Social Media and the Employment Relationship: Balancing the Employer's Right to Regulate and the Employee's Privacy Interest

Peter L. Biro

February 24, 2011

Employees On-Line: What Employers Need to Know About Social Media and Workplace Law in Canada

Co-presented by the Association of Corporate Counsel Ontario Chapter and WeirFoulds LLP
Social Media and the Employment Relationship: Balancing the Employer’s Right to Regulate and the Employee's Privacy Interest

Peter L. Biro

Introduction

Employees are spending increasing amounts of time online, both inside and outside the workplace. Much of this time is spent not only reading online content, but creating and sharing it through online social media such as blogs and the social networking sites Facebook and MySpace. The main role of employment law with respect to these developments is to outline the scope of the employer's interest in the social media activities of employees. The basic analytical framework requires a balancing of two principal interests: the employee's expectation of privacy and the employer's legitimate interest in monitoring, regulating and reacting to employee conduct. While the analysis requires a balancing exercise, the two interests are not necessarily of equal weight. The employer's interest will often be a more dominant consideration, especially with respect to activities that occur inside the workplace given the historical "master and servant" context of the employment relationship and the employer's attendant authority and control.

By asking the appropriate questions concerning an employee's activity, the analysis in determining an employer's right to regulate can be relatively straightforward. The most important question to ask is: does the employer have an interest in the activity of the employee or the electronic content created by the employee?

This question requires that the employer inquire into whether the activity bears on or involves interests such as, inter alia, the employer's right to the employee's full time and attention, use of company property, the reputation of the company, the welfare and well-being of other employees, the employer's economic interests, compliance with company policies, loyalty and avoidance of conflict of interest, protection of trade secrets, intellectual property and other confidential information, and job performance.

At the same time, however, this analysis must also take into account the legitimate privacy interests of the employee. These privacy issues help define the employer's interest. If

* Peter L. Biro is a Partner at WeirFoulds LLP, Toronto.

** With thanks to Christopher Bitonti, student-at-law at WeirFoulds LLP, and to Yoav Harel, a graduate of Osgoode Hall Law School, for their assistance.
the activity in issue is taking place in the workplace and during working hours, the employer may have a presumptive interest in the conduct. On the other hand, if the activity is taking place outside the workplace and outside of working hours, the employee is more likely to have a presumptive privacy interest. This also demonstrates the importance of time and place in assessing whether the employer has a legitimate interest in regulating the employee’s activity. But these presumptions are, of course, rebuttable.

Before the employer can assert an interest in the employee’s activity, the analysis must also take into account whether the right to discipline arises. This requires the employer to ask whether there is some sort of misconduct inherent in or arising from the employee’s activity that gives cause for discipline, such as insubordination or some other breach of duty. This analysis will be informed by the scope of the interest claimed by the employer, which, as noted above, also takes into account the privacy interests of the employee.

Using some basic questions relating to an employer’s interest in the activities of an employee, an employer can more easily determine whether it has a right to regulate the activity of the employee.

It is evident that these new forms of interaction via social media do not call for the development of new legal theories or principles. Using first principles of employment law, the many issues that arise in the context of social media can be appropriately addressed.

After discussing the issues outlined above, and keeping in mind the importance of the basic principles of employment law, this paper concludes by providing some suggestions for the content and use of employment policies as a means by which employers can limit the scope of the employee’s expectation of privacy and reduce the risks that can arise through employees' social media activities.

The Prevalence of Social Media

Social networking sites are defined as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system; (2) articulate a list of other users with whom they share a connection; and (3) view and traverse their list of connections and those made by others within the system. In other words, social networking sites are Internet applications that allow users to easily share information about themselves and view information posted by others. This information may be shared among a network of connections and may be made available to the general public. Well known examples these sites include Facebook and MySpace.

---

A "blog" (a contraction of the term "web log") is also considered as a type of social networking. Blogs are websites, usually maintained by an individual, with regular entries of commentary, descriptions of events or other material such as graphics or video. The more recent phenomenon of Twitter can be thought of as a 'micro-blog', as entries are limited to 140 characters.

As social networking sites are playing an increasing role in society, the example of Facebook is most illustrative. From 2008 to 2010, the number of active Facebook users grew from 132 million to approximately 500 million. People spend over 700 billion minutes per month on Facebook and more than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month. Facebook is the second-most popular website in North America and the most popular photo-sharing website in the world. Blogs are also becoming ubiquitous, increasing in number from approximately 57 million blogs in 2006 to over 112 million in 2007.

The medium now commonly known as e-mail must also be included in the types of online communication that are relevant to the discussion of employment law. Including this medium, the broader term "social media" can be used rather than the more technical term "social networking sites." Social media can be defined as Internet-enabled means of cheap, instantaneous communication that can reach a single person or can be widely disseminated.

A review of some of the statistics on social media in the workplace will help put this discussion into context. According to Statistics Canada, in 2007 e-mail was used by an estimated 81% of private sector employers and 100% of public sector employers in Canada. This use, however, was not always work-related. Canadian employees send an average of 2.6 personal e-mails from work every day, and 7% of employees admit to sending 10 or more personal e-mails from work daily.

In 2007, 87% of private sector and 99% of public sector employees had access to the Internet. Similar to e-mail, the Internet is often used for non-work related purposes during an employee’s working hours. For example, in 2005 68% of all workers in the information

---

3 Ibid.
4 Ibid.
5 Ibid.
6 Ibid.
7 Ibid.
8 Ibid.
technology, professional, scientific and technical sectors accessed the Internet for personal use while at work.  

The Employer's Interest in an Employee's Activities

In order to ensure that a balance is struck between the employer's right to regulate and the employee's privacy interest, the first question an employer should ask when considering whether it has a right to regulate an employee's conduct is: does the employer have an interest in the employee's activity? Interests such as the right to an employee's full time and attention, economic interests related to confidentiality, reputation and defamatory statements, and an employer's duty to prevent workplace harassment are some of the more common interests that arise in the context of employee conduct. Determining this interest also requires an assessment of the reasonableness of an employee's expectation of privacy (which itself is affected by the time and place of the activity) and potential grounds for discipline.

