Investigating and Forgetting on the Web:
“Privacy law and Social Media in the Employment Context—The Canadian Perspective”

By Roy L. Heenan and Philip D. Dawson*
Heenan Blaikie LLP
1250 René-Lévesque Blvd. West, Suite 2500
Montreal, Quebec H3B 4Y1
T 514 846.1212 ext. 3264
rheenan@heenan.ca

A. The Canadian Privacy Legislative Framework

Canada has established an extensive privacy law framework that includes numerous federal and provincial statutes that govern the public, private and health sectors. Each statute sets out a regime for the protection of personal information, although varying in scope, substantive requirements and remedy and enforcement provision.

In large part, however, two federal Acts—the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA)—have served as the basis for the system’s evolution.1 Compliance with these Acts is supervised by the Privacy Commissioner of Canada, who is authorized to receive and investigate complaints filed under the Acts.

---

*Roy L. Heenan is the Chairman and Founding Partner of Heenan Blaikie LLP. Philip Dawson is a summer student at Heenan Blaikie LLP and will be articling at the firm in 2013.
1 While certain provisions of the Canadian Criminal Code and provincial and federal Charters of Rights and Freedoms also deal with the right to privacy, these are not the focus of this paper.
(i) The Privacy Act

The Privacy Act has been in force since July 1, 1983, and imposes obligations on all federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. The Act has three basic components: first, it grants individuals a right of access to personal information about them that is held by the federal government; second, it imposes fair information obligations on the federal government in the management of personal information under its control; and third, it empowers the Privacy Commissioner to resolve problems and oversee compliance with the legislation.

The central principle of the Act is that the personal information held by the federal government should only be used for the purposes that an individual has consented to. As such, any person may apply for access to his or her personal information, and to have this information corrected if inaccurate. If the applicant is not satisfied with the government’s actions in these regards, a complaint can be made to the Privacy Commissioner who will attempt to resolve the situation.

(ii) The Personal Information Protection and Electronic Documents Act (PIPEDA)

The federal Personal Information and Protection of Electronic Documents Act (PIPEDA) provides the foundation for the protection of personal information in the private sector. Phased in from 2001 to 2004, the Act was designed to confront an “era in which technology increasingly facilitates the circulation and exchange of information”, with the twin

---

2 “Fact Sheet: Privacy Legislation in Canada” online: Office of the Privacy Commissioner http://www.priv.gc.ca/fs-fi/02_05_d_15_e.cfm.
4 Ibid., at p. 5; see also “Fact Sheet: Privacy Legislation in Canada” supra note 2.
goals of “support[ing] and promot[ing] electronic commerce”. PIPEDA’s purpose is to establish rules that govern the collection, use and disclosure of personal information in a manner that recognizes both the right of privacy of individuals and the need of organizations to acquire and handle such information for legitimate business purposes. Similar to the Privacy Act, the premise underlying PIPEDA is that Canadians have the right to know why a business is handling their personal information and the right to verify that such information is accurate.

PIPEDA applies to organizations that collect, use and disclose “personal information” in the course of a commercial activity which takes place within a province, unless the province has enacted legislation that has been deemed to be "substantially similar". Thus far only British Columbia, Alberta, Quebec, and Ontario (with respect to personal health information only) fall into this category. However, PIPEDA continues to apply to the federally regulated private sector in these provinces—such as banks, telecommunications companies, airlines, railways and interprovincial trucking companies—and to all personal information used by commercial entities in the course of interprovincial and international transactions.

In the workplace, PIPEDA applies to employee personal information of the federally regulated private sector only. The substantially similar privacy legislation in Alberta, British Columbia and Quebec applies to the employee personal information practices of organizations in those provinces. Therefore, provincially regulated private sector entities in provinces

---

5 Please refer to the preamble and s. 3 of the Act.
6 Please refer to s. 3 of PIPEDA; see also, “An Overview of the Personal Information Protection and Electronic Documents Act” online: Office of the Privacy Commissioner of Canada http://www.priv.gc.ca/legislation/02_06_07_e.cfm.
7 “Fact Sheet: Privacy Legislation in Canada” supra note 2.
8 Personal Information is broadly defined in PIPEDA and other Canadian privacy statutes as information about an identifiable individual. Most business contact information is expressly excluded from the definition of personal information.
9 Private sector privacy legislation in British Columbia, Alberta and Quebec have been deemed "substantially similar", as have certain health privacy statutes.
10 “Substantially Similar Legislation – Legal information related to PIPEDA” online: Office of the Privacy Commissioner of Canada http://www.priv.gc.ca/legislation/ss_index_e.cfm ; also see “Fact Sheet: Privacy Legislation in Canada” supra note 2.
without substantially similar privacy legislation are not governed by privacy legislation with respect to their employee personal information practices. Such employees are protected by the common law tort of invasion of privacy, described further below.

