International Municipal Lawyers Association
2014 Annual Conference
Baltimore, Maryland

September 12, 2014

WORK SESSION VII: Mobile Devices & Your Municipality - Managing the Legal Risks

Mobile Awareness and Requirements– An Overview of the Legal Framework and Approach

by

Lou Milrad B.A. LL.B
IMLA Associate General Counsel, Canada
Milrad Law
Toronto, Ontario Canada

©2014 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2014 Annual Conference, held September 10-14, 2014 in Baltimore, MD. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Legal and Policy Considerations and Challenges

Legal Perspective

"We've now gone from mainframe computers to desktops and on to the coffee shop."

As BYOD affords employees access to ***Government Resources****, there is a need to safeguard against potential downstream liability to*

1. *the enterprise itself,*
2. *its employees & external advisors, and to*
3. *third parties.*



Access & Storage & Control of the Device

- ***Access, Storage & Control* of Mobile Devices**
- *Tablets, smartphones, GPS devices, flash drives,* flash drives, solid state hard drives, and other devices
- ***The Cloud***
  - Dropbox, Box, Google Drive, One Drive, etc.
- ***Data Storage***
  - Devices store data differently than traditional computer hard drives.
  - "**Jailbreaking**" and "**Rooting**" further complicate matters
- Present real ***forensic collection challenges***, and in terms of analysis, there are significant issues – in not being able to verify if all data has effectively been gathered.
- ***Biggest Issue in data collection*** - who has *control* of the device?



Today's Data Storage and Retrieval Sources Gathering Forensic evidence

- *Today's Data Storage and Retrieval Sources*
  - *Workplace & Personal*
  - *Extends beyond traditional hard drives*
    - *Personal – used at home and in cars, cloud storage and app access, and on the move*
    - *Business and Organizational use – desktop, mobile, local, remote and cloud servers,*
- *Mobile devices have empowered and evolved into a way of life – texting, emails, cell & Skype, virtual meetings, apps, etc.*

BYOD
Key Legal Challenges
It's all about the Data & Data Governance

- ✓ Data Security and Protecting Data Integrity
- ✓ Prohibition against "jail breaking" or "rooting"
- ✓ Confidential Information
- ✓ Electronic communications, document preservation and evidentiary obligations
- ✓ Insurance and Liability Considerations
- ✓ General Duty of Care
- ✓ Privacy (Personal Information)
- ✓ Employee – Employer relationship
- ✓ Training & education
- ✓ Licensing & Intellectual Property Rights





1. Data Security and Protecting Data Integrity

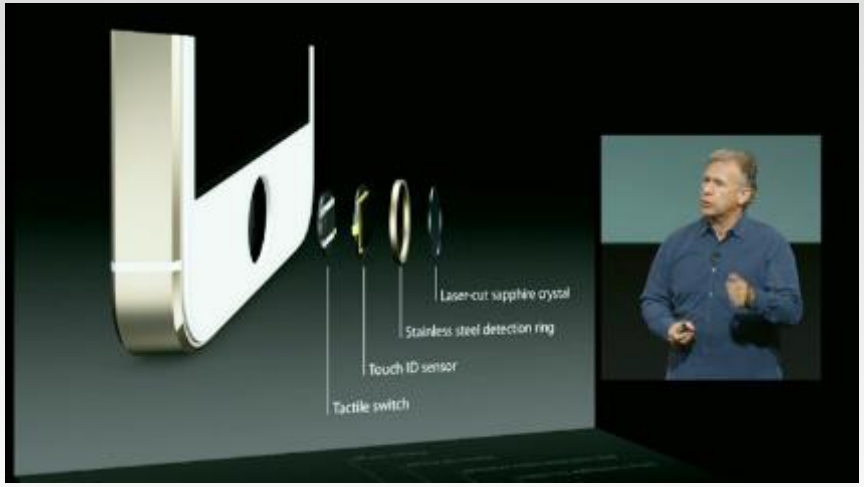
- All about the data, and not the device and separation of personal from business
- "The biggest hazard for organizations is not mobile malware, but data leakage caused by employees losing their devices, or selling sensitive corporate information collected on their mobiles."*
- Employees need to understand - what constitutes acceptable use – examples:
  - Restricted access to Confidential Information
  - Up-front employee's consent to remotely wipe
  - Rules about loading of third party apps – do they need to be first vetted?
  - Rooting & Jail breaking
  - Use of device by family members



*Gartner via Economist, Nov 30th, 2013.

