# Lexpert Information Privacy and Data Protection Seminar

BYOD and Social Media – Legal issues and Best Practices to Reduce Employer Liability

December 1, 2016

By: Sheryl Johnson

Fogler, Rubinoff LLP

# BYOD Programs

BYOD programs cannot be ignored by corporate employers given that much more mobile employees are not likely to draw a line between corporate and personal technology without one, which can expose corporate employers to a plethora of challenges involving how their corporate IT departments can adequately manage their employer's technology while protecting corporate networks, systems and data - including the security of client documents and information - where the corporate employer has not procured and may not even be aware of the technology being used to access its network, systems and data.

# Legal Issues and Challenges

"**BYOD**", which stands for the Bring You Own Device mobility program. Under a BYOD program employees are permitted to use the same mobile and other technology devices for personal and office use. Such a program can be broken down into three categories:

1. Employer allowed usage of employee owned mobile devices;

2. Employer owned mobile devices, with or without liability, whole or partial, for the monthly service costs of employee use; and

3. A hybrid approach.

# Advantages

- Connectivity
- Greater innovation
- Use of more cutting edge technology
- Better work-life balance
- Better user experience
- Increased productivity
- Increased effectiveness
- Higher employee morale and job satisfaction
- Reduced costs

# Disadvantages

*To the Employer:*

- Increases pressure on organization’s IT departments
- It could threaten a company’s IT security and put a company’s sensitive systems at risk
- Large legal and competitive advantage risks for an organization in implementing BYOD programs arise out of the fact that the organization is permitting employee users to hold corporate data on personal smartphones, tablets and other devices, which could lead to a myriad of confidentiality and IP issues
    - ➢ Corporate data could be compromised
    - ➢ Legal obligations tied to client intellectual property, personal medical and other confidential or proprietary information that an employee may be required to store on the employee's personal device

# Continued…

- Associated damage to the organization's reputation, which will result in loss of business and thus lost profits

- Employee privacy concerns

- The potential that implementing BYOD programs can runaway IT department service and help desk hours and costs

- Service charges that employees expense back to their employers

## *To Employees:*

- The costs involved with the employee buying the equipment and paying for both personal and business Internet usage
- Negative user experience
- Reduced employee privacy
- Program functionality challenges and associated lost productivity

# Minimizing the Risks Associated With Developing A BYOD Program - Best Practices

- Look at each employee’s job individually
  - ➢ Do you need user groups based on role, function, division, geographic location or other factors?
  - ➢ Perform a privacy and security analysis
- Establish security measures
  - ➢ What security measures are in place if employees’ mobility devices are lost, stolen or compromised?
  - ➢ What limits are placed on devices, apps, access and content?

# Continued…

- Create policies to address:

  - What types of information or content that can and can’t be held on personal devices, as well as what the consequences are if inappropriate information is contained on employees' devices?

  - Where and when an employee can access the organization's network and any limits on what data and/or a limit on the number of apps employees may access?

  - What types of user privacy will be provided?

  - Compliance and remediation

  - Obtain employee's sign off on the BYOD program

- Obtain legal advice

# <u>BYOD Programs</u>: Recognize the Need to Implement and Enforce An Effective BYOD Policy

*Best Practices for Developing and Implementing A BYOD Policy:*

- Tailor the policy to your organization and <u>make it simple</u>
- Be realistic with expectations
- Do not ignore your policy once it is drafted and rolled out
  - ➢ It is not enough to publish the policy and hand out copies to everyone.
  - ➢ Educate and train your employees on the policy
  - ➢ Follow up to ensure that employees are adhering to it
  - ➢ Be consistent in both enforcement and implementing corrective action when there are any breaches of the policy.
- Update your BOYD policy regularly
  - ➢ Creating and implementing a BYOD policy is not a one-time job
  - ➢ Keep employees in the loop on the changes and field any questions arising out of the distribution of the updates.

# Continued…

- In tandem implement a Non-Disclosure Agreement
  - ➢ As a precondition of participating in your organization's BYOD require that employees sign a non-disclosure or confidentiality agreement

- Manage implementation of your BYOD program
  - ➢ Enforce policies
  - ➢ Ensure employees are adhering to the program

# Recommended Steps for Developing a BYOD Policy:

**Step #1:** Start by writing a basic policy.

**Step #2:** Tailor it to your organization by expanding the basic policy to now address specific issues and concerns of your organization in order to define the parameters of your organization's BYOD policy.