PIPEDA’s core privacy provisions are set out in Schedule 1 of the Act, the Model Code for the Protection of Personal Information (the “CSA Code”). While different in form, each of the substantially similar privacy statutes in Alberta, British Columbia and Quebec set out similar rules. Below is a high-level overview of the CSA Code, as articulated in PIPEDA.

- **Accountability**: An organization is responsible for personal information under its control and shall designate an individual who is accountable for the organization's compliance with the other privacy principles.
- **Identifying Purposes**: The purposes for which an organization collects personal information shall be identified by the organization at or before the time the information is collected.
- **Consent**: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, subject to limited exceptions.
- **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
- **Limiting Use, Disclosure, and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
- **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is used.
- **Safeguards**: Personal information shall be protected by physical, technical, and administrative security safeguards appropriate to the sensitivity of the information.
- **Openness**: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- **Individual Access**: Upon request (and subject to limited exceptions), an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the privacy principles to the designated individual accountable for the organization's compliance.
It is important to note that the privacy principles have been drafted in a technologically-neutral fashion\(^{11}\) and are based, in part, on international data protection standards established by the 1980 Organization for Economic Cooperation and Development (OECD) Guidelines on Privacy.\(^{12}\) As such, Canadian privacy law has been designed to keep pace with innovation and to evolve in harmony with common international practices.

**B. The Tort of Invasion of Privacy**

Under the common law, the tort of invasion of privacy is the main source of privacy rights for employees. Though this cause of action has a mixed reception in Canada, after the 2006 Ontario decision in *Somwar v. McDonald’s* the tort of invasion of privacy cannot be discounted.\(^{13}\) There, an employee alleged that his employer had invaded his privacy after performing an employment-related credit check on him without first obtaining his consent. The court refuted the employer’s assertion that invasion of privacy had no basis in Canadian law, and stated that “the time [had] come to recognize invasion of privacy as a tort in its own right”.\(^{14}\) While the Ontario Superior Court recently rejected this assertion in *Jones v. Tsige*, this decision is being appealed.

**C. Role of the Privacy Commissioner of Canada**

The task of supervising compliance with federal privacy legislation is centralized within the Office of the Privacy Commissioner of Canada (OPC).\(^{15}\) The Privacy Commissioner

\(^{11}\) Adam Kardash and Rhonda Shirref, “Privacy Law”, (Electronic Commerce) (2002), at p. 11.

\(^{12}\) Holmes, supra note 3.

\(^{13}\) (2006) 79 O.R. (3d) 172 (S.C.)

\(^{14}\) Ibid., at para. 31.

\(^{15}\) “Mandate and Mission” online: Office of the Privacy Commissioner of Canada http://www.priv.gc.ca/aboutUs/mm_e.cfm.
(the “Commissioner”), who heads OPC activities, works independently of any other part of the government and reports directly to Parliament. One of the Commissioner’s central functions is to investigate individual complaints filed under the *Privacy Act* and under PIPEDA.\(^\text{16}\) While the Commissioner resolves complaints mainly through negotiation, or mediation and conciliation, if voluntary cooperation is not feasible the Commissioner retains additional powers to summon witnesses, administer oaths and compel the production of evidence. Where these initiatives fail, the Commissioner also retains the power to take the matter to the federal courts for judicial relief. The Commissioner may also, of its own accord, conduct audits of organizations under its jurisdiction. Other responsibilities of the Commissioner include public reporting on the personal information-handling of public and private sector organizations; taking a leadership role in promoting awareness and understanding of privacy issues; and working with other Canadian and international privacy stakeholders to address global privacy issues stemming from the increasing trans-border flow of data.\(^\text{17}\)

