# 10 legal challenges to creating a BYOD policy

## The company's acceptable use policy isn't enough to cover employee-owned devices

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.

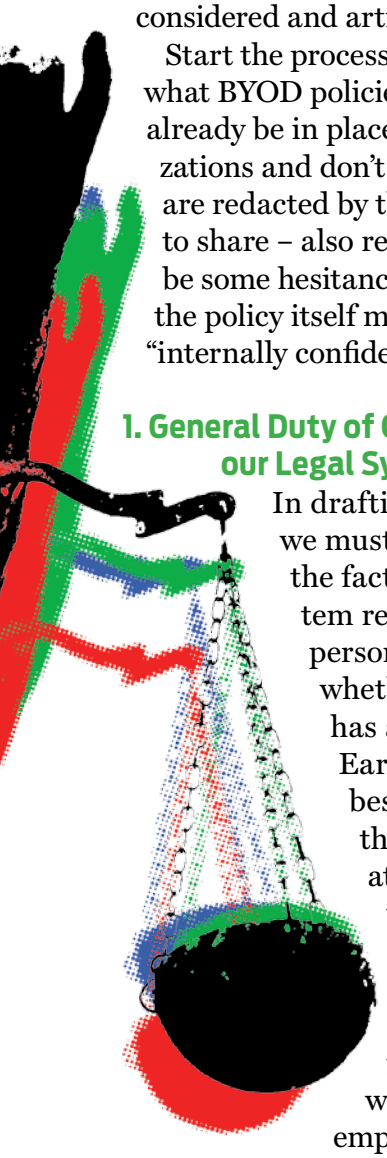
While workplace access through previously furnished corporate devices may well be covered under the organization's earlier articulated Acceptable Use Policy (AUP), the array of mobile devices that are being independently adopted by employees that enjoy access privilege or capability (whether authorized 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 pro-



vincial 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.

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.

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".



## 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 Confidential Information (refer to item 5. below).

## 4. Prohibition against "Jail Breaking" or "Rooting"

While it is important to include strict prohibition against "Jail Breaking" or "Rooting"

employees' devices, it is critically important to communicate to employees the underlying rationale supporting this prohibition and the associated security risks. Trojans, mobile malware, and pirated software are often associated with "Jailbreak" sites. It is important to point out the possible legal sanctions associated with bypassing digital rights management restrictions intended to protect copyrighted works; other concerns to be recognized, on this side of the firewall, include direct access to locked file systems, user interfaces, and normally hidden or locked network capabilities. Additionally, Rooting or Jail Breaking a device to run a free Wi-Fi hotspot may well violate the contract service terms thereby providing affected carriers with cause to terminate subscribers contracts.

Also, there is the potential risk of loss of manufacturer's warranty and carrier throttling for BYOD.

## 5. Confidential Information

Employees and others acting on Company's behalf are responsible for protecting the Company's confidential information, including trade secrets (whether the company's own or those entrusted to it by third parties), from unauthorized disclosure whether internal or external, deliberate or accidental.

It is critical to secure a written, signed confidential disclosure agreement before taking any steps to disclose confidential information to a party outside of the organization. While a general manager or technical director might well possess the necessary signing authority, it is suggested that a medium to high level member of management, such as a vice president, be the designated party responsible for signing confidential disclosure agreements. In addition to maintaining a fully signed copy of that document, a log recording the date, time and location of signing should likewise be maintained for future reference.

For a comprehensive discussion around "confidential information", please refer to this author's article in the September 2012 issue of CIO Canada "For your organization's eyes only - IT governance requires vendor relationships that treat confidentiality as job one. How to make sure your contract includes it."

## 6 Licensing & Intellectual Property Rights

It is important to recognize that 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. Therefore, it is critically important to spend time carefully reviewing the terms of use under such applicable licenses to ensure that corporate implementation of BYOD technologies will not breach the licensing terms in place with the software and providers. Allowing employees to use company applications on their own devices, for example, may breach the company's current licensing agreement. Consider also the licensing terms for the BYOD applications and the accompanying licence rights - what are the limitations, to whom do they apply (largely dependent on whether it is the company or the employee that signs up with the provider), and are they, or will they be in violation of any existing third-party contracts or corporate policies? It is incumbent upon the company, as well as the employee, to mitigate against potential intellectual property and contractual claims from third parties.

## 7. Employee-Employer relationship

Employees are obligated to respect the company'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. 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. 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. 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 company to make certain that all confidential information has been deleted. The actual timing of the checking procedure becomes a critical factor.

## 8. Electronic Communications, Document Preservation and Evidentiary Obligations

While not really part of a BYOD policy or of this article, CIOs need to be mindful of general legal requirements governing electronic communications and e-commerce.

