



Rubin
Thomlinson LLP

Social Networking: What Employers Need to Know

Presented by:

James D. Heeney
Sharaf Sultan
Rubin Thomlinson LLP

Date: October 14, 2009

Social Networking: What Employers Need to Know

James D. Heeney and Sharaf Sultan

Index

| | |
|---|----------|
| Why does an employee’s activities on social networking sites matter? | 3 |
| Potential Legal Liability..... | 3 |
| Other potential risks to an organization | 4 |
| Courts’ Willingness to Enforce Discipline and Discharge in Relation to Employee Online Activity | 4 |
| <i>Alberta v. Alberta Union of Provincial Employees</i> | 5 |
| <i>Chatham-Kent (Municipality) v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance)</i> | 5 |
| <i>Kelly v. Linamar Corp.</i> | 6 |
| <i>EV Logistics v. Retail Wholesale Union, Local 580</i> | 6 |
| <i>Robertson v. Complex Services Inc.</i> | 7 |
| What should employers take away from the case law? | 8 |
| Privacy Issues: Employers’ Ability to Monitor Employee Online Activity..... | 9 |
| <i>Milsom v. Corporate Computers Inc</i> | 9 |
| <i>Camosun College v. C.U.P.E. Local 2081</i> | 9 |
| <i>Eastmond v. Canadian Pacific Railway</i> | 10 |
| <i>United Food and Commercial Workers International Union, Local 1000A v. Janes Family Foods</i> | 11 |
| <i>R. v. Cole</i> | 11 |
| Surreptitious Monitoring: Employers Beware | 11 |
| <i>Colwell v. Cornerstone Properties Inc.</i> | 12 |
| <i>Konop v. Hawaiian Airlines, Inc</i> | 12 |
| What should employers take away from the case law? | 13 |

| | |
|--|----|
| Managing Employee Activities on Social Networking Sites: Strategy for Employers | 13 |
| Technology awareness and response | 14 |
| Monitoring employee activity | 14 |
| Policy design and implementation | 14 |
| Conclusion | 15 |

Social Networking: What Employers Need to Know

People are under ever increasing time pressures in their daily lives. Technology has evolved to facilitate increased speed and efficiency not only in the workplace but also in the social sphere. As a result, at the click of a button people can access a virtually unlimited number of social contacts at a faster pace than ever before possible. One of the major tools to facilitate this new form of socializing is the so-called Social Networking Site (“SNS”), such as Facebook and MySpace. These websites facilitate social interaction through allowing users to create their own personal profiles, while at the same time being able to access significant amounts of information about other users.

Although SNSs have many positive attributes, there also exists the potential for them to be used in deleterious ways. The same SNS technology that allows the fast and efficient transfer of data can, in the hands of ill-intentioned users, be used just as effectively to spread confidential and destructive information. The challenge for employers is to be aware of both the inherent risks posed by online communication tools such as SNSs and to respond appropriately. The following reviews some of the major legal issues raised by SNSs and strategies for risk management. This paper will specifically discuss case law that addresses the online activity of employees at work, an employer’s ability to monitor employees, as well as strategies for risk management.

Why Does an Employee’s Activities on Social Networking Sites Matter?

Potential legal liability

The advent of SNSs has brought a range of potential legal liabilities for employers. For example, an employee may attempt to hold an employer responsible for human rights violations in relation to the activities of another employee on a SNS. Human rights legislation in Canada, including the Ontario Human Rights Code (the “Code”), places a positive obligation on employers to actively respond to either discriminating or harassing behaviour in relation to a prohibited ground under the Code, such as sex or race.

Alternatively, employers may face charges of defamation and/or workplace harassment where employees attempt to hold employers responsible either directly or indirectly for negative comments made online by an employee about other employees. This can be particularly significant where employees are found to either threaten or disparage others within an organization. In such a case, if

employers have not taken reasonable steps to limit such behavior, they could find themselves vicariously liable for the actions of their employees.

Employers also have good reason to be concerned about harassment as it gains more legislative attention. Section 264 of the Criminal Code of Canada (“CCC”) explicitly addresses Criminal Harassment as including all forms of virtual communication and unsolicited messaging, punishable by summary conviction or indictment. The Government of Ontario has also recently introduced Bill 168 which specifically addresses harassment in the workplace through a proposed amendment to the Occupational Health and Safety Act. Should Bill 168 be adopted into law, it will require employers to not only react to issues of workplace harassment but to also take proactive steps to prevent their occurrence.