Canada’s current Privacy Commissioner, Jennifer Stoddart, has taken an active role in these respects, both nationally and internationally. For instance, Ms. Stoddart was the first data protection authority to conduct a comprehensive investigation of the privacy policies and practices of the popular social networking site, Facebook. More recently, she found that Google Inc. contravened Canadian privacy law when it collected personal information from unsecured wireless networks for Google StreetView. She has also led numerous important investigations pertaining to the information practices of the federal government.\(^\text{18}\)

\(^{16}\) A similar process exists in provinces having enacted “substantially similar” legislation, i.e. Alberta, British Columbia, Ontario (for personal health information only) and Quebec.

\(^{17}\) “Mandate and Mission, supra note 15.

\(^{18}\) “Biography of Jennifer Stoddart” online: Office of the Privacy Commissioner of Canada

http://www.priv.gc.ca/aboutUs/bio_e.cfm.
On the international stage, Ms. Stoddard continues to collaborate on global privacy issues with, for example, both the Organization for Economic Cooperation and Development (OECD) and with Asia-Pacific Economic Cooperation. In these capacities she recently led an unprecedented collaboration involving ten other data protection authorities who issued a joint letter reminding online companies, such as Google, of their responsibility to respect privacy laws in countries where they launch their products or services.

D. Brief Overview of Canadian Privacy Law in Comparative Context

Canadian privacy law has often been described as a “middle ground” between Europe and the United States. Below is a brief overview of the respective jurisdictions and their distinct approaches to privacy protection.

(i) The European System

There are a number of striking similarities between the Canadian and European approaches to privacy. Specifically, Canada has joined European Member States in affirming the OECD Guidelines on Privacy by incorporating them into the ten privacy principles articulated in schedule 1 of PIPEDA. This principles-based approach was also adopted in certain provinces within their privacy legislation. These initiatives were in part motivated by the European Union’s Directive 95/46/EC on Data Protection, which prohibited EU Member States and their enterprises from transferring personal information to a non-member if that

---


country’s laws did not adequately guarantee protection of that information.\(^{22}\) PIPEDA has been carefully drafted to be compatible with the Directive on Data Protection and has been officially recognized by the EU as providing an adequate level of protection. Consequently, privacy law has not produced barriers to trade between Canada and European Member States.

\textit{(ii) The American Approach}

The American approach to privacy stands in contrast to the Canadian and European emphasis on principles-based legislation and centralized supervision. In the U.S. privacy protection is described as piecemeal and a “patchwork quilt,” as it is found in myriad sources, including the common law, constitutional provisions, as well as federal and state legislation.\(^{23}\) The European Union has taken the position that the American approach to privacy regulation provides an inadequate level of protection under the Directive on Data Protection. Accordingly, organizations operating in the EU are prohibited from freely transferring personal information to the U.S.

To facilitate the transfer of data, the EU and the U.S. Department of Commerce developed the Safe Harbor framework, which allows U.S. organizations to voluntarily self-certify that they are in compliance with seven key principles.\(^{24}\) These principles are consistent with the EU’s “adequacy” standard. Organizations that self-certify as compliant with the principles and fail to abide by them may be subject to an enforcement action by U.S. regulatory authorities.

\(^{22}\) Holmes, supra note 3 at p. 3.

\(^{23}\) Avner Levin and Mary Jo Nicholson “Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground” University of Ottawa Law & Technology Journal 2:2 (2002) at para. 3.

\(^{24}\) See U.S. Department of Commerce:  \text{http://www.export.gov/safeharbor/}.  

E. Privacy Law and Social Media in the Employment Context

The proliferation of social media such as Twitter, Facebook, and YouTube has compounded privacy law issues by making vast amounts of personal information available to potentially countless persons and organizations. For instance, depending on an individual’s knowledge and manipulation of the media’s privacy settings, tweets, Facebook postings and individual profiles containing comments, phone numbers, relationship statuses, names, personal photos, employment information, etc., may reach as far that individual’s friends, his or her friends of friends, their professional network or city. Open display settings make a person’s social media activity available to all 500 million Facebook users or the 200 million odd users in the Twitterverse. Traditionally protected dissemination channels have been rendered porous by personal computers, tablets, smart phones and applications that enable individuals to transmit emails, conversations, blog posts and comments, photos, PDF files and word documents containing all types of information to any person, at any time and from any location.