Creating a BYOD Policy - What Should it Include? Some Examples (Cont'd)

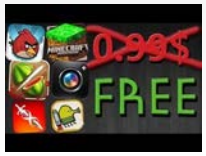
- **No Family or Third Party Access**: The Policy must clearly specify no access or use by family or third parties. No family member or third-parties should be permitted to use and/or gain access to any device used as part of the BYOD policy.





2. Prohibition against "jail breaking" or “rooting”

- Why?
- Potential third party liability to both Organization and Employee by
  - Bypassing digital rights management restrictions & enterprise safeguards thereby opening the gateway to
    - Sharing copyrighted media;
    - Providing direct access to the file system, user interfaces, or network-based capabilities that are otherwise hidden or locked;
  - Some curious-minded developers wish to gain root access to
    - Learn more about how the OS works, or
    - Scour the device and applications for exploitable vulnerabilities (and which might well include firewall bypass apps).

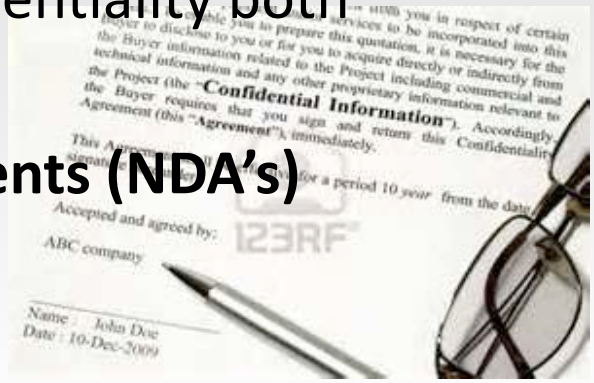




3. Confidential Information



- ***How broadly or narrowly will it be defined in the policy?***
- **Defining Characteristics of Confidential Information:** Typically includes intangible assets (and associated materials) such as trade secrets, designs, processes, programs, procedures, third party Information, developments, disclosed under terms of a software license or services agreement
- **Breach of Confidentiality:** Legal obligation of employees to respect the organization's intangible assets, business and trade secrets etc. and maintain their confidentiality both during and after term of employment
- **Confidentiality & Non-Disclosure Agreements (NDA's)**



4. Electronic communications, document preservation and evidentiary obligations

Need to Be Mindful of General Legal Requirements Governing

- ***Electronic Communications*** *and* ***E-commerce***
- **ESI – Electronically Stored Information** and digital evidence.
  - Civil or criminal matter, there's a legal framework for introducing into evidence any electronically stored information (ESI).
- **Legal retention requirements may also apply to documents comprising**
  - Document retention (and Destruction) requirements arising under
    - Diverse statutory schemes that include provincial and federal and corporation acts, income tax as well as privacy-related legislation, and, where applicable, in accordance with
      - ***Generally Accepted Record Keeping Principles (ARMA International)***
  - as well as
    - Private contracts
    - employment records,
    - workplace safety, and
    - pension benefits.
- **<u>Information Management vs. Data Governance</u>**



5. Insurance and Liability Considerations

- A BYOD policy will need to consider how liability will be apportioned between the individual and the organization
- It is necessary to identify in a BYOD policy whether the user or company will be liable for loss or theft of BYOD devices (particularly important if the organization's insurance policies cover an employee-owned device being used under a BYOD policy.
- Review applicable insurance policies for coverage/non-coverage
- Pay particular attention to the protection and compliance with all Intellectual Property and licensing issues.
- Is the employee or organization to be responsible for lost or stolen devices?



Insurance and Liability Considerations (Cont'd)
Cyber Risks and Threats

A series of new and/or different risks to which organizations are exposed

- Increasing cost arising through sheer volume of data breaches
  - Business leaders now viewing data breaches as more than a purely technical issue – transformed into larger Business Risk.
  - Cyber insurance – being more frequently considered help mitigate the cost of these issues.



Insurance and Liability Considerations (Cont'd)
Cyber Risks and Threats

Categorizing Threats - Top 5 Emerging Cyber Threats

1. Malware (steady threat)
2. Social Engineering (rising threat)
3. Mobile devices (rising threat)
4. Data Loss (steady threat)
5. Internet attacks (rising threat)

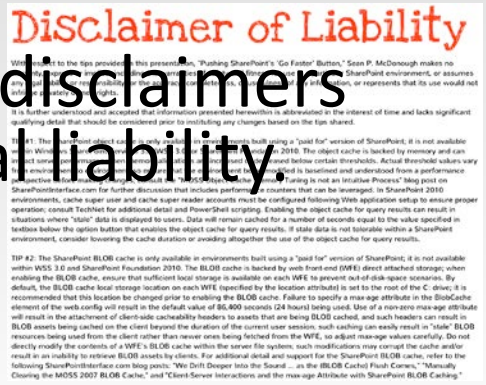


Source:CoNetrix

6. General Duty of Care

Our legal system recognizes that every person and every entity, whether public or private, has a general duty of care.