In tailoring your BYOD policy, the following issues and concerns should be considered:

- Which devices are allowed to participate in a BYOD program?
- Specifications on who gets to bring their own device
- Specifications on who pays for the device and/or monthly charges
- A zero-tolerance policy for texting or emailing while driving
- Specification on whether devices with cameras and video-recording capabilities are allowed on-site and/or whether cameras will be disabled while on site
- Specification as to when should the user may call the company help desk/IT department for support

# Continued…

- Specification as to whose responsibility it is to keep devices operating in compliance with network security policies
- A procedure for reporting lost or stolen devices
- A white list/black list of platforms and apps
- A listing of what is acceptable use at work vs. at home
- Defining what information employees can share with others from their mobile device
- Notification that the organization will have the ability to track, log data and remotely delete data from and/or remotely lock mobile devices under this policy
- Establishing the organization's exit policy

**Step #3**: Specify what the consequences of noncompliance with the policy are, including but not limited to legal responsibility for illegal activity and/or breaches of the policy.

- Employees need to be clearly warned that they and not the organization will be responsible for any losses or damages arising out of illegal activity or a breach of the program and its policies.

# Continued…

*Examples:*

- Jailbreaking
- Rooting

**Step #4:** Budget for your BYOD program. Be sure to factor in all of the true costs of a BYOD program.

**Step #5**: Train employees - management and rank and file alike on the terms and conditions of the policy as well as the consequences for non-compliance.

**Step #6:** Monitor adoption rates, adherence to terms and conditions of the policy and effectiveness of the policy.

**Step #7:** Fairly and consistently apply the policy and the consequences for non-compliance.

**Step #8:** Audit and update as necessary your BYOD program to ensure that it effectively balances organizational needs, legal obligations and employer and employee preferences.

# Social Media

# Introduction: Use of Social Media in Canada

- Canada has the highest social media network site penetration
- 82% of all Canadians use social media network sites
- Canada ranks 12th in the world in the number of hours spend actually using social media network sites daily with Canadian individuals using it daily approximately 2 hours and 19 minutes
- 93% of social media users polled said they were on Facebook, 31% on LinkedIn and 27% on Twitter

# Legal Considerations

- Social media enables communication and connectivity. Social media can be a successful and cost effective marketing and recruiting tool

- In addition for organizational employers there are a number of issues that arise from social media usage for their employees

  - ➢ First, are employees engaging in time theft?

  - ➢ Second, whether inside or outside of the office, are employees engaging in conduct that breaches another person - whether another employee of the organization or one of its client's common law or statutory rights or entitlements?

    That is, are the comments of a social media message:

    - in breach a person's privacy rights?

    - establish anti-Union animus and expose the employer to an unfair labour practice complaint and/or grievance?

# Continued…

- amount to an intellectual property infringement and expose the employer to liability?

- harassing or bullying? Does the content fit within the definition of workplace harassment or workplace violence under the *Occupational Health and Safety Act*? Are the contents contrary to the *Human Rights Code* (the "**Code**")? Are the contents contrary to *Criminal Code* in that the contents constitute illegal speech (obscenity; hate)? Does such comments expose the employer to statutory, civil or criminal liability?

- creating a poisoned work environment to such an extent that it constitutes a constructive dismissal?

- damaging to the organization's reputation, goodwill, business interests/activities and profitability?

- constitute defamation and explode the employer to liability?

# Best Practices for Employer Implementation of Social Media Policies:

- Employers need to ensure that they have, distributed to employees, effectively implement and properly enforce policies with internal complaint or reporting procedures in their workplaces that deal with codes of conduct, issues of harassment, privacy, respect for human rights, use of electronic devices and use of social media.

- Communicate organization's philosophy on social media?

- Consider whether a social media policy can be a comprehensive, stand-alone policy OR a concise section of a general IT resources and communication systems policy.

# Continued…

- Where employers encourage or require their employees to use social media for marketing, recruiting or other business purposes, they need to establish guidelines or procedures for such conduct. These guidelines should establish:

  - ➢ Clear expectations on content
  - ➢ Whether and to what extent the posting requires authorization or approval prior
  - ➢ Linkages to other organizational policies
  - ➢ Clear warnings
  - ➢ A clear acknowledgement

- Consider implementing in employment contracts and severance packages the requirement that former employees immediately update their social media profiles to reflect changes in their employment history and/or status

# Best Practices for Employer Use of Social Media In Hiring:

- Adopt an employee/candidate privacy policy that outlines in broad categories the types of information that it will collect and from where about employees and/or candidates

- Request candidates written consent on application or other forms to collect personal data about them

- Document and record what personal information was collected about a candidate

- Delete or destroy collected personal information once the purpose for which it was collected and/or its use has been completed AND all applicable limitation and record keeping obligations have expired