It is important to note that in many of the cases discussed in this paper, a number of issues arise ranging from human rights considerations to the scope of the employee's privacy interests and the extent to which employment policies permissibly limit that interest. This is to say that these potential interests rarely exist in a vacuum and often occur in connection with other interests and issues.

Employers' Right to Full Time and Attention

The prevalence of social media use in the workplace has caused the issue of full time and attention of employees to become a growing problem. In this context, full time and attention means the expectation that the employee will give all of his or her attention and effort to the responsibilities of his or her employment during working hours and that he or she will avoid engaging in personal business or in work unrelated to the responsibilities of the position for which he or she is employed.

For example, in *D.D. v. H.A*  

the employer's information technology department had noticed an unusual pattern of Internet use by an employee. He was found to have been accessing pornographic sites, Facebook, and various other sites for several hours during each day. The employer gave the employee the option of resigning or of being dismissed due to his inappropriate use of the Internet during working hours. This activity contravened the employer's computer use policy, and was considered "time theft". The employee brought a complaint under section 13 of the British Columbia Human Rights Code alleging that a regional provincial health authority, and members of its staff, discriminated against him by failing to properly take account of and accommodate his psychological or mental disability. The employee argued that, at a

---

9  Ibid.
minimum, the employer ought to have investigated the state of his mental health prior to pressuring him to resign.

The arbitrator accepted the employee's submission that the employer had previously been made aware of psychological problems suffered by him that could lead to inappropriate workplace activity, such as depression. However, the employee's allegation of discrimination was rejected because the employer was found to have properly acted upon the information about psychological problems and had tried to assist the employee. Moreover, the arbitrator found that there was a sufficient connection between the impugned Internet activity and any health issues of the employee.

Confidentiality

A breach of confidentiality may also give an employer an interest in an employee's activities. The case of Northcott v. Abbott\(^\text{11}\) shows the relative ease with which social media can be used to breach confidentiality and cause major financial harm to an employer. The plaintiff employer commenced an action against the defendant employee for tortious conversion of email accounts. The employer owned a company named Newpond and had hired the employee to run a website. The employee had great influence on those who visited the website's message board and he violated his confidentiality agreement by announcing on the message board that Newpond was changing owners. The employee then set up his own website and lured customers there.

Newpond had the potential to bill $2,850,000 during the period after the employee set up his website, but its actual billings were $869,250. The court held that the employee was responsible for 80% of the loss and awarded general and punitive damages.

In Chatham-Kent (Municipality) v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance),\(^\text{12}\) the employee who was a Personal Care Giver at a nursing home asserted an unjust dismissal claim. The employer terminated the employee for cause due to breach of the confidentiality agreement, insubordination, and conduct unbefitting a Personal Care Giver. The employee had created a website where she published text and pictures about various residents without their consent.

The union defended the employee in the arbitration. It argued that the contents of the blog were akin to what employees would normally discuss during break times and was not out of the ordinary. The arbitrator, however, pointed out that standards of confidentiality in the health care sector are especially high, and the employee had signed a confidentiality

\(^{12}\) [2007] O.L.A.A. No. 135 [Clarke Grievance].
agreement. Moreover, the training manual expressly stated that this type of information should be kept out of "social conversation." Accordingly, even if the blog were "private" and limited to "a few people", the employee's conduct would already be wrongful and subject to discipline. The arbitrator also considered and rejected a second element of the employee's defence: that the blog had been intended to be private. The instructions associated with the blog site made it clear that unless certain privacy settings were expressly selected by the account holder, the blog would be publicly accessible to all Internet users. Furthermore, some of the blog's content implied that a wide readership was expected.

In addition to demonstrating a potential employers' interest in the activities of employees, the examples from the law of confidentiality demonstrate that courts and tribunals employ the existing basic principles of law in assessing these disputes in the employment relationship rather than developing new principles to address the fact that they arise in the context of social media. The *Clarke Grievance* case also clearly demonstrates how the privacy analysis comes into play in defining the scope of the employer's interest in the employee's activity.

**Reputation**

An activity by an employee that hurts the employer's reputation is another example of a potential legitimate interest. In a case involving a claim of injury to reputation resulting from hurtful statements disseminated by an employee on his blog, another employee complained to the employer about the disturbing content of the first employee's blog. The blog identified the employer by name but did not denigrate the employer. Rather, it contained highly offensive and racist content involving Nazism and violence, among other things. When the blog came to the employer's attention, the content was so alarming that arrangements were made for the RCMP to intercept the employee when he showed up for his next shift.

The arbitrator applied the general test for the right to discipline an employee for misconduct, affirming the employer's legitimate interest in parts of an employee's activities outside work. Since the employee's blog identified the employer, and based on other elements of the blog's content, all three questions from the general test were answered in the affirmative.

The arbitrator, however, ultimately decided that termination was too severe and that a lesser form of discipline was warranted. This was largely because the blog did not seem to be directly aimed at the employer, and the employee was genuinely remorseful and sincerely apologetic. The arbitrator also took into account that the employee had a clean work record and agreed to enter therapy.

---

13 *EV Logistics v. Retail Wholesale Union, Local 580 (Discharge Grievance)*, [2008] B.C.C.A No. 22.
Much like the confidentiality cases do for privacy, this example from the law of reputation demonstrates how the discipline analysis also comes into play in defining the employer's interest in the employee's activity.

**Defamation**

Defamation is another area of law where social media and employment issues converge. Defamatory statements about an employer are actionable and, therefore, certainly give the employer an interest in the activity of the employee.