- Early implementation of a best practices approach
- Must embrace appropriate employee education and training
- In addition, carefully drafted liability disclaimers can to a certain extent reduce general liability.


Disclaimer of Liability

6. General Duty of Care (cont'd)

- The BYOD strategy and resulting policy should always reflect a keen observance of this general duty of care.
- May well preclude your organization from third party liability, financial or otherwise, arising through employees' or consultants' personal failure to comply with all applicable regulatory, privacy, IPR and confidentiality obligations.



7. Privacy (Personal Information)

Makings of a perfect storm with the convergence on one device of both personal and corporate data

- Presents a complication - the trusteeship by the organization of personal information of the person using the BYOD device coupled with possible access, handling and disclosure of personal information of others stored on the corporate servers.
- A workplace surveillance strategy may also be envisioned and in which event, employers will need to have in place, and made easily available and accessible, a data surveillance policy.
- Will the company be permitted access to an employee's own emails and text messages (SMS) on a personal smartphone or tablet used by that employee for work?
- And what about browsing history, installed software and other data?

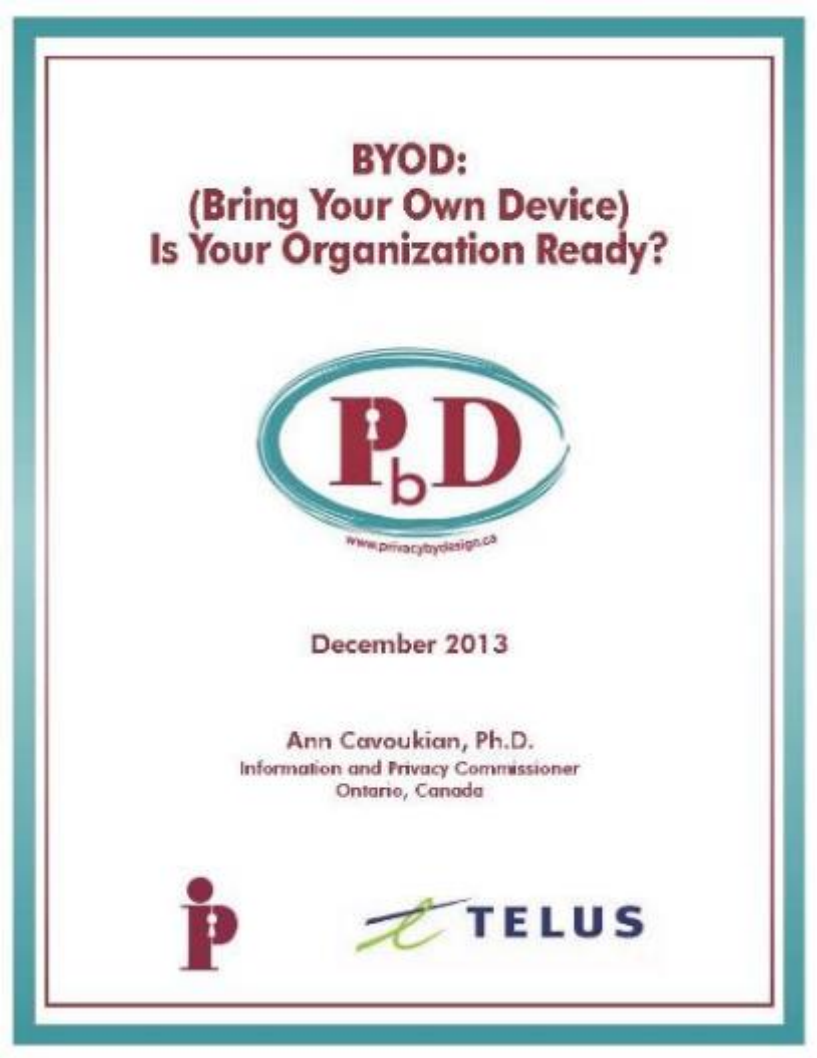


Personal Information
Provincial, Federal & Contractual Prohibitions and Restrictions

- **Privacy Statutes**
  - **Federal -** 250 government institutions are subject to the compliance and prohibit unauthorized use and disclosure
  - **Ontario** - applies to local government institutions, including municipalities, police services boards, public library boards, school boards, conservation authorities, boards of health, transit commissions, certain municipal electricity corporations and certain local housing corporations



- **Access to Information Statutes**
- **Lawful Access & Prohibited Disclosure Legislation**
- **Non-Disclosure & Confidential Disclosure Agreements (NDAs) and contractual terms in *commercial* and *private* contracts**
  - Primary focus is on protecting ***Intellectual Property Rights (IPRs)***
  - Can also include bodies of ***Personal Information*** (e.g.. Membership Lists, Customer Lists, etc.)



