



**GROSMAN, GROSMAN & GALE LLP**  
BARRISTERS & SOLICITORS

## Workplace Law E-ssentials

Monday, October 03, 2011

### Social Networking: Workplace Friend or Foe?

#### Introduction

While organizations are right to embrace these sites as an extra weapon in their sales and marketing armory, they need to ensure that organizational and employee security and privacy are not being compromised.

Unfortunately, the extremely rapid growth in popularity of these sites risks catching many HR and IT departments unprepared. Complacency is not an option for organizations faced with such a powerful, yet potentially problematic, communications channel.



#### Getting the balance right

Social and business networking sites are changing the way people communicate with each other, both for business and pleasure. Some might think it makes sense for organizations to simply block employees' access to these sites while at work, citing cyber-slacking as the reason, but it isn't that straightforward. These sites provide employees and organizations they work for with a very real business advantage. Some of the benefits of allowing employees to access social and business networking sites while at work are outlined below.

#### (a) Networking, collaboration and information sharing

Social networking sites can be very effective for business networking. Almost like an informal customer relations management system, people can use social networking sites such as LinkedIn to maintain business contacts and to introduce colleagues or contacts to one another in an informal manner.

#### (b) Marketing

Social networking sites have also opened up new marketing and promotional opportunities for businesses. Companies can pay for banner ads on the sites themselves and can also create their own home pages. Appealing to the tech-savvy, less formal, Web 2.0 generation who have become used to hearing about the latest bands on YouTube or Facebook, social networking sites have become a valuable, low cost marketing tool, particularly for consumer-facing organizations. Publishing corporate blogs on social networking sites can also be a very effective way of sharing information and strengthening brand image.

#### (c) The Facebook Generation

### Previous Survey Results

**What workplace issue does your organization find the most challenging?**

Managing Job Performance: 0%

Managing Sick Leaves / Disability Accommodation: 17%

Innocent Absenteeism: 33%

Employee Retention: 50%

But it goes further than that. They also play a very important part in the lifestyle of anyone under age 35: accessing social networking sites is as important to these younger employees as using their mobile phone. Preventing these employees from using all the technology tools they take for granted has the potential to lead to disgruntled, unhappy workers. By contrast, giving them the freedom – albeit regulated – to use these social networking sites in the workplace can help both employees, and the organizations they work for, to flourish.

**(d) Approach with caution**

It is therefore important to get the balance right: allow employees to use these sites, but ensure that they do so without subjecting themselves or the organization to undue risk. Most employees will have the common sense to use these networks to socialize and do business without compromising security, but it only needs one employee to use a social networking site unwisely for the repercussions to be significant.

**THREATS**

From a purely technical perspective, social networking is simply another example of employees accessing websites while at work. However, social networks do present specific challenges for employers due to the type of content published on these sites. Some of the key threats that organizations need to guard against are discussed below.

**(a) Viruses/Malware**

Criminal gangs target social networking sites because they offer an effective way of propagating malware to a wide unsuspecting audience. The MySpace Trojan (2006), the Orkut worm (2007) and the Secret Crush Facebook widget (2008) are examples of how criminal gangs can use social networking sites to their advantage. And if the user is accessing the social networking site from a work PC, then the organization's entire network risks being compromised. This is especially the case when people believe they are receiving something from a friend and hence their defences are automatically lowered.

**(b) Privacy**

It is easy for people to get carried away and post too much information about themselves on social networking sites. This can lead to identity theft or phishing attacks and helps to promote cybercrime. There has also been several instances where employers or prospective employers have used information posted on these sites in evaluating employees. Many sites, such as Facebook, recommend that users do not post sensitive information on these sites and that they apply the necessary security measures to prevent their personal home pages from being viewed illicitly. That said, there have also been some concerns over what social networks do with the information that they are privy to. For example, Facebook is constantly in the news defending itself against various privacy complaints.

**(c) Cyberbullying/Cyberstalking**

Similarly, employees using these sites are putting themselves at risk of becoming victims of cyberbullying or cyberstalking. A survey carried out by the trade union Amicus, reported that one fifth of employees in the UK were being bullied electronically. Whilst cyberbullying includes e-mails, it also extends to social networking sites; the overall effect can be seriously detrimental to morale within organization. Often, a cybervictim's only recourse is to secure or remove his profile from the offending site.

**(d) Data Leakage**

It is very easy for an employee to post confidential information about their company – be it unwillingly or deliberately – in a blog or on a social networking site. Whether it is the product road map, confidential financial information or even just derogatory comments about management, data leakage can lead to internal reprimands or worse, litigation, fines or even imprisonment of company officials may occur as the result of poor data control.