The 2004 case of *Hay v. Partridge*[^14] shows that the use of social media for the communication of defamatory statements can be found to enhance the harm caused and may be considered an aggravating factor in determining the seriousness of the misconduct and its deleterious effects. While this case did not arise as a grievance or claim of wrongful dismissal resulting from an employer's effort to discipline a wayward employee, it nevertheless arose out of the employment context and its facts could as easily give rise to a disciplinary response by the employer. This case was a civil action in defamation for damages. The plaintiff was an acting deputy warden at the Baffin Correctional Centre. The defendants were employees below the plaintiff in rank, one of whom reported directly to him. The defendants circulated a newsletter at the Centre that the plaintiff claimed contained defamatory statements.

The court determined, before considering the means of dissemination, that the defendants' statements were defamatory. The statements implied that the plaintiff was a drug user and that he was incompetent at his job. The court then noted that an established factor in assessing damages for defamation is "the mode and extent of publication" of the libellous content. In this case, the content was initially published in an internal newsletter but it was soon discussed on an Internet message board and made known to other employers and to the community at large. The court observed that the Internet made dissemination of the defamatory content "anonymous and instantaneous." The distribution of the defamatory content via the Internet was the factor that justified the awarding of aggravated damages in addition to general damages.

Finally, defamatory statements about the employer or about fellow workers or stakeholders of the employer made by an employee, whether on the Internet or elsewhere, will almost certainly found just cause for termination of employment.

Harassment

Employers will generally be concerned about the welfare and well-being of their employees and other individuals involved in their workplace. As a result, issues of harassment can trigger an employer's interest in the employee's activities.

The power of social networking sites to spread and facilitate the dissemination of gossip that may amount to harassment is emblemized by the case *Alberta Distillers Ltd. v. United Food and Commercial Workers, Local 1118 (Whiteside Grievance)*. This case also demonstrates the confusion that can arise from a lack of understanding of how social media operates.

In this case, one employee, Conrad, told management that the work environment in the Alberta Distillers packing department was "toxic" and that she had been subjected to derogatory remarks posted by another employee, Carlson, on the Facebook page of a third employee, Whiteside. As a result, the employer conducted an investigation into the alleged remarks.

The employer had a workplace harassment policy in place, but no policy concerning employees' use of social media outside the workplace. The employer terminated Whiteside in line with its joint obligation with the union to ensure a harassment-free workplace. Based on interviews with some employees, but not with Whiteside, the employer acted upon the misapprehension that Whiteside had posted derogatory comments about Conrad on his own Facebook "wall".

The board determined that it was in fact Carlson and not Whiteside who had posted those comments on Whiteside's Facebook wall and there had been no reply or other expression of approval or acquiescence by Whiteside to the comments on his wall. Since Whiteside had not made the derogatory comments about Conrad, the board held that there was no just cause for discipline and ordered that Whiteside be reinstated.

The matter of *York University Board of Governors v. York University Faculty Association (Laurendeau Grievance)* also involved an allegation of harassment leading to a termination. This case also had an element of uncertainty with respect to the use and reliability of evidence derived from a Facebook page. The employee, a university professor, had been discharged by the employer for offering to improve a student's grade in return for sexual favours. Part of the evidence against the employee was apparently in the form of content on the student's Facebook page. The arbitrator held that this content could not be attributed to anyone without authentication and verification of authorship and that if this could not reliably be ascertained, the Facebook content could not be used as evidence in the case.

---

Another important aspect of cases concerning harassment is that an employer can be held responsible for human rights violations perpetrated by its employees. Human rights legislation, such as the *Ontario Human Rights Code*, places a positive obligation on employers to respond to discrimination or harassment in relation to a prohibited ground.\(^7\) Employers are required not only to react decisively to allegations and evidence of harassment, but also to proactively take measures to prevent it. In Ontario for example, a recent amendment to the *Occupational Health and Safety Act* requires employers to be proactive in addressing workplace violence and harassment by implementing policies, training programs and identifying problem employees.\(^8\)

In *Robichaud v. Canada (Treasury Board)*, a leading case on sexual harassment decided under the framework of the *Canadian Human Rights Act*, the Supreme Court of Canada confirmed that employers could be held liable for the actions of employees in the course of employment.\(^9\) In looking at the purpose of the Act, the court found that it was necessary to impose liability, as the employer is the only one in the position to remedy the discriminatory conduct.

The issue of an employer's liability for failure to prevent harassment in the workplace has also been addressed by the American courts. In the 2005 New Jersey case of *Jane Doe Individually and as G/A/L for Jill Doe, a Minor v. XYC Corporation*,\(^20\) the court found an employer liable for not stopping an employee from distributing child pornography by way of the employer's computer network. The employee videotaped highly inappropriate images of one of his children, took the videos to work and used the employer's computer system to distribute the images over the Internet. The company knew the man was viewing pornography but did nothing to stop him. The court found the company vicariously liable to the depicted child's mother, who worked at the same company. There is no reason to believe that a similar occurrence in Ontario would meet with a different legal result.

As we can see from the review of employers' interests in full time and attention, confidentiality, reputation, defamation and harassment, the advent of social media has not required a completely revamped set of legal principles to address the novel scenarios it has spawned. Rather, the same basic principles that have always been at play are used, if not somewhat adapted to the new context of social media in the workplace. The extent of an employer's interest, however, cannot be completely determined without assessing the employee's expectation of privacy in the given situation. This issue arises both inside the workplace and outside the workplace. The expectation of privacy differs in each context, but

---

\(^{17}\) R.S.O. c. H.19 (1990) [OHRC].
\(^{19}\) [1987] 2 S.C.R. 84.
they are both potential concerns for an employer when assessing the scope of its interest in an employee's activities.