BYOD:
(Bring Your Own Device)
Is Your Organization Ready?

PbD
www.privacybydesign.ca

December 2013

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

TELUS

CanadianCIO

10 legal challenges to creating a BYOD policy

The company's acceptable use policy isn't enough to cover employee-owned devices, lawyer Lou Milrad writes

By: Lou Milrad

Overheard recently at a BYOD symposium: "We've now gone from mainframe computers to desktops and on to the coffee shop." This says it all.

While today's workplace environment reflects IT consumerization through widespread proliferation of consumer mobile devices that include an array of smartphones, tablets, and netbooks, a host of enterprises still lack strategies regarding mobile device management (MDM) and in particular, strategies that are coupled with a formalized and well-articulated set of mobile use policies. This combining, in the workplace, of personal and business technology on a single device is of mounting concern to corporate IT departments – it reflects a changing dynamic that challenges those that are responsible for the particular technology being used by employees to do their jobs. This challenge applies to both institutionally provided and employee-owned devices. It is critical for IT departments to comprehend the nature and power of the smartphone and tablet devices that are connecting to their networks so that access to their networks is not only convenient and secure, but also authorized.

While workplace access through previously furnished corporate devices may well be covered under the organization's earlier articulated Acceptable Use Policy (AUP), the array of mobile devices that are being independently adopted by employees that enjoy access privilege or capability (whether authorized or not) that is augmenting a host of IT-related governance and liability concerns, particularly, those relating to privacy and security breaches. Understandably, these threats remain top of mind, recognizing that there is organizational responsibility for maintaining (i) the non-disclosure of "personal information" as mandated under the applicable federal and provincial privacy legislation (that covers all of the organization's employees, customers, suppliers), in addition to (ii) strict protection of the soft assets of the organization, namely its commercially sensitive and valuable business information and associated intellectual property.

A further complication is the potential use by employees, on both sides of the firewall, of cloud-based personal e-mail services such as Gmail or Yahoo, as well as their personal postings through a variety of social media sites such as Facebook and LinkedIn.

We're now witnessing personal emails coming into corporate servers through services that include AOL, Gmail or Yahoo. Information, in the nature of organizational assets, is now transforming from the workplace to the Cloud. Corporate emails are leaving the enterprise through BYOD users forwarding them onto their own personal accounts.

In an effort to reduce security risks, organizations are beginning to focus on creating BYOD policies that will both support and protect mobile devices. Hence, the necessity to create a BYOD program that introduces a phased rollout for "empowered" workers. As prerequisites to any such program and as a first consideration, there is an absolute need to define the necessary MDM and the required mobile security tools, together with a well-considered and articulated BYOD policy.

Given the number of considerations, the BYOD policy should be developed prior to committing to any technology and should start off by reviewing any previously existing Acceptable Use Policy (AUP) with a view to updating, enhancing, or replacing that policy or integrating that policy with the BYOD one.

While not necessarily applicable in all instances, there are a variety of legal issues requiring attention as part of the overall policy, and for this reason, organizations need to include their in-house lawyer or legal department, or external counsel, in the preparation and/or revitalization of a previously enforced policy.

Start the process by requesting copies of what BYOD policies or structures might already be in place with colleague organizations and don't be surprised if portions are redacted by those that are willing to share – also recognize that there may be some hesitancy in sharing given that the policy itself might be designated as "internally confidential".

In starting, it is important to bear in mind that the BYOD policy will need to be well balanced and be void of any unauthorized monitoring techniques, or sanctions that are considered invasive, or disproportional prohibitions. Otherwise, there's a real possibility that any evidence gathered in support of the policy, might well be excluded in court.

The following (not in any particular order of priority) are the key legal risk issues that need to be considered as part of your organization's strategy in developing and implementing the policy:

1. General Duty of Care under our Legal System

In drafting the BYOD policy, we must remain mindful of the fact that our legal system recognizes that every person and every entity, whether public or private, has a general duty of care. Early implementation of a best practices approach, that embraces appropriate employee education and training may well preclude your organization from third party liability, financial or otherwise, arising through employees' or consultants' personal failure to comply with all applicable regulatory, privacy, IPR and confidentiality obligations. In addition, carefully drafted liability disclaimers can to a certain extent reduce general liability. The BYOD strategy and resulting policy should always reflect a keen observance of this general duty of care.