Other potential risks to an organization

Employee activity on SNSs also represents a risk to employers through the misuse of confidential information or through activity which damages an employer's brand and/or reputation. Employees using SNSs may divulge information to others through various internet portals, believing either that they have a right to do so or that they benefit from protection since SNSs represent forums outside of the workplace. Depending on the ability of users to access information left on a SNS, organizations could find their confidential information compromised. Given the growing importance of intellectual property to commercial competitiveness, the threat of confidential information leaking into the public sphere is a significant one.

Employee activity on SNSs can also pose a risk to organizations through defamatory statements posted regarding an organization or those associated with an organization. Disparaging remarks left on a SNS could potentially be accessed and spread by millions of individuals, making it hard for an organization to control messages central to maintaining a positive public image.

Courts’ willingness to enforce discipline and discharge in relation to employee online activity

Employers have traditionally restricted concern regarding employee behaviour to the workplace. However, the potential harm that employee activity on SNSs can cause has made it necessary for employers to be more vigilant about employee activity outside of the traditional work environment. Employers are increasingly responding to inappropriate employee online activity through discipline and/or discharge. Correspondingly, courts have demonstrated a willingness to enforce employer reactions through holding employees responsible for inappropriate online activity.

Significantly, an increasing number of Canadian boards and courts have upheld terminations for cause where an employee's activity outside of the workplace is sufficiently injurious to the interests and/or reputation of an employer. These decisions appear to reflect recognition from the judiciary that employee activity outside the workplace can have serious and damaging consequences both to a work environment and to an organization as a whole.

A strong example of an upheld termination in relation to online activity is seen in the case of **Alberta v. Alberta Union of Provincial Employees (R. Grievance), [2008] A.G.A.A. No. 20 (Ponak)(QL)**. In this case, the employer terminated an employee following an investigation related to negative comments the employee had made in an online forum regarding co-workers and management. The employee had kept a personal blog with open public access whereby she ridiculed co-workers and denigrated administrative processes. Although she used aliases in place of actual names of those who she wrote about, she provided detailed descriptions which made it easy to identify who she was referring to. She also used her own name in one entry and identified her place of employment. She used negative terms when referring to her colleagues, such as "Nurse Ratched" and the "lunatic in charge" for her supervisor. The grievor did not apologize to those whom she mentioned but rather posted only an apology on her blog.

The Board of Arbitration (the "Board") upheld the termination because of both the disparaging nature of the comments and the employee's belligerent reaction and lack of remorse when confronted by management. The Board also pointed to the fact that the employee took no steps to block public access to her comments.

Another case involving inappropriate online employee activity is **Chatham-Kent (Municipality) v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance) [2007] O.L.A.A. No. 135 (Williamson)(QL)**. Here, the grievor, a Personal Care Giver at a nursing home, was terminated for cause for breach of the confidentiality agreement, insubordination, and for conduct unbecoming a Personal Care Giver at the Home for the Aged (the "Home") where she worked. She subsequently brought forward an unjust dismissal claim.

The employer justified the termination on the fact that the grievor had created a website wherein she published both text and pictures about various residents without their consent. The blog entries referred to her workplace as "a Hole". She also stated that she was "friggin pissed off", alleging that she was "blackmailed by management." She then used several expletives to describe management. In one entry, she made the following statement about a resident of the Home: "What a treat. He has Parkinson's and 'freezes up' so he can't do a thing for himself. The only part of his body that doesn't freeze up is his damn thumb, that baby can really

push a call light a million times a shift.” The blog contained several other comments similar in tone and effect.

Beyond the obvious inappropriateness of the comments, particularly troubling for the employer was the fact that the site was both publicly accessible and that the employee had publicized the first names of many of the people who she disparaged. While accepting her role in both designing and publicizing the website, the grievor stated that she believed the blog was private and available only to three co-workers.

In upholding the termination, the arbitrator held that there was sufficient evidence to establish just cause and to terminate the grievor. The specific factors which contributed to a finding of just cause included a breach of confidentiality, the inappropriate nature of the remarks about management, as well as the general disregard for the residents of the Home.

The case of **Kelly v. Linamar Corp., 2005 CanLII 42487 (ON S.C.)** shows that employee online behaviour which may prejudice an employer’s reputation can form the basis for discharge. This case involved an employee who was charged with possession of child pornography. The charge related to activity which was conducted outside of the workplace. The employer decided to terminate the employee despite the fact that the activity was conducted outside of the workplace and that he was not yet convicted of the charge. In upholding the termination, the Court pointed to the potential impact which the charge had on the positive reputation of the employer which had been carefully built over a long period of time. The company specifically had a long record of working with young people through various philanthropic initiatives. The Court accordingly held that the risk to the employer’s reputation was sufficient to justify terminating the employee for just cause.