Perhaps, more aligned with a BYOD strategy are document retention requirements arising under private contracts as well as under diverse statutory schemes that include provincial and federal and corporation acts, income tax as well as privacy-related legislation. Legal retention requirements may also apply to documents comprising employment records, workplace safety, and pension benefits. In addition, in any civil or criminal matter, there's a legal framework for introducing into evidence any electronically stored information (ESI). Hence the need to become aware of document retention (and destruction) laws and policies as well as those pertaining to digital evidence.

## 9. Insurance and Liability Considerations

Review applicable insurance policies for coverage/non-coverage, as the BYOD policy will need to consider how liability will be apportioned between the individual and the organization. Pay particular attention to the protection and compliance with all Intellectual Property Rights (IPR – see 6. Licensing & Intellectual Property Rights above) and licensing issues. Is the employee or organization to be responsible for lost or stolen devices? What about responsibility for malware or virus attacks on BYOD device? Does the employer's existing insurance provide coverage for employee owned devices that are part of a BYOD policy? Who is to be specified as responsible for replacement upon theft or loss should employer's insurance coverage not provide for employees device coverage – 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.

## 10. 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. Companies 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.

*Lou Milrad is a Toronto-based business lawyer at Milradlaw.ca.*



CanadianCIO

EDITORIAL

EDITOR
Shane Schick

CONTRIBUTORS
George Gorsline
Bruce Stewart

ART & PRODUCTION

SENIOR GRAPHIC DESIGNER
Mel Manasan

CREATIVE DIRECTOR
Jeff Coles

CANADIANCIO SALES

VICE PRESIDENT, ASSOCIATE GROUP PUBLISHER
Brad McBride

SENIOR ACCOUNT MANAGER
David Hamilton

ACCOUNT EXECUTIVE
Desere Ross

CIRCULATION

CIRCULATION MANAGER
Cheryl Patfield

CORPORATE

CHAIRMAN
Michael R. Atkins

PRESIDENT & GROUP PUBLISHER
Fawn Annan

CONTROLLER
Rob Novorolsky

IT World Canada is an affiliate of International Data Group (IDG), the world's largest publisher of computer-related information and the leading global provider of information services on information technology. IDG publishes over 300 computer publications in 85 countries. Ninety million people read one or more IDG publications each month.

CanadianCIO is published 6 times per year by IT World Canada Inc., a unit of the Laurentian Media Group, Michael R. Atkins, Chairman, 55 Town Centre Court, Suite 302, Scarborough, Ontario M1P 4X4 Telephone: (416) 290-0240 Fax: (416) 290-0238. Publishers of **Computing Canada, Canadian Dealer News and Direction Informatique.** One year subscription rates: Canada $55, US $65 (US) and foreign $95 (US). Single copies $6.00. Please add GST where applicable. Address subscription to CanadianCIO Circulation Department, 55 Town Centre Court, Suite 302, Scarborough, Ontario M1P 4X4. When notifying us of a change of address, please include address label to assure continuity of service. All rights reserved. The contents of this publication may not be reproduced either in part or in whole without the consent of the copyright owner. The views expressed in this publication are not necessarily those of the publishers. Requests for missing issues are not accepted after three months from date of publication.

Date of publication November/ December 2012. Published in Canada. GST Registration # R122605769 ISSN: 1195-6097

HOW TO CONTACT CanadianCIO

**Telephone:** (416) 290-0240
**Fax:** (416) 290-0238
**Mail:** CanadianCIO
55 Town Centre Court, Suite 302, Scarborough, Ontario M1P 4X4
**E-mail:**
editor@itwc.ca
Also, employees may be reached using a combination of their first initial and last name, for example:
sschick@itwc.ca
**Online:**
**www.ITWorldCanada.com**

SUBSCRIPTION INQUIRIES
**Telephone:** (613) 475-3217 or 1-800-565-4007
**Fax:** (416) 290-0239 or 1-800-565-8148
**E-mail:** circulation@itwc.ca

For printed and electronic reprints, please contact Jeff Coles at 416-290-0240 jcoles@itwc.ca

Canada

We acknowledge the financial support of the Government of Canada through the Canada Periodical Fund (CPF) for our publishing activities.

PUBLICATIONS MAIL AGREEMENT NO. 40063800
RETURN UNDELIVERABLE CANADIAN ADDRESSES TO CIRCULATION DEPT – IT WORLD CANADA INC.
302-55 TOWN CENTRE COURT
SCARBOROUGH ON M1P 4X4
E-mail: circulation@itwc.ca