#### **(e) Lost productivity**

Social networking sites can become addictive, so much as that it is relatively easy to spend two or three hours of the working day socializing online instead of working. Recent surveys indicate that 43 percent of organizations in the UK have banned the use of social networking sites at work completely, for productivity and security reasons. Indeed, in August 2007, Kent County Council banned all of its 32,000 employees from using Facebook, citing 'time-wasting' as the principle reason. This was shortly after the 'I have dosed around on Facebook all day and consequently have done no work' group had been set up!

#### **TO BAN OR NOT TO BAN?**

So where does all this leave organizations that are concerned about the use of social networking sites in the workplace? The answer is that it doesn't have to be that black and white. The technology is available – in the form of secure Web gateways – to allow employees to use social networking sites safely and securely. A secure Web gateway, such as WebMarshal, combines advanced Web access controls, data leakage prevention and inbound threat controls in one centrally managed solution or service that makes accessing social networking sites a low-risk, high-reward option for organizations.

#### **HOW A SECURE WEB GATEWAY CAN HELP**

A secure Web gateway sits between the Internet and the edge of the corporate network and keeps the bad things on the outside of the organization while ensuring that the good things remain within. From a social networking perspective, a secure Web gateway enables employees to collaborate safely with business partners and friends/colleagues on approved, malware-free social networking sites, while also controlling what content can be downloaded or uploaded onto such sites. A secure Web gateway can also be used to provide bandwidth and time of day quotas to employees, to ensure that they do not waste valuable work hours, or use up valuable network bandwidth, on social networking sites.

#### **POLICY ENFORCEMENT**

Whether the technology is in place, or not, organizations should adopt a workplace internet, computer use policy which expressly addresses social networking sites, and which allows enough flexibility for employees to feel as though they are trusted, but is robust enough to provide a secure and productive environment. Part of the policy should include an employees acknowledgement that their actions are being monitored, in the hope that if they know that any inappropriate use is likely to be uncovered, they will think twice about doing anything wrong.

## CONCLUSION

While social networking sites are currently enjoying a high profile, the challenges that they pose do not differ significantly from other forms of Web-based threats. Most of today's employees, particularly the younger generation, expect to be allowed at least some access these sites while at work – albeit with some restrictions. Although some organizations are preventing employees from accessing such sites, the more progressive ones are deploying secure Web gateway technology combined with clear workplace policies to keep the organization and their employees safe, while also providing a flexible and productive work environment. Not only will this powerful combination protect against the current threats posed by social networking sites, it will also protect organizations from many, as yet unknown, Web-based threats.

By: Jeff C. Hopkins

## Is Your Organization Compliant with the Accessibility Standards For Customer Service" Regulations that Take Effect January 1, 2012?

This means that corporations, organizations, or individuals that deliver "goods, services, or facilities" to the public must ensure that their services are accessible to individuals with disabilities. Failure to ensure that such services are provided in an accessible manner and or failure to comply with these regulations can have severe legal consequences for the delinquent organization. Such consequences include heavy fines and penalties that are enforced by government inspectors. There is less than 3 months to become compliant with the ASCS standards and this article attempts, albeit by way of an overview, to highlight some of the main steps organizations ought to take before January 1, 2012.



The AODA is aimed at eliminating discrimination against persons with disabilities in Ontario. To this important end, the AODA seeks to establish, implement, and enforce accessibility standards in the delivery of goods and services, facilities, accommodation, employment, buildings, structures, and premises while, at the same time, providing for the participation of various stake holder groups such as persons with disabilities, industry, and government, in accessibility standard establishment. An accessibility standard sets various "measures, policies, practices or other requirements for the identification and removal of barriers with respect to goods, services, facilities, accommodation, employment, buildings, structures, premises or other such things as may be prescribed, and for the prevention of the erection of such barriers." In addition, accessibility standards "require the persons or organizations named or described in the standard to implement those measures, policies, practices or other requirements within the time periods specified in the standard." In this connection, private and not-for profit sectors must comply with the ASCS regulations as of January 1, 2012.

Accordingly, the ASCS standards apply to a broad range of corporations, organizations, and individuals. For instance, the ASCS applies but is not limited to unions, educational institutions, manufacturers, retailers, professional firms, public and private venue operators among many other entities and enterprises. The

ASCS regulations require that management turn its attention to the establishment of policies, practices and procedures that relate to the provision of goods and services to persons with disabilities.

### **Overview of Key ASCS Requirements**

#### **(1.) *Establish Policies***

These policies, practices, and procedures must be consistent with the following core principles:

- Goods and services are to be provided in a way that respects the "dignity" and "independence of persons with disabilities;
- The provision of goods and services to persons with disabilities and others must be "integrated" unless an alternate measure is necessary;
- Persons with disabilities must be given "equal opportunity" to that given to others to "obtain, use and benefit from the goods or services".