**Employees' Expectation of Privacy in the Workplace**

The nature of the privacy interest was explored by the Supreme Court of Canada in a case discussing the right to be free from unreasonable search and seizure in section 8 of the *Canadian Charter of Rights and Freedoms*. In this case, the Court confirmed that privacy is protected by the *Charter* and stated that "privacy is at the heart of liberty in a modern state...[g]rounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual." Justice La Forest added that "[c]laims to privacy must, of course, be balanced against other societal needs."

In the employment context, the key "societal need" in question is arguably the protection of the employers' legitimate interests, including safeguarding proprietary and confidential information, the right to the full time and attention of the employee during working hours, the assurance that employees will not place their own interests in conflict with those of the employer, the protection of the employer's reputation, the protection of every employee's right to be free from harassment and violence by others in the workplace.

Traditionally, courts and tribunals have recognized an employer's right to monitor the workplace; the test is whether there is a reasonable expectation of privacy in the circumstances. In *Milsom v. Corporate Computers Inc.*, the court held that an employee had no reasonable expectation of privacy with respect to his work e-mail because there was no e-mail policy in the workplace promising any type of e-mail privacy. The court went further, stating that there may not be a reasonable expectation of privacy even when an e-mail policy provides some privacy rights if the e-mails in question are offensive or unprofessional. The court also opened the door to the possibility that employees could not reasonably expect any privacy for e-mails sent and received using company property, regardless of stated company policy.

This, however, has changed since the introduction in 2004 of the *Personal Information and Protection of Electronic Documents Act* (PIPEDA), which gives employees stronger privacy protection. PIPEDA only applies to employees in federally regulated industries, such as banking and telecommunications. But the principles of PIPEDA have also been applied by

---

22 Ibid. at para. 18.
23 [2003] A.J. No. 516, 2003 ABQB 296. In other cases, such as *Owens-Corning Canada Inc.* (2002), 113 L.A.C. (4th) 97, and *Briar v. Canada* (Treasury Board) (2003), 116 L.A.C. (4th) 418, it was held that there was no reasonable expectation of privacy in work email because the employees were warned that inappropriate emails were not tolerated and could be subject to monitoring and that discipline might follow a breach of the company standards.
24 S.C. 2000, c. 5 [PIPEDA].
courts and tribunals with respect to employees outside of regulated industries (i.e., even where PIPEDA itself may not be applicable).

The 2006 Ontario labour arbitration of United Food and Commercial Workers Union, Local 1000A v. Janes Family Foods (Surveillance Grievance)\(^{25}\) is illustrative of this point. The contested issue was the right of the employer to engage in video surveillance of employees at work. The arbitrator noted that:

> [t]he accepted approach… is to balance the employer's interest against the union's or the employee's. In the case of surveillance cameras, the analysis weighs the problem the cameras are intended to address against the employee's interest in not being constantly surveilled, and... not having her or his image recorded. When weighing the balance of interests, one needs to consider the seriousness of the problem the employer is addressing, the effectiveness of the cameras in addressing that problem and the availability of other methods of addressing the problems.\(^{26}\)

In weighing these factors, the arbitrator compared the "constant gaze of a camera" to the "all-seeing eye of a supervisor." Certainly, being watched by a supervisor at work could be reasonable; as opposed to being observed by an employer at home. On the other hand, the arbitrator observed that:

> there is no expectation of having one's image recorded and kept for as long as an employer chooses to keep it. The appropriating of that personal information is a significant intrusion on privacy interests... [e]ven if PIPEDA does not apply in this case, the interest it seeks to protect exists. That interest must be balanced, along with the discomfort of being constantly surveilled by a camera, against the company's objectives in installing the cameras.\(^{27}\)

Taking all these factors into account, the arbitrator found that installing cameras at strategic points, such as entrances and exits, was justifiable for the employer in question, while installations in other areas was not. There must be a reasonable concern for employee impropriety to justify the type or extent of monitoring undertaken.

The application of these principles to social media can be seen by analogizing between monitoring the physical movements of employees with a camera and monitoring their online activities with keystroke logging or screen capture programs. These programs can be compared to extremely efficient supervisors standing behind employees and their computers. Under certain circumstances, it would be reasonable for supervisors to observe what types of activities employees are doing on company time and while using company resources. Thus, factors taken into account by the arbitrator in Surveillance Grievance can also be used to guide an employer's actions in the modern realm of monitoring online activity in the workplace.

\(^{25}\) [2006] O.L.A.A. No. 611 (Arb) [Surveillance Grievance].

\(^{26}\) Ibid. at para. 38.

\(^{27}\) Ibid. at para. 40.
There is also a parallel to be drawn with well-established guidelines concerning audio taping employees. For example, in a British Columbia arbitration, an employer was found to have acted improperly by secretly audio taping a department meeting. The employees filed a grievance alleging harassment on the part of the manager for using a hidden recording device. The employer conceded that surreptitiously recording the employees may have been improper, but maintained that to rectify the situation, it was only necessary to notify employees that their conversations at department meetings were being monitored. The arbitrator agreed with this view. This principle can also be applied to monitoring online activity on social networking sites.

Secretly recording private employee communications can also engage the criminal law. For example, intercepting a "private communication" without consent or appropriate judicial authorization could violate the "wiretap" provisions of the Criminal Code. Section 184 of the Criminal Code makes it unlawful to intercept a "private communication" by means of any electromagnetic, acoustic, mechanical or other device, except where consent to the interception is given... " Section 183 defines "private communication" as a communication made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the intended recipient. However, section 184 does not apply where there is express or implied consent from either the originator or the recipient of the communication.

Uncertainty concerning the enforceability of an employer's practices and policies or the employer's risk of liability in respect of monitoring an employee's social media activity is diminished if the employee consents to the monitoring to which he/she will be subjected or if the employer publicizes the degree of monitoring and makes the practice a condition of employment, whether through the employment agreement or by way of enforceable policies. In Colwell v. Cornerstone Properties Inc., the employer secretly installed a camera in a manager's office. The court confirmed that employers, in appropriate circumstances, do have a right to install cameras, but found that the employer in this case did not have such a right by virtue of the secrecy of the monitoring practice. Installing the camera secretly violated "the implied employment term of good faith and fair dealing".