Made conspicuously absent by these relatively sudden developments, moreover, is the formerly obvious distinction between an individual’s professional and private life. Briefly, the ignorance of social media’s expanse, coupled with the sense that its use is analogous to private interaction among friends—albeit a much larger group of friends—has led to confusion about whether that use should be protected as private or recognized as public. As a result, individuals have attracted liability—and certainly notoriety—for social media activity they believed to be private, but that was held to be public.

The use of social media in the workplace raises privacy implications for both employees and employers. Specifically, two aspects of social media’s potential involvement in
the employment relationship are worth mentioning. On the one hand, employers who provide employees with computer and internet access have an interest in ensuring that their equipment is used to enhance workplace productivity. Accordingly, employers may be inclined to engage in monitoring internet and social media use in the workplace, which would make them privy to personal information about their employees. In these circumstances, an employer will usually inform employees of the company’s policy on personal use of company resources, and take measures to supervise compliance.

On the other hand, where employees may remain ignorant of this fact, they may use the Internet or social media in ways that jeopardize the employment relationship. For instance, employees may feel free to make disparaging comments about their employer or co-workers using social media such as Facebook, believing that such activity will remain private. Depending on the employee’s privacy settings or friend list, however, such comments may have numerous unintended viewers. In essence, social media’s ability to export personal information from the private sphere to the public creates tensions in the employment context.

Accordingly, employers and employees may deal with privacy issues at all stages of the employment relationship: during the pre-employment screening of applicants; in the course of an employee’s conduct at work; and, though perhaps most surprisingly, in the course of an employee’s conduct outside of work.

(i) Pre-employment

Employers may be tempted to rely on social media websites such as Facebook as screening tools during their recruitment processes. However, such a practice may become problematic if it replaces a formal and thorough reference check.25 Employers should be aware

---

that the content of social media website may contain inaccurate, distorted or out of date personal information about job applicants and should be cautious about relying on that information.26 Employers may run also into trouble if it is revealed that they gathered information or turned down an applicant based on discriminatory grounds. For instance, depending on the nature of a prospective employee’s privacy settings, an employer may be able to access an array of personal information about the employee, including: ethnicity, sexual orientation or religion. Employers should guard against using personal information gleaned from social media in a discriminatory way, as doing so opens the door to human rights claims from prospective employees.

(ii) At the workplace

In Alberta Union of Provincial Employees v. Alberta, an employee of the Alberta Public Service had been dismissed after it was revealed that she authored a publicly accessible blog that was severely critical of her co-workers and immediate supervisor.27 The grievance arbitrator, the Alberta Court of Queen’s Bench and the Alberta Court of Appeal all ruled that the employee’s conduct breached the employment relationship and served as grounds for dismissal. A grievance arbitrator considered a similar situation in Government of Alberta and Alberta Union of Provincial Employees (Grievance of R).28 In that case, the employee defended her blog postings as humorous and as a valid exercise of her right to freedom of expression. The arbitrator rejected the employee’s assertions and held that the comments were very damaging and serious enough to undermine the employment relationship beyond repair, justifying the discharge.

26 “Fact Sheet: Privacy and Social Networking in the Workplace (May 2009)” online: Office of the Privacy Commissioner http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm
27 2009 ABCA 266.
In *Chatham-Kent (Municipality) v. CAW*, an employee in a senior’s residence was dismissed after posting negative and inappropriate comments about management, colleagues and residents on a personal blog.\(^{29}\) In upholding the employee’s dismissal, the arbitrator noted that the employee made two major errors: firstly, in making her tasteless comments on a publicly accessible website—not the private one she had evidently wished to create; and secondly, in breaching the employer’s confidentiality agreement, by including personal information about the residents on her blog. The arbitrator had no trouble finding that the employee had provided the employer with ample cause for termination.