#### **(2.) *Adopted Policies, Practices and Procedures Must Incorporate Assistive Devices and Consider Communication***

Organizations must contemplate and address how individuals with disabilities who require assistive devices (i.e. wheel chair) will obtain, use, or benefit from the provider's goods or services such that the provider's goods and or services are both accessible and available in a way that is consistent with dignity and integration with others.

#### **(3.) *Communication that Takes into Account an Individual's Disability***

As a common sense approach to accessibility, integration, dignity, and independence, provider's must adopt appropriate communication methods so that individuals with disabilities are not prevented or barred in any way from services and goods access delivered by the provider. Communications must take the person's disability into account and would reasonably extend to considering measures to facilitate communication such as, for instance, website content accessible to the visually impaired among other means.

#### **(4.) *Providers of Goods or Services with 20 Employees or More***

Organizations that fall within this class must take additional measures which include preparing and having available for access one or more documents describing the policies, practices, and procedures in place to meet ASCS obligations and upon request, shall give a copy of a document to any person.

#### **(5.) *Service Animals and Support Persons***

This requirement applies to providers that own or operate premises (i.e. buildings where services are provided) and requires that organizations allow persons with disabilities to use their service animals (i.e. guide dog) on premises unless the particular animal is excluded by law (i.e. public health regulations). In the event of an exclusionary regulation, the provider shall make other measures. Similarly, if an individual

with a disability requires the assistance of a support person, the ASCS requires that the support person also be granted access to the premises to accompany the individual with a disability. If there is a fee for admission to the premises it is required that notice is given in advance as to the amount (i.e. admission to an amusement park).

**(6.) *Notice of Temporary Service Disruptions***

The ASCS requires that notice of temporary service disruptions to facilities or services utilized by persons with disabilities to access the provider's goods and services, be posted in a place where the public is likely to be able to access information about the disruption. This may include notice about building maintenance when an elevator is out of service, during construction that may disrupt the accessibility of the premises, and other types of disruptions, whether planned or unplanned. The notice is to include information about the disruption, the reasons for it and the anticipated duration together with alternate arrangements in place to assist with accessibility needs.

**(7.) *Training Staff***

Organizations are required to provide training about the provision of goods and services to persons with disabilities to staff, volunteers and every other person associated with the organization that deals with the public or other third parties on the provider's behalf. The requirement to train is further extended to individuals who are involved in developing the employer's policies, practices, and procedures on the provision of goods or services to the public.

**(8.) *Feedback Process***

Every provider is required to establish a "feedback" mechanism that allows for both the receipt of "feedback about the manner in which it provides goods or services to persons with disabilities, and to respond to such feedback. The feedback mechanism must allow for feedback "in person, by telephone, in writing, or by delivering an electronic text by email or on diskette or otherwise." In addition, the feedback process must be accessible to persons with disabilities and must specify the actions that the provider must take if a complaint is received. If your organization employs at least 20 or more individuals, you must have a document that describes the feedback process available upon request.

**(9.) *Documentation***

If your organization employs at least 20 or more individuals, must document its policies, practices, and procedures in connection with the ASCS in writing and make such documents available for inspection by anyone upon request. Notice that the documents are available should be posted in a conspicuous place (i.e. on the provider's website) and the documents must be made available in a format that takes into account an individual's needs.

The above mentioned requirements provide a very brief overview of the types of requirements and action that organizations will need to take to become ASCS compliant by January 1, 2012. It is recommended that organizations take immediate steps to anticipate the new requirements and to ensure that policies, practices, and procedures are considered, developed and documented well before the New Year. It will also be necessary to arrange for the required staff training necessary to meet the ASCS obligations. Everyone should bear in mind that the sanctions for non-compliance include but are not limited to extraordinary fines (i.e. up to \$100,000.00 **per day**) for offences under the AODA.

By: R. Mark Fletcher

## What's On Our Schedule?

On October 21, 2011, Sheryl Johnson will speak at Lorman Employment Standards Act Conference in Toronto, on Holidays and Vacations - Employer Obligations.

On November 2, 2011, Natalie MacDonald, will be teaching at The Osgoode Certificate in HR Law for HR Professionals - Module 5, Terminating the Employment Relationship: Minimizing Your Legal Exposure.

On December 12, 2011, Natalie MacDonald will speak at Osgoode's annual Employment Law Conference, on Misclassification of Employees.

On October 27, 2011, Norm Grosman will speak at the HRPAO HR Law Conference.

On September 20, 2012, Natalie MacDonald will co-chair the Law Society of Upper Canada's Conference: New Lawyer Practice Series - Employment Law.

Norm Grosman writes regularly for Workopolis. To read Norm's latest article, click [HERE](#).

---

[www.grosman.com](http://www.grosman.com)

Grosman, Grosman and Gale LLP  
390 Bay Street, Suite 1100  
Toronto, Ontario  
M5H 2Y2

This email was created and delivered using [Industry Mailout](#)