This can be contrasted with R. v. Cole. This was a successful appeal by the Crown regarding the exclusion of evidence, including email communications and Internet activity, in relation to charges against a schoolteacher for possession of child pornography. The accused

30 Ibid., s. 184.
31 Ibid., s. 183.
32 Ibid., s. 184.
33 2008 CanLII 66139 (ON S.C.).
34 2009 CanLII 20699 (ON S.C.).
teacher did not intend to distribute the prohibited material, and had taken steps to prevent other people from seeing it. But the material was located on the accused's work laptop and the school's computer network. The court held that the employee did not have a reasonable expectation of privacy, largely because the school had explicit policies stating that files and emails located on school computing resources should not be considered by employees to be confidential, and were subject to access by the school under certain circumstances.

These examples showing parallels between traditional issues of workplace privacy and their potential use in issues relating to social media reiterate the important notion that the advent of online activity and social media has not necessitated new legal tenets, but rather leads to more creative applications of the fundamental existing principles of law. Therefore, when considering the nature and extent of social media monitoring from an efficiency, workplace morale, and legal perspective, employers can apply the following test:

- Is the monitoring of social networking activity being done to meet a legitimate need?
- Is the monitoring likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there no less invasive way of achieving the same objective?

Asking these questions will also help employers anticipate future technological, societal, and legal developments. For example, commentator Michael Geist predicts that in the future courts will put increasing emphasis on whether the type of monitoring undertaken was reasonable, and not merely on whether the employee had a reasonable expectation of privacy.\(^{35}\) Having used these questions as guidelines, an employer will have an easier time justifying the reasonableness of their monitoring activities.

### Employees' Privacy Interest outside the Workplace

Concerns over social media use in the workplace relate to employee productivity and time and attention devoted to their work. What then, about employee online activity outside the workplace and after regular hours of work creates concerns for employers?

In this context, the privacy interest of the employee is given more weight than the employer's right to monitor or to regulate. This may also be called a presumptive right of privacy. It bears noting, however, that as self-evident as it may be, where online activity such as blogging or social networking are concerned, the information at issue has potential to be in the public domain. Thus while the privacy interest is not directly engaged, a sort of privacy analysis is frequently used to demarcate the sphere of employer interest from the scope of the

---

employee's reasonable expectation of privacy. In many cases, however, this analysis is a fiction. This is because the real test is not whether the blogging or social networking activity engages a privacy privilege, but whether the specific online activities are or should be matters of interest to the employer such that the powers to discipline or to institute proceedings against the employee are engaged.

The American case of *Konop v. Hawaiian Airlines*\(^{36}\) offers a useful fact pattern to illustrate this point. In this case, the employee created a website on which he criticized his employer, coworkers and union. One online posting stated that the company president employed a "Soviet negotiation style." The website was not publically accessible and required a password for access. The company president found out about the comments by gaining access to the site using another person's identity. The court stated that it would be a violation of privacy legislation to access private website content without the website owner's consent; but that an employer did have the right to access any online information that is available to the general public. The court did not comment on the employer's reputational interest and is decided with reference to American privacy legislation, but such a facts pattern is not unique to the United States.

How then can we differentiate between content that is 'private' or 'available to the general public'? Several Canadian cases have addressed this question with respect to social media activity. In the *R. Grievance*\(^{37}\) case discussed in detail below, the defendant employee claimed that she did not know that her blog posts were publicly accessible. She supposedly did not know that, when first setting up her blog, the default setting was "public", which made all the contents fully searchable on Google. The blog-creation site clearly stated this setting and explained what it meant. As a result, the arbitrator made this observation:

> While the [employee] has a right to create personal blogs and is entitled to her opinions about the people with whom she works, publicly displaying those opinions may have consequences within an employment relationship. The Board is satisfied that the [employee], in expressing contempt for her managers, ridiculing her co-workers, and denigrating administrative processes, engaged in serious misconduct that irreparably severed the employment relationship, justifying discharge.

> That a blog is a form of public expression is, or ought to be, self-evident. Unless steps are taken to prevent access, a blog is readable by anyone in the world with access to the Internet. Unless steps are taken to prevent access, a blog is readable by anyone in the world with access to the internet. The [employee] took no steps to prevent access. On the contrary, the tone of her blogs placed them very much in the public arena and suggested that the [employee] relished addressing a wider audience.\(^{38}\)

\(^{36}\) No. 99-55106 (9th Cir. August 23, 2002).


\(^{38}\) Ibid. at paras. 98-99.
Another example is the *Clarke Grievance* discussed above. In that case, the employee claimed that she believed her offensive blog was private. The employer led evidence from Microsoft Corporation, however, showing the series of web pages that would-be bloggers must navigate in order to set up a site for themselves. That evidence showed that the employee must have known that her postings would be public. In dismissing the appeal of termination, the arbitrator stated:

It is clear from this Program that the default setting for ‘Permissions’ in this program is to ‘Public’, and that the descriptive text below the 'Permissions' text box states that "With permissions set to "Public", your information is accessible to everyone on the web". This would have been seen by [the employee] when she arrived at this screen and, in the absence of making any changes to this setting, when she left this screen and moved on to the next one [the employee] would have created a public setting for her blog. That this is what happened is verified by [the employee]'s testimony that she did not make any changes to settings because she is not a computer literate person. She must have known, however, from reading the text message below the 'Permissions' text box that she had created a blog that was accessible by the public. At the best she was careless in ignoring the clear message given when setting up her blog that it was publicly accessible.

These case examples demonstrate that the principles used to evaluate employee conduct outside of the workplace have not changed merely because that activity has moved into the online sphere. These cases also help to show how the analysis of an employer's legitimate interest includes a privacy analysis. That is to say, the privacy analysis cannot be wholly separated from the employer's interest analysis.