*Lougheed Imports Ltd. (West Coast Mazda) and United Food and Commercial Workers International Union, Local 1518*, is another frequently mentioned case.\(^{30}\) There, three unionized employees who made violent and obscene Facebook comments about their employer were terminated. The union alleged that the terminations were motivated by anti-union sentiment as all three employees had been involved in the UFCW’s certification campaign and the employer had been recently certified. The British Columbia Labour Relations board calculated that the comments were made to an audience of as many as 100 to 377 Facebook friends, including many former and current employees. Accordingly, in ruling that the employees were validly terminated the Board concluded that the employees’ Facebook comments were “akin to comments made on the shop floor” and “amount[ed] to insubordination”.

On occasion, however, arbitrators have also afforded the employee a measure of leniency. Such was the case in *EV Logistics v. Retail Wholesale Union, Local 580 (Discharge Grievance)*, where the arbitrator assessed the discharge of a 22 year old employee who had


\(^{30}\) *Lougheed Imports Ltd. (West Coast Mazda) v. United Food and Commercial Workers International Union, Local 1518*, 2010 62482 (BC L.R.B.).
published racist postings and disparaging comments about his employer on a publicly accessible blog.\textsuperscript{31} Though the arbitrator agreed that discipline was appropriate, he nonetheless ordered the employee to be reinstated due to his young age, candid apology, and honesty at the hearing. In light of these factors, the arbitrator held that notwithstanding the seriousness of the employee’s comments, the employment relationship could be repaired.

Another line of cases illustrates how, in the absence of a clearly defined and enforced policy on Internet use, employers may experience difficulties dismissing employees for online misconduct. In \textit{Consumers Gas and Communications, Energy and Paperworkers Union}, an employee was dismissed after sending an email containing pornographic video clips, which caused the employer’s entire computer system to crash.\textsuperscript{32} An inquiry revealed that the employee had sent, received, stored and deleted similar pornographic files on other occasions over an extended period of time. The arbitrator agreed that the employee should be disciplined but held that dismissal was excessive—the company had made no previous attempt to administer or inform employees of its Internet policy. Accordingly, the employee was reinstated subject to a one-month suspension.

Similarly, in \textit{WestCoast Energy Inc. and Communications, Energy, and Paperworkers’ Union, Local 686B} the arbitrator reinstated an employee who had been dismissed for sexually harassing a co-worker via the company email system.\textsuperscript{33} In making this determination, the arbitrator held that in light of the employer’s failure to outline and enforce its policy prohibiting personal use of company computers, the employee’s conduct, however inappropriate, could not constitute just cause for termination. The employee was reinstated subject to a six-month suspension.

\textsuperscript{31} [2008] B.C.C.A.A.A. No. 22.  
(iii) **Outside the workplace**

In *Teck Coal (Cardinal River Operations) and United Mine Workers of America Local 1656*, an employee was terminated for regular absenteeism associated with excess drinking and partying. While the employee defended his absence on medical grounds, the employer provided evidence demonstrating the employee’s lack of credibility—including evidence gleaned from the employee’s Facebook page, indicating that the latter was “in the city and ready to party” during the period of his absence. In upholding the dismissal, the arbitrator ruled that the employer had good reason to lose all confidence and trust in the employee.

In *Brisindi and STM (Réseaux des Autobus)* the Quebec Commission des Lésions Professionnelles denied an employee’s claim to workplace injury compensation, after reviewing evidence obtained by the employer from the employee’s Facebook page. Based on the Facebook evidence, it was found that the employee had lied about the nature and extent of his injury—in the two months following the alleged accident, he had participated in four triathlons.

Similarly, in *Marchese and Garderie Les “Chats” Ouilleux Inc.* a day care worker who had allegedly pulled a muscle while carrying a child in the course of her duties applied to the Quebec Workplace Health and Safety Commission for workplace injury compensation. While the Commission accepted the employee’s claim, the employer soon appealed. The employer produced photos found on the employee’s Facebook profile, showing her vacationing in the Dominican Republic, swimming, doing aerobics and posing in positions that

---

35 *Brisindi and STM (Réseaux des Autobus)* 2010 QCCLP 4158.
36 *Marchese and Garderie Les “Chats” Ouilleux Inc.*, 2009 QCCLP 7139.
contradicted the nature and extent of her alleged injury. Accordingly, the employee’s entitlement to worker’s compensation benefits was overturned.

