to business unit info through a municipally-furnished iPad or Windows tablet. The other four in attendance unanimously agreed that their institutionally-provided Blackberries were more than adequate for their respective municipal functions, which included information gathering and uploading to municipal servers, work related emails, and texting. None of the four had any pressing desire to exchange personal emails from those devices, nor any desire to access any of their friends' Facebook postings while at work; and, as far as tweeting, they'd prefer to leave that to the elected officials!

This demographic shift of combining workplace and personal use onto a single device, particularly prevalent among younger people, is commonly referred to as the consumerization of IT. A recent *Forbes* survey concluded that, in the U.S., the number of employees that are now carrying multiple portable devices daily amounts to 3.5 devices on average.[1] *Employees want their business data available on all these devices all the time.*[2]

This evolving trend that allows employees to connect to institutional network servers through their own personally owned, or organizationally provided (or subsidized) devices has become known principally as Bring-Your-Own-Device (BYOD) – along with a host of variants such as Bring-Your-Own-Computer (BYOC), Here-Is Your-Own-Device (HYOD), Bring-Your-Own-Information (BYOI), etc.

While there are a number of contributing factors driving this trend, it is the "evolution of cloud and virtualization technologies"[3] that has shifted us into high gear, while at the same time trying to better understand and assess the impact of this evolution on privacy, security, and separation of workplace from home and family life. And, what effect will current and evolving technologies (such as wearable devices like Google Glass, smart watches, and intelligent bracelets) have on what we understand to have been carefully thought out and implemented (or about-to-be implemented) mobility policies?

### BYOD Strategy vs. BYOD Policy

BYOD introduces a mix of security, privacy, intellectual property, database and software licensing, and employment law challenges that need to be carefully considered.

Minimizing legal risk and its allocation between and amongst the municipality, its employees, and third parties needs to be addressed as part of the overall BYOD strategy. The strategy then needs to be reflected in the design and implementation of the municipality's detailed BYOD policy (it is the policy that sets out the terms of the program). Much of the policy may not, directly, spell out the underlying legal concerns within the actual language of the document, and that needs to be clear and concise and in plain English (hence as a best practice). In parallel, educating employees on the underlying deliberations to assist in reducing legal exposure, is critical.

The policy needs to cover matters such as the type of devices that can



**LOU MILRAD** is a business and IT lawyer who assists municipalities and private sector clients with technology licensing, mobility strategies and policies, IT procurement, commercialization, cloud computing, open data, and public-private alliances. Lou is Associate General Counsel to IMLA in Canada (International Municipal Lawyers Association) and a frequent presenter on technology law relative to government. He can be reached at 647-982-7890, <lou@milrad.ca>, or via <www.milradlaw.ca>.

1 <www.forbes.com/sites/sap/2012/05/11/average-mobile-worker-carries-3-5-devices-heres-the-downside>.

2 Whitepaper: BYOD File Sharing - Go Private Cloud to Mitigate Data Risks <www.accellion.com/sites/default/files/wp_Accellion10BYOD.pdf>.

3 BYOD (Bring Your Own Device) Is Your Organization Ready? <www.ipc.on.ca/site_documents/pbd-byod.pdf> p. 2.

be used by employees, access rights, support arrangements, tracking and monitoring, remote wiping, prohibitions against visiting or downloading from unauthorized websites, and precluding use of the device by family and friends, etc. Differentiation between the employee's private and personal data access rights and those of the municipality will need to be clearly expressed, as will support arrangements and attendant reciprocal obligations on termination of employment.

Hence, the necessity to create a program that introduces a phased rollout for "empowered" workers. Of course, none of this happens overnight; but, it is necessary to remain mindful of a variety of implementation and policy challenges.

## BYOD Policy Considerations

A time-sensitive, engaging, and tedious process of information gathering, consultation, evaluation, and decision making must first be undertaken before a finalized policy can be developed, launched, and signed off on by employees. Employee education and training must also be factored into the plan. Provision for periodic updates of that policy will need to be made in recognition of potential unintended impacts on the municipality's risk profile (as, for example, in circumstances where prevailing circumstances result in a realizable threat or a wrongful action that was not contemplated at the time of drafting the policy).

The BYOD policy will need to align with the municipality's employment policy, as well as with any existing IT "acceptable use" policy.

Municipalities have a legal obligation to safeguard that body of highly sensitive information required by statute, contract, or policy to be maintained as confidential and non-public. This obligation applies regardless of information residing in either paper or digital format. Under BYOD, the device holder, through the device, is authorized to access and receive specified data sets – but inadvertently (or, quite possibly, intentionally or nefariously) might choose to store that data in the device's internal memory (currently ranging from 16 to 128 Gigabytes and likely to be measured in Terabytes in the near future), or transfer the data to some unauthorized and encrypted, password-unknown, external network or cloud location.

## Devices as Intrusive Access Points

The device itself is a fully equipped access point to a host of authorized and unauthorized storage facilities (e.g., the municipality's servers, the cloud, external networks, computers, etc.), and in itself can be an exceptionally dangerous weapon that can circumvent the best laid strategy and plan. The municipality's IT and data governance structure must ensure a strict and absolute separation of the municipality's non-public and operational information from the employee's device and access to the employee's personal information and data assets.

Heck, is that really a whole lot different that forwarding internal emails directly to the employee's Gmail or Yahoo account? What about downloading or saving attachments to the employee's home computer or to a public cloud? Yes, these things do happen … quite regularly. How are these to be addressed, if at all, in the policy?

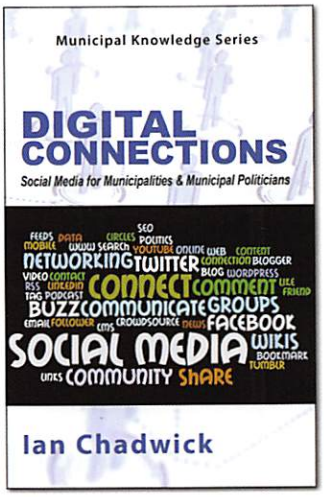
## Conclusion

Prior to engaging upon any particular mobile strategy, it is critical to first evaluate the:

- current adoption and specific uses in conjunction with the projected needs, benefits, and HR;
- cost/benefit analysis of devices within the municipality;
- where and in which departments (and associated boards, agencies, and commissions) they are currently being used and for what purpose(s); and
- whether or not, and to what extent, they might be incorporated into the municipality's mobility strategy.

In addition to the considerations outlined above, it will be important for policies to address some social media usage, while also precluding family members, friends, and colleagues from using the device and accessing municipal data. MW


**SOCIAL MEDIA MUST-HAVE**




**$29.95**

Plus applicable taxes, shipping and handling

Social media: everyone's using it today. Facebook, Twitter, LinkedIn, Google+, blogs, and photo/video sharing sites. These and other services have literally hundreds of millions of users. But what does it mean for your municipality? Or for you as a municipal politician? Is it a potentially huge audience for marketing, business attraction, staff recruitment and even votes? Or is it all hype?

As Ian Chadwick explores in his book, *Digital Connections: Social Media for Municipalities & Municipal Politicians,* social media is both a boon and a minefield for municipalities. For newcomers, this book is a practical guide about where to start. For municipalities already using social media, it offers thought-provoking issues: liability, staff access, compensation, security, and crafting social media policies.

Ian Chadwick is a veteran of 40 years working in and with the media.

**MW BookShop**
***books.municipalworld.com***
***or call 1-888-368-6125***