With the rapid increase in employee social media use, privacy issues affecting the employer's interests both inside and outside the workplace arise commonly in the context of monitoring the online activities of employees and the screening of prospective employees.

**Monitoring of Online Activity by Employers**

The American Management Association has conducted detailed surveys on workplace monitoring in the U.S. and in 2007 found that 66% of American employers monitored Internet use, 45% monitored keystrokes at workstation computers, 43% regularly reviewed computer files, 12% monitored blogs and 10% monitored Facebook.

This data suggests that employer monitoring of more traditional online activities is a well-established practice, while monitoring social media use is still emerging. The issue is not that reviewing this use is overly difficult. The technology for monitoring a great deal of employees'...
online activity is available, particularly when the employer's communications technology is used by employees to engage in online activity. Keystroke and screen-capture programs can be used to access any computer activity regardless of password or privacy protections.\textsuperscript{42} The use of these technologies, however, has the potential to attract liability for breach of the privacy interest. For example, the use of keystroke and screen-capture software to access an employee's personal off-site email account, such as Gmail or Hotmail may constitute an illegal interception of the employee's electronic communications, which is akin to wiretapping.

In addition to information gathering, there is the concern that employers may be acting on the information they collect. In 2007, nearly a third of the employers surveyed had fired a worker for some type of Internet misuse.\textsuperscript{43} The question for employers, therefore, is how to balance their interest in monitoring and/or regulating and with the employee's reasonable expectation of privacy.

In the balancing test there is a distinction between the question of whether an employee enjoys a right or reasonable expectation of privacy and the question of whether an employee's conduct can nevertheless give rise to liability to the employer or to an employer's right to discipline the employee in connection with the conduct. For example, if defamatory words are uttered or a breach of confidence occurs in an otherwise private setting or context (such as a "private" on-line chat room), the employer may have recourse to the courts and to disciplinary action even though there may have been no right or ability to monitor the communications themselves. In other words, the potential for employee privacy interests to be in issue and the corresponding prohibition on employer monitoring do not necessarily dispose of the question of whether the employer has recourse against the employee.

Accordingly, there must be an inquiry both into the context (time, place, public/private sphere, statutory insulation of information from use or scrutiny, ownership of technology of communication, etc.) of the employee's social media activity and into the nature of the activity to which the employer asserts an interest (reputational interest, proprietary or confidentiality interest, insubordination, potential vicarious liability to third parties, etc.).

**Screening of Prospective Employees**

Another aspect of the employment relationship that is being revolutionized by the continued increase of social media use is the screening of prospective employees. In 2007 the online employment website CareerBuilder conducted a survey on employers’ use of online services for conducting screening and background checks on prospective employees in Canada. The survey's results showed that 12% of employers regularly used online resources to screen candidates, and that roughly 20% indicated that they intended to start doing so in the

---

\textsuperscript{42} See e.g. the product information for SpectorSoft, online: <http://www.spectorsoft.com>.

\textsuperscript{43} American Management Association, supra at note 41.
These figures attest to the important role of social networking sites in acquiring current, inexpensive, useful information about job candidates. Several issues may arise from this growing use of screening technology. A significant one is the potential for negligence claims because of failed screenings. For example, in Wilson v. Clarica Life Insurance Co., an insurance company was found to have negligently hired an insurance agent. The negligence stemmed from failing to act on a referee's advice and opinion that the agent was not trustworthy.

On the other hand, if employers do make use of social networking sites to obtain information about candidates, care must be taken to avoid accessing or using information for improper or impermissible purposes. Human rights and discrimination issues are important considerations. Section 15(1) of the Canadian Charter of Rights and Freedoms protects individuals from state discrimination based on "race, national or ethnic origin, colour, religion, sex, age or mental or physical disability." As demonstrated in the 2002 Supreme Court case of Lavoie v. Canada, the protection also applies in an employee selection context. In that case favouring Canadian citizens over non-citizens in the hiring process for public sector employees was found to be discriminatory.

The spirit of the Charter is reflected in provincial and federal human rights statutes, which directly apply to the private sector and expressly prohibit the use of certain categories of information (pertaining to enumerated or analogous grounds) in making hiring decisions. For example, section 5(1) of the OHRC states that "[e]very person has a right to equal treatment with respect to employment without discrimination because of race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, age, record of offences, marital status, family status or disability." The protection also extends to analogous grounds. Subsection 23(2) of the OHRC explicitly confirms that this protection extends to the selection of employees, stating that "equal treatment with respect to employment is infringed where a form of application for employment is used or a written or oral inquiry is made of an applicant that directly or indirectly classifies or indicates qualifications by a prohibited ground of discrimination."

---

47 [2002] 1 S.C.R. 769. This case also shows that discrimination on analogous grounds, and not just the enumerated grounds, is prohibited. (In this particular case, the discrimination was saved by Section 1 of the Charter.)
48 OHRC, supra note 17.
49 Ibid.
Accordingly, if an Ontario employer screens out a candidate based on an enumerated or analogous ground, it faces liability for discrimination. For example, in the 1996 OHRC matter of Abdolalipour v. Allied Chemical Canada Ltd., the employer was found to have discriminated against a job applicant based on his "race, colour and ancestry." What does this mean for an employer who 'Googles' an applicant's name as part of the screening process? The question remains largely untested in the courts, but this is likely to change based on the statistics concerning employer screening practices cited earlier.