**F. Recent Statements by the Privacy Commissioner of Canada**

These cases illustrate that the traditional notion of public and private spaces is changing. Indeed, the Privacy Commissioner of Canada has admitted as much in her most recent Report of May 2011. In her report, the Commissioner frequently refers to social media’s role in “blurring the public-private divide” and in “shifting expectations of privacy”. She also reflects on the apparent contradiction of social media participation, namely, that at the same time as individuals “are embracing [social media] and sharing or creating increasing amounts of personal information, they still say that value privacy”. Later, the Commissioner suggests that beyond posing risks to individual reputations, social media could threaten businesses as a whole. She notes that companies may eventually be held responsible for improper employee disclosures or misconduct, and that whole institutions might be thrown into disrepute. The timing of the Commissioner’s pronouncements in May 2011 was nothing short of clairvoyant.

**G. The Vancouver Riots and the Weakening of Expectations of Privacy**

In the hours following the Vancouver Canucks’ NHL Stanley Cup final loss to the Boston Bruins, citizens of Vancouver took to the streets. A riot eventually broke out in which a gang of troublemakers torched and flipped police cars, looted stores, and laid public garbage

---


38 Ibid. at p. 17.

39 Ibid.
bins and toilets on their sides. In a horrifying display, the rioters turned the city upside down, as they had also done in 1994—the last time Vancouver reached the Stanley Cup final.

A central difference in the reactions to the two otherwise similar episodes rests in the new role played by social media. Using smartphones, hundreds documented the events by uploading photos and videos to various social media websites, as well as through real-time tweets and Facebook status updates. Soon there was a wealth of evidence and citizens, spurred on by remarks from both the city mayor and the Premier of the province, began contributing to the law enforcement effort. As the matter came within the context of a police investigation, there was no need under Canadian privacy law for individuals to obtain consent for the collection, use and disclosure of potential rioters’ personal information. In a particularly ironic twist, Facebook friends began outing Facebook friends.

Identified rioters and others who blogged in approval of the riots were ferociously denigrated by thousands of social media participants who used “public shaming” websites—whether via blog or Facebook groups—to voice their contempt. The ripples of disgust soon enveloped stores whose employees had been implicated in the riots. Several employers received hundreds of angry emails and phone calls threatening boycott if they refused to discipline their employees. Several employees were fired and other employees were disciplined as a result.

On June 22nd the Canadian Broadcasting Corporation reported that, “public outrage over the looting during the riot is taking its toll not only on those outing as offenders but also, in many cases, their employers. Several local companies are scrambling to save their

---


reputations after employees have been identified in on-line photographs and videos.” The CBC went on to report that, “experts say public pressure is forcing many companies to fire employees involved in the riots. [An employee who] worked at Burrard Acura for two years. When her employer say a video of her looting - he fired her on the spot.”

The aftermath of the Vancouver riots thus poses significant questions for both privacy and employment law in the age of social media. The most obvious of these relates to the seismic weakening of the expectation of privacy: can the personal information contained in social media still be considered private? More importantly, when smartphone technology prevents individuals from controlling how their personal information finds its way onto the world wide web, is there any room left for the notion of privacy at all? The Vancouver riots suggest not. Privacy settings alone could not prevent such information from reaching the public; and privacy law helped bring this information to the state. Accordingly, some experts fear that the notion of privacy in general is vanishing. And while others are concerned that the mobilization of social media by law enforcement agencies may affect the right to a fair trial, the use of “public shaming” web sites makes clear that social media does not need the criminal justice system to inflict permanent stigma.

As for employment law, the Vancouver riots put a different spin on the classic question as to whether an employee’s off-duty conduct can result in termination. In the context of the Vancouver riots firings, employers will still have to show that the trust and confidence essential to the employment relationship has been irreparably undermined; or, that maintaining the employment relationship will directly harm an employer’s interests. The feasibility of either strategy is a matter of evidence. Accordingly, employers cannot rely on hearsay or

incriminating photographs that assign guilt by association alone. Moreover, companies with policies relating to the use of social media or conduct off the job will likely have more leeway to fire employees who participated in the riots or who made comments approving of them. Whatever the case, it is clear that social media has the potential to widen the nexus of the employment relationship significantly beyond the “shop floor”. The question to be resolved, then, is, where does it stop?