Other case law demonstrates however that even egregious online behaviour may not in and of itself justify discipline and/or discharge. An example is the case of **EV Logistics v. Retail Wholesale Union, Local 580 (Discharge Grievance) [2008] B.C.C.A.A.A. No. 22 (Laing)(QL)**. The case involved an employee who worked as a Forklift Driver for a dry goods storage warehouse. The employee had created a blog which included hate messages about Indians and several comments supporting Nazism. Some examples of blog entries included “I just hate humanity I wish the earth would do a massive eradication to the homo sapiens and kill us off for good especially those good for nothing people from South Asia aka INDIA,” and “I didn’t get my SS costume due to lack of funds for it. I will have it for Halloween 2007 for sure! I could always find a KKK costume as that’s the next best thing to Nazi’s.” The blog also made it obvious that the employee worked for

EV Logistics Gloucester. Upon discovering the blog, the employer terminated the employee for cause.

The employer claimed that it was justified in terminating the grievor's employment because of the offensive, racist and hateful nature of the entries in his blog. This was despite the fact that the blog entries were for the most part made outside of the workplace. The employer believed that its response was both justified and proportionate given the fact that the hateful and racist comments were intended to be read by co-workers, were designed to respond to a co-worker's comments regarding racial hatred, and were written in the context of a workplace that was experiencing problems with racially motivated graffiti and vandalism.

In analyzing the circumstances, the arbitrator pointed to a connection between the activities of the grievor and the legitimate business interests of the employer. The case law in particular referred to the following three questions in determining the appropriateness of any discipline and/or discharge: 1. Was the employee's conduct sufficiently injurious to the interest of the employer; 2. Did the employee act in a manner incompatible with the faithful discharge of his/her duties; and 3. Did the employee do anything prejudicial or likely to be prejudicial to the reputation of the employer?

The arbitrator then analyzed the employee's online activity in light of these questions. The arbitrator found inappropriate not only the nature of the employee's comments, but also the fact that the employee identified the employer, including several references to various employment activities including Employee Appreciation Day. As a result, the arbitrator imputed an intention on the part of the employee for the blog to be read by co-workers.

Despite the evidence, the arbitrator ultimately reversed the discharge of the employee based on a number of factors. First, the arbitrator held that the blog was not directly aimed at the employer. Second, the arbitrator pointed to the fact that the employee had in general a clean employment record. Third, the arbitrator found it significant that the grievor had provided the employer with a letter of apology wherein he accepted responsibility for the blog. Based on these factors, the arbitrator ordered the employer to return the employee to his previous position.

Case law has also demonstrated that a court may be willing to uphold a termination for cause in relation to a singular incident. A good example is **Robertson v. Complex Services Inc., 2006 CanLII 23956 (ON S.C.)**. This case involved an employee who was a table games supervisor at Casino Niagara. During a shift, the employee was seen blowing kisses, making vulgar comments, as well as making gestures simulating oral sex towards his male supervisor. This activity was done in an area where both the employees and the public could hear him. Despite repeated

requests by his supervisor to stop, the employee continued to act inappropriately. The employee was subsequently terminated by the employer for cause. The employer specifically claimed it had just cause to terminate the employee based on this one incident of misconduct, or in the alternative, a culmination of incidents involving this employee. The employee for his part stated that termination for cause was not appropriate since his acts were done in a joking manner and that neither the public nor employees witnessed the gestures.

The Court upheld the termination based on this one incident. In justifying the termination, the Court specifically stated that the incident was sufficient to “strike at the heart of the employment relationship” and that “continuing the employment relationship was not reconcilable with this conduct.” The Court placed particular emphasis on the Casino’s comprehensive rules and regulations about inappropriate conduct. Although focusing on the one incident, the Court also pointed to other moments before this one including repeated lateness, improper etiquette and professionalism.

What should employers take away from the case law?

The case law discussed above indicates that there are circumstances in which employers have the right to discipline and/or discharge employees in relation to inappropriate online activity. The case law also describes a subjective test for determining the threshold beyond which an employer has the right to intervene. This threshold is triggered when it can be demonstrated that there is a sufficient connection between the activities of the employee and the legitimate business interests of the employer.