How does this differ from the more traditional hiring practices? In the classic hiring process, the employer (or agency) solicits applications based on the most important and directly relevant criteria for the job. As an applicant proceeds through interviews and the like, a broader scope of information is acquired. Only in the later stages does the employer access information that would not, or should not, have been used to make earlier decisions in the process. For example, once a positive hiring decision is made, disclosure of certain information such as marital status and age may be required for purposes of the employer's health coverage. But 'Googling' an applicant early in the selection process inverts this narrow-to-broad information stream. Accessing a candidate's Facebook profile or blog can immediately reveal marital status, disability, race, age, and a myriad of other data that an employer is prohibited from considering as a basis for screening or hiring. Even if the employer makes use of permissible information from a social networking site, the basis for a screening decision could be later called into question because the employer also possessed the prohibited information.

There are steps that employers can take to reap the benefits of information gained from social media, while avoiding the legal pitfalls. Some of the steps are:

- Screen applicants in a uniform manner. Create a list of social media that will be searched for each applicant. Document the permissible categories of information by establishing a set of search criteria that will enable you to effectively and safely conduct the social media search. Screen all applicants using those lawful criteria.

- Have a neutral party (e.g., an employee in a non-decision-making role or an outside consultant) conduct the social media search, filtering out any prohibited types of information about the applicant and reporting only the info that can lawfully be used in making the screening decision.

- Do not obtain special access (e.g., becoming a "friend" of the applicant on Facebook) in order to access an applicant's non-public social networking profile. The applicant may feel pressured to accept the request, and such a request may make it harder for the employer to prove that it did not use the information discovered when making its employment decision.

---

Employers must be able to point to a legitimate, non-discriminatory reason for the screening decision, with supporting documentation. Employers who are considering making an employment decision based on information found in social media must explain the actual reasons.

The key analysis of balancing the employer's right to regulate and the employee's privacy interest requires an employer to ask a very basic question: does the employer have a legitimate interest in the employee's activity? As we have seen, this analysis is informed by the employee's expectation of privacy; but it is also informed by potential grounds for discipline, such as insubordination and other forms of misconduct.

The Employer's Right to Discipline an Employee

Even if the employer can assert an interest in the employee's activity, the analysis must also take into account whether there is cause to discipline the employee. The right to discipline an employee for misconduct or breach of the express or implied terms of the employment contract has always been an essential feature of the employment relationship dating back to the origins of the law of master and servant. Long before the advent of the Internet, the 1964 Ontario arbitration, *United Automobile Workers, Local 195 v. Huron Steel Products Co. (Discharge Grievance)*, set out the test in a manner that contemplated the employer's interest in the activities engaged in by employees even when such activities occurred outside the traditional context of workplace and regular working hours. The Labour Relations Board stated:

[Under normal circumstances an employer is only properly concerned with an employee's due and faithful observance of his duties on the job. However, no hard and fast rule can be laid down, and in each case the determination of three questions of fact will determine the issue. These are:

(a) Was the employee's conduct sufficiently injurious to the interests of the employer?
(b) Did the employee act in a manner incompatible with the due and faithful discharge of his duty?
(c) Did the employee do anything prejudicial or likely to be prejudicial to the reputation of his employer?

...If one or more of the above questions must be answered in the affirmative on all the evidence, then the company is properly concerned with the employee's conduct regardless of whether it occurred on or off the company property or in or out of working hours, and depending on the gravity of that conduct, the company will be justified in taking appropriate disciplinary action.](^51^)

Although the misconduct in *Huron Steel Products* involved a physical altercation between workers, it remains applicable to a wide range of transgressions, including those that

---

occur online. It is also well established, and remains true in cases involving social media, that the onus is on the employer to show that the employee's conduct adversely affects its legitimate business interests.\textsuperscript{52}

A common example of misconduct that arises in the context of social media is insubordination. Insubordination can occur both during working hours and outside the workplace after regular hours of work. The latter is where most of an employee's online activity falls. The case of Alberta v. Alberta Union of Provincial Employees (R. Grievance – reversed in a judicial review on other grounds)\textsuperscript{53} illustrates the notion that employee comments made online can amount to insubordination and justify termination of the employee. In this case, the union sought reinstatement of an employee after the employer terminated the employee following an investigation relating to negative comments she made in an online forum regarding co-workers and management. The employee had kept a personal blog with open public access where she ridiculed co-workers and denigrated administrative processes. Although she used aliases in place of actual names, it was easy to infer who was being referred to. The employee 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 employee's main defence was that she did not know that her blog was accessible to the public. The employee also argued that she did not realize that her blog postings were hurtful or insubordinate. The arbitrator, however, observed that the employee took no steps to block public access to her comments. The arbitrator also took into account the disparaging nature of the comments and the employee's belligerent reaction and lack of remorse when confronted by management. As a result of these findings, the termination was upheld.

In a subsequent judicial review of the arbitrator's decision, however, the termination was reversed.\textsuperscript{54} The court confirmed that termination based on the employee's online actions could have been justifiable, but ordered reinstatement because management failed to comply with the due process for discipline provided in the collective agreement. This highlights the importance of following the processes stated in or associated with workplace social media policies.

Our discussion now turns to some suggestions for workplace technology and social media policies. If we take the lessons learned from the foregoing discussion, the basic framework of balancing the employer's right to regulate and the employee's privacy interest should justify, if not also determine the principles underpinning these policies. Moreover, the basic pillars of employment law should not have to change in any dramatic way because of the

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{52}] See e.g. \textit{Air Canada v. International Association of Machinist and Aerospace Workers, Lodge 148, [1973] C.L.A.D. No. 7.}
\item[\textsuperscript{53}] \textit{R. Grievance, supra note 37.}
\item[\textsuperscript{54}] \textit{Alberta Union of Provincial Employees v. Alberta, [2009] A.J. No. 368 (AB Q.B.).}
\end{itemize}
\end{footnotesize}
advent of social media. Rather, they should simply address new circumstances of applicability for these first principles of employment law.