2. Privacy (Personal Information)

We have the makings of a perfect storm with the convergence on one device of both personal and corporate data and which presents a complication - the trusteeship by the organization of personal information of the person using the BYOD device coupled with possible access, handling and disclosure of personal information of others stored on the corporate servers. A workplace surveillance strategy may also be envisioned and in which event, employers will need to have in place, and made easily available and accessible, a data surveillance policy. Will the company be permitted access to an employee's own emails and text messages (SMS) on a personal smartphone or tablet used by that employee for work? And what about browsing history, installed software and other data?

3. Data Security and Protecting Data Integrity

Employees will need to be educated as to what constitutes acceptable use. There is a fundamental duty upon the organization to take reasonable steps to protect the information it holds from misuse and loss and from unauthorized access, modification or disclosure. It's about the data - not the device and the ability to separate "personal" from "business" while also ensuring data is backed up, and that relevant documents are not deleted. Consider the procedures that are required for separating personal from work-related data, so as to ensure that appropriate non-delete, backup and redundancy features are implemented.

Restrict access to highly sensitive Confi-

Copyright © 2013 from CanadianCIO by IT World Canada Inc., 55 Town Centre Court, Suite 302 Scarborough, ON M1P 4X4

A Cited source: Milrad, L. (2013). *10 legal challenges to creating a BYOD policy*.

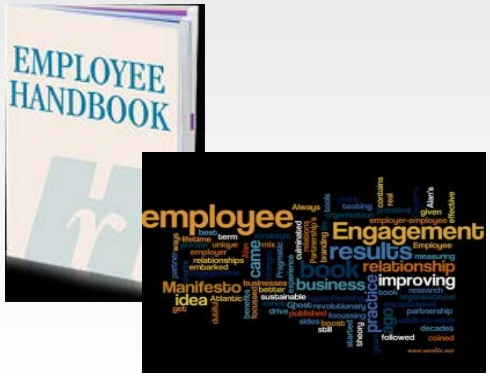
8. Employee – Employer relationship

Employees are obligated to respect the organization's confidential information, including business and trade secrets, lists of sales leads, and other proprietary data and to keep and maintain the confidentiality of such corporate assets after termination of an employment contract.



8. Employee – Employer relationship (cont'd)

- Criminal prosecution may result from any failure to maintain the confidentiality of such information, particularly if intentionally misappropriated.
- In addition, companies often require employees, consultants, contractors, and freelancers to sign confidentiality agreements (NDA's) to establish a legal framework for non-compliance.



8. Employee – Employer relationship (cont'd)

- Organizations become challenged in gathering proof of a breach of confidentiality and enforcing policy when people store any such proprietary data on their own personal iPhones, Androids, and other smartphones or tablets.



Fifth of enterprise BYOD projects doomed to fail by 2016, claims Gartner

Restrictive MDM offerings blamed for BYOD failures.

A fifth of enterprise Bring Your Own Device (BYOD) projects will fail by 2018 because of IT departments' heavy-handed approaches to mobile device management (MDM).

Gartner has made the prediction, claiming employees are lining up to the fact many MDM tools allow IT departments to access their personal information and apps.

Therefore, the market watcher is urging IT decision makers to opt for products that keep their work and personal data separate.



8. Employee – Employer relationship (cont'd)

- Therefore, an **absolute requirement of a BYOD policy needs to require employees (and project consultants, etc.) to permit the company to check out their device when they leave the organization** to make certain that all confidential information has been deleted.
- **Written Consent** - Monitoring, Location Tracking & Remote Wipe
- The **actual timing of the checking** procedure becomes a critical factor.
- **Employment laws vs. Privacy Laws**





9. Training & Education

- Implementation and adherence to a policy can only be effective if there has been proper training and education for employees and those others having access to corporate information.
- Organizations are well advised to organize programs that will serve to familiarize employees with the strategy and with the thinking that preceded implementation of the BYOD policy.





10. Licensing & Intellectual Property Rights

Watch out for software licensing infractions:

- The enterprise's various software applications may be licensed to the company under a variety of software proprietors' individual or collective strategies
- Software and service services providers typically have fairly comprehensive and detailed fees-based licensing structures and charges that range from a per user, or per device type of license, to a number of users concurrently accessing the software from a single location, through to an enterprise wide arrangement.