Analysis of the threshold can be assisted through questions such as whether an employee’s conduct is sufficiently injurious to the interest of the employer, whether an employee has acted in a manner incompatible with the faithful discharge of his/her duties, and finally, whether the employee has done anything prejudicial or likely to be prejudicial to the reputation of the employer. Employers should however carefully analyze an employee’s activities on a case-by-case basis in order to accurately assess the appropriateness of any response.

Privacy Issues: Employers' ability to monitor employee online activity

The discussion above makes it clear that there are risks to employers associated with inappropriate employee activity online. Such risks provide ample reasons for employers to remain aware of their employees' online activity. The question to be determined however is how far an employer can go in monitoring the online activity of its employees. In particular, employers who monitor employee online activity may face a claim that they have improperly interfered with the privacy rights of its employees.

Traditionally, Canadian boards and tribunals have recognized an employer's right to monitor the workplace. The legitimacy of any workplace monitoring was accordingly evaluated on the basis of whether there was a reasonable expectation of privacy in the circumstances. Many of these cases supported an employer's right to monitor work emails. An example is **Milson v. Corporate Computers Inc., 2003 ABQB 296 (CanLII)** [*"Milson"*]. The Court in this case held that an employee had no reasonable expectation of privacy in his work email because there was no email policy in the workplace. The Court, in referring to similar case law from the United States, stated that there may be no reasonable expectation of privacy even when an email policy provides for some privacy rights if emails are offensive or unprofessional. The Court even went as far as to suggest that an employee may have no right to privacy even where a policy exists if emails are sent and received using corporate property.

In another decision, **Camosun College v. C.U.P.E. Local 2081 unreported (November 15, 1999)** [*"Camosun"*], an arbitrator held that an employee had no reasonable expectation of privacy with respect to work email. This case involved the grievance of an employee who was terminated after the employer discovered an email from the employee which included a series of allegations towards other employees and the administration. The union argued that the email messages could not be used as a basis for termination since they were confidential and privileged. In dismissing the grievance, the arbitrator stated that an employee could not expect privacy in relation to work emails. In supporting his finding, the arbitrator pointed to the fact that the College's system was used in transmitting the emails and the fact that emails by their nature could easily be copied and circulated. These cases reflect the view that employers have an implied right on the part of employers to monitor online activity in the workplace.

More recently, it appears that the privacy pendulum has increasingly swung in favour of employees. This appears to have been the case since the federal government and several provinces have introduced legislation specifically geared towards the protection of personal information. The federal legislation, the

Personal Information and Protection of Electronic Documents Act (“PIPEDA”) was introduced in 2004. The legislation regulates all employees working for Crown corporations or in federally regulated industries such as banking, telecommunications, inter-provincial transport and broadcasting. The legislation specifically regulates employers in the collection, use and disclosure of personal information.

PIPEDA at its core prohibits most businesses from collecting, using or disclosing personal information about an individual in Canada in the course of commercial activities without the individual’s informed consent. As part of this process, PIPEDA lays out mandatory procedures governing the handling of personal information. Personal information is broadly defined to include information collected from internet and email monitoring.

The principles of PIPEDA must however be measured against the implied right of an employer to protect its own interests. Courts therefore recognize that employers have the right to monitor the workplace, such as through video surveillance of the workplace. This right however must be exercised in a manner that is reasonable, in good faith and fair dealing.

One of the first cases addressing PIPEDA was **Eastmond v. Canadian Pacific Railway, 2004 FC 852 (CanLII)** [*“Eastmond”*]. In this case, the Federal Court refused to uphold a finding of the Privacy Commissioner that Canadian Pacific Railway (“CPR”) was in breach of its obligations under PIPEDA. The employee had brought a claim relating to the installation of six digital recording surveillance cameras in its mechanical facility area. CPR had previously installed cameras to track the movement of trains. These latest cameras were intended to monitor activity around door entrances and exits. The employee complained that the cameras were inappropriate as they were brought in without any consultation, that it violated employee dignity, that there was no security issue justifying the installation of cameras, and that the cameras negatively affected workers’ morale.

CPR retorted through stating that the surveillance system was necessary to reduce vandalism and to deter theft. In support of its position, CPR pointed to two incidents of vandalism and to two incidents in which female employees reported feeling violated. The Privacy Commissioner agreed with the employee’s position and found that the video surveillance was not appropriate.