**Workplace Policies Concerning Technology Use and the Use of Social Media**

The most effective way for an employer to defensibly balance the employer's right to regulate and the employee's privacy interest is by implementing a comprehensive and consistently enforced workplace policy on the use of information technology, including the use of social media. In doing so, employers can reduce lost or unproductive employee time, increase protection of proprietary and confidential information, protect the company's reputation, and enhance their ability to impose discipline in the workplace. Such a policy can also help shield employers from statutory and common law liability by distancing the employer from the wrongful acts of employees as well as prevent employees from pleading ignorance when confronted with allegations of their own inappropriate online activity.

Moreover, these policies provide employees with fair warning of activities that are subject to monitoring and conduct that is liable to incur discipline. Thus, a case for discipline or dismissal can be bolstered by pointing to a clear, consistently enforced policy that employees have been made aware of.

The first step to consider in developing a policy is the proper level of restriction of social media use in the workplace. This will likely depend on the employer's industry and culture. In some professions, industries, or specific positions, the use of social media might be appropriate or beneficial for business development purposes (i.e., for sales people to make and maintain contacts). On the other hand, an outright ban may be appropriate for others because the workforce simply has no business reason to access or use social media while at work or while using the company networks, facilities, or equipment.

At the very minimum, employers should insert broad language encompassing social networking sites, blogs, and virtual worlds into current IT, code of conduct, harassment, and confidentiality policies. However, employers should also consider adding some or all of the following features, as appropriate, to create a comprehensive social media policy:

- The scope of permitted usage, if any, of social media in the workplace and during working hours, as well as the purpose of such usage.
- A reminder that all communications and transactions using the employer's server, modem, computer or other communications technology (save for the telephone) will be monitored and that all records of such communications are effectively the property of the employer.
- Instructions concerning the manner in which employees are expected to conduct themselves on permitted social media.
- Information regarding the importance of maintaining a safe and discrimination / harassment-free environment.
- An 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's social media activity.
- A reminder to employees that social media 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 permanence of information left on social media sites.
- Potential consequences for social media activity that violates employer policy (i.e. discipline up to and including termination).
- The manner in which the policy relates to other policies (i.e. employee obligations towards maintaining confidentiality of information).
- A prohibition on disclosure of the employer's confidential, trade secret, or proprietary information.
- A request that employees keep company logos or trademarks off their blogs and personal web pages or profiles (this includes a prohibition of photos of employees in uniform, unless it is for business purposes) and not mention the company in posts, unless for business purposes.
- An instruction that employees not post or blog during business hours, unless it is for business purposes.
- A request that employees bring work-related complaints to human resources before blogging or posting about such complaints.
- A prohibition on using company e-mail addresses to register for social media sites (unless the social networking activity is related to official business and subject to appropriate guidelines).
- A prohibition on posting false information about the company or its employees, customers, or affiliates.
- A general instruction that employees: use good judgment and take personal and professional responsibility for what they publish; think before posting a comment; and avoid discussion of controversial topics online.
- A demand that all employees with personal blogs that identify their employer include a disclaimer that the views expressed on the blog are those of the individual and not the employer.
- Language specifically referencing social media into the confidentiality provisions of separation agreements.
A reminder that even the social media activity of employees engaged in outside of work and using the employees' personal computers and internet accounts must avoid all injury to the employer's reputation, must refrain from harassing or defaming the employer or any employees of the employer, must be respectful of the employer's proprietary and confidentiality interests in information, trade secrets, etc. . . and that any failure to adhere to these requirements could result in discipline and legal action.

Even having taken all the above considerations into account, the most forward-looking policies must still be monitored and updated on an ongoing basis. The underlying legal principles may be well established, but the scenarios for their application continue to evolve.

Conclusion

While the modern technology of communications continues to evolve with lightening speed and the use of social media and the Internet are so prevalent that it is scarcely possible to imagine any workplace functioning without them, the basic principles governing the employment relationship have not changed. The law has simply been adapted and applied to fact situations that appear novel because of the new technologies involved. Accordingly, whether in the context on-line activity by an employee or in more conventional contexts, the dominant paradigm within which to ascertain the respective rights and interests of employer and employee continues to be the balancing of the employer's right to regulate conduct and the employee's reasonable expectation of privacy.

Most of the facts presented to employers, courts and tribunals will continue to require this balancing of the employee's expectation of privacy or insulation from employer scrutiny and control against the employer's legitimate interest in knowing, monitoring, regulating and reacting to employee conduct. Employees will always engage in conduct, both inside and outside the workplace, in which employers claim a legitimate interest. Likewise, employers will always take an active interest in the activities of employees inside and outside the workplace in which employees will assert a reasonable expectation of privacy.

The employer's interest cannot extend to employee information that is protected by human rights legislation from employer scrutiny and consideration in the human resources decision-making process. On the other hand, an employee's privacy interest cannot be used to shield him/her from liability to or discipline by the employer for breach of trust or confidence or for defamation.

As has always been the case, the analysis ought to begin with the question of the nature and scope of the employer's interest in the employee's activity (be it social networking, blogging or other activity) and the nature and quality of the competing interest in insulation or immunity from employer scrutiny, regulation or control, which may be asserted by the employee in respect of that same activity.
While the use of these new technologies by employees may seem inevitable, the scope of the employee's privacy interest in the workplace can be substantially restricted by way of enforceable policies. Employers can also implement policies concerning social media activity undertaken outside the workplace but in which the employer can demonstrate a legitimate interest.

The social universe ushered in by the technology of the Internet and by Facebook are surely revolutionary in ways too numerous to mention and this revolution surely presents fascinating fact patterns and dicey evidentiary challenges for the law to grapple with. But the essential principles that govern or ought to govern the legal relationships between employer and employee have not been markedly altered by these developments.

Peter L. Biro is a Partner at WeirFoulds LLP. He is a leading commercial and civil litigator and employment lawyer. He is known for his passionate advocacy and his commitment to effective pro-active problem solving and crisis management on behalf of his clients. Peter can be contacted at 416.947.5094 or pbiro@weirfoulds.com.