The Federal Court subsequently overturned the decision of the Privacy Commissioner on the basis that there were several past incidents justifying the installation of cameras, that the cameras were not surreptitiously implemented or limited to CPR employees, and that there was not a less invasive manner of collecting the same data. The Court based its decision on an analysis of the

following four questions: (1) Whether the measure is necessary to meet a specific need; (2) Whether the measure is likely to be effective in meeting that need; (3) Whether the loss of privacy is proportionate to the benefit gained; and finally (4) Whether there is a less intrusive manner to achieve the same end.

In applying the test, the Court ultimately determined that the camera surveillance was reasonable. The Court also held that no consent was required for the use of cameras based on the exception within PIPEDA that consent is not required where this process might compromise the availability or accuracy of the information.

Although Ontario does not currently have privacy legislation similar to PIPEDA, courts and tribunals in Ontario appear willing to apply its principles in attempting to balance the interests of the employee and employer. This approach is clear from case law addressing privacy issues in the workplace in both the union and non-union context. A good example is the case law of **United Food and Commercial Workers International Union, Local 1000A v. Janes Family Foods, 2006 CanLII 36615 (ON L.A.)** [*Janes*]. The case involved a union grievance in relation to the installation of cameras in the workplace. The union argued that the cameras violated employees' right to privacy.

In ruling in favour of the employer, the arbitrator commented on the application of PIPEDA. Specifically, while recognizing that PIPEDA was federal legislation, the arbitrator held that the principles governing PIPEDA nevertheless applied to Ontario. The arbitrator then analyzed the appropriateness of the installation of cameras in the workplace through balancing the privacy interests of employees against the company's objectives in installing the cameras.

Case law indicates that employees face a greater challenge arguing that their privacy has been compromised when an employer has policies in place regarding the monitoring of online activity. A good example is **R. v. Cole, 2009 CanLII 20699 (ON S.C.)**. This case involved an appeal by the Crown regarding the exclusion of evidence, including email communications, in relation to charges against a school teacher for possession of child pornography. The accused had argued that he had a reasonable expectation of privacy with respect to his emails and the contents of his laptop's hard drive.

In allowing the appeal, the Court held that the employee could not have had an objectively reasonable expectation of privacy. Specifically, the Court pointed to school policies which made it clear that employees should not expect either files stored on hard drives or emails to be confidential. The policies also made it clear that the school reserved the right to open emails if the action appeared necessary for the health of the school system. The Court also pointed to the fact that the policies were clear and that all employees were aware of their existence. The case

makes clear that well-designed employer policies which address privacy issues related to online activity can significantly reduce liability associated with employer monitoring.

Surreptitious monitoring: employers beware

Recent case law indicates that employers should be extremely cautious before considering any kind of monitoring activities which could be interpreted as simply spying on employees. This was the issue in the recent case of **Colwell v. Cornerstone Properties Inc., 2008 CanLII 66139 (ON S.C.)** [*“Cornerstone”*]. This case involved a commercial manager who learned that her manager had secretly installed a camera in her office. The employee subsequently confronted her immediate superior regarding the camera who explained that the camera was installed to detect theft on the part of maintenance staff. The employee was never informed of the existence of the cameras despite the fact that she was directly responsible for maintenance staff. The employee subsequently left her position, claiming that she had been constructively dismissed.

While recognizing that employers may have a right to install a camera, the Court felt it was unacceptable in these circumstances. Specifically, the Court pointed to the fact that this was the only installed camera and that the employee was head of surveillance. The Court therefore found that the camera installation was contrary to an implied employment term of good faith and fair dealing. This case makes it clear that employers must have a reasonable apprehension of abuse by employees to secretly monitor employee activity. Further, this right is limited by an implied obligation of an employer to exercise their rights in good faith and fair dealing.

Case law from the United States provides an example of the risk an employer faces in surreptitiously accessing employee online activity. The case of **Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 882 (9th Cir. 2002)** [*“Hawaiian”*] involved an airline pilot, Mr. Konop (*“Konop”*), who sued his employer, Hawaiian Airlines, alleging that the airline had unlawfully retaliated against him for publishing articles on his blog. The employee had created a website on which he posted comments which criticized the airline, officers, as well as his union in relation to labour concessions which the union was considering making. The blog included statements which questioned the competence of the company president, including that he did his *“dirty work ... like the Nazis during World War II,”* and stating that he employed a *“Soviet negotiating style”*.

The website was not open to the general public. Rather, individuals required specific user information in order to access the site. Only select Hawaiian Airlines employees were provided passwords to access the site. A Vice President of the company subsequently contacted a Hawaiian pilot, who had access to the site. The

pilot then provided his username to the Vice President who then used the information to gain access to the site. Having viewed Konop's comments, the Vice President relayed the information to the airline's president. Konop was later told that Hawaiian Airline's president was upset with Konop's comments.

The employee subsequently sued the company, claiming that he was improperly retaliated against on the basis of his comments. The employee specifically stated that he had been involuntarily placed on medical leave and that the company had threatened to sue him for defamation in relation to the online activity. The employee then claimed that the company's access of the website violated legislation related to wiretaps and stored communication.

In upholding the employer's claim, the Court held that it would be a violation of privacy legislation to access protected web site information without the consent of the owner of the site. The Court further stated that an employer could properly access information which is available to the general public. The Court held that the comments were opinion rather than deliberate false statements of facts and as such did not justify discipline and/or discharge. Although derived from the United States, the case nevertheless raises the important principle that employers should be cautious in taking steps to monitor employee activity online.

What should employers take away from the case law?

The case law described above indicates that boards and courts have traditionally recognized an employer's right to monitor the workplace, including the activities of employees online. The scope of this right however appears to be narrowing as recognition of an employee's right to privacy increases. Employers therefore would be wise to create policies which clearly lay out employer expectations regarding the scope of privacy for online employee activity. These policies should be both clear and well publicized to avoid claims from employees that they were uninformed. Policies governing online behaviour are particularly important in the case of online activity conducted outside of work because of the more tenuous link to the workplace. The following section accordingly describes strategies related to both the design and implementation of policies addressing online activity.

Managing Employee Activities on Social Networking Sites: Strategy for Employers

The above discussion demonstrates the complexities involved in managing online activity in the workplace. The advent of electronic technology, including SNSs, requires that employers be proactive to reduce the potential for legal liability and damage to an employer's operations and/or reputation. The following accordingly

provides information regarding steps employers can take in order to both prevent and respond to inappropriate online employee activity on forums such as SNSs.

Technology awareness and response

The technology driving electronic communication such as SNSs is consistently changing at a rapid pace. Employers should therefore ensure that they remain aware of both the variety and function of available social networking tools. Understanding how the technology functions can help to ensure that employers are aware of the manner in which information can be disseminated and any corresponding potential risk. To this end, employers should remain flexible and willing to consider adopting new approaches in the face of changing technology.

Monitoring employee activity

Managing employee activity on SNSs may require a certain level of monitoring of activity. As discussed earlier, Ontario does not currently have explicit legislation governing privacy in the workplace. The case law described above nevertheless makes it clear that employees have a right to a reasonable expectation of privacy.

Employers would therefore be wise to govern themselves in a manner consistent with the principle that employees have the right to a reasonable level of privacy. Employers should accordingly keep employees as informed as possible regarding the extent to which an employer may monitor online activity. It is also advisable that employers seek the consent of employees with respect to monitoring activities whenever possible. These steps can, through maintaining open communication channels with employees, help to increase employee understanding while reducing potential liability associated with any monitoring of activity.

Policy design and implementation

Another way to manage SNS activity is through the creation of clear policies which lay out employer expectations with respect to employees' usage of SNSs. These policies should address a range of issues including confidentiality, respect among co-workers, loyalty, as well as the importance of avoiding workplace harassment. The following provides a list of items which organizations should consider including within their respective policies:

- Allowed usage, if any, of SNSs in the workplace, and the purpose of such usage;
- The manner in which employees are expected to conduct themselves on SNSs with respect to work issues;

- Information regarding the importance of maintaining a safe and discrimination/harassment-free environment;
- Emphasis that employee activity consistent with employer policies is expected both inside and outside of the workplace;
- The extent to which the employer may monitor any employee SNS activity;
- Reminder to employees that SNS information can be accessed by a wide range of individuals and organizations including current or former employees and employers, competitors, clients, or government agencies;
- Reminder of the potential permanency of information left on SNSs;
- Potential consequences for SNS activity which violates employer policy (i.e. discipline up to and including termination); and
- The manner in which the policy relates to others (i.e. employee obligations towards maintaining confidentiality of information).

The creation of comprehensive employer policies with respect to SNS usage can act as a deterrent for employees against inappropriate activity, while outlining potential consequences associated with inappropriate SNS usage.

Conclusion

Online communication tools such as SNSs present a practical example of how technology can foster social networking. But they are not without risks. Employers can however properly manage the potential downfalls associated with online technology. Through due diligence and proactive steps, employers can not only minimize risks associated with SNSs, but also be adequately prepared to respond when necessary.