Carving Out Space:
Social Media & Expectations of Privacy in the Workplace

By Lisa Stam, Baker & McKenzie LLP[1]

May 2013

Social media has busted open how we communicate with each other, how we buy things and how we announce big events - and the results have infiltrated all corners of the workplace. This paper sets out a brief update of the key developments in social media, technology and privacy in the workplace over the last half year or so. The topics covered in this paper are:

1. Expectation of Privacy in the Workplace
    (a) *Jones v Tsige*
    (b) *R v Cole*
2. BYOD – The Continued Blurring of Our Personal and Professional Lives
    (a) Benefits of BYOD
    (b) Risks and Costs of BYOD
    (c) Workplace BYOD Policies
3. Who Owns Social Media Content?
    (a) *Eagle v Morgan et al*
    (b) *@PhoneDog_Noah*
    (c) Netflix – Social Media's Impact on the Markets
    (d) Securities & Disclosure in Canada
4. Conclusion

1. Expectation of Privacy in the Workplace

The theme that threads it way throughout the caselaw and social media headlines is the evolving concept of the *expectation of privacy*. As more information about our lives shows up online, expectations of privacy continues to increasingly be shaped by the impact and breadth of social

[1] Connect with Lisa on Twitter @lisastam or visit her employment law blog, Employment & Human Rights Law in Canada: http://www.canadaemploymenthumanrightslaw.com/

media. Our individual expectations of privacy are shaped by our workplace, our personal beliefs and our broader social context.

The law is in a state of flux on privacy in the workplace, as adjudicators, employers and the marketplace struggle to find the right balance between managing the workplace while respecting employee privacy rights. Gen-Y and the generations coming up after Gen-Y increasingly demand a separation between their personal and public lives online, and this has increasingly been spilling into the workplace.

(a) Jones v Tsige

In 2012, two appeal level cases solidified the expectation of privacy in the workplace. In January 2012, the Ontario Court of Appeal released *Jones v Tsige*[2], the case that brought the new tort of intrusion upon seclusion to Canada. In *Jones,* one employee, Tsige, accessed the other employee's bank account 174 times over four years. When Jones found out, she complained to her employer, who subsequently enforced the applicable workplace policies and suspended Tsige for one week without pay, and denied Tsige a bonus.

In addition to the internal workplace remedy, Jones sued Tsige in a civil action for a breach of privacy. Although she lost at the trial level, she won at the appeal level and was awarded $10,000 in damages for the breach. Justice Sharpe held that the facts "cry out for a remedy", and he recognized Jones' right to bring an individual civil action for the invasion of privacy.[3]

Based on the US' *Restatement (Second) of Torts (2010)*, the three elements of the tort of the intrusion upon seclusion are:

a) Defendant's conduct must be intentional or reckless;

b) Defendant must have invaded the plaintiff's private affairs or concerns without lawful justification; and

[2] *Jones v. Tsige*, 2012 ONCA 32, http://www.canlii.org/en/on/onca/doc/2012/2012onca32/2012onca32.pdf
[3] *Ibid*., para. 69.

c) A reasonable person would regard the intrusion as highly offensive, causing distress, humiliation or anguish.[4]

Given that employees face the ongoing statutory gap in Ontario that carves out employee information from the definition of "personal information" protected by privacy law, introducing the new tort into Ontario now avails individuals of a civil action upon which to base a claim in the courts.

Notably, the Ontario Court of Appeal did not include proof of harm to a recognized economic interest as an element of the cause of action[5], but did include a damages cap fixed at $20,000.[6]

The court acknowledged its role in catching the law up with the privacy interests that society already values, concluding that:

> [65] In my view, it is appropriate for this court to confirm the existence of a right of action for intrusion upon seclusion. Recognition of such a cause of action would amount to an incremental step that is consistent with the role of this court to develop the common law in a manner consistent with the changing needs of society.[7]

Until the *Jones* case, there were inconsistent lines of cases speaking to the issue of a civil cause of action based on the breach of privacy. The court in *Jones* noted the fact that technology poses new and greater threats to privacy interests:

> [67] For over one hundred years, technological change has motivated the legal protection of the individual's right to privacy. In modern times, the pace of technological change has accelerated exponentially. Legal scholars such as Peter Burns have written of "the pressing need to preserve 'privacy' which is being threatened by science and technology to the point of surrender": "The Law and Privacy: the Canadian Experience" at p. 1. See also Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967). The internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic data bases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled, and the nature of our communications by cell phone, e-mail or text message.
>
> [68] It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been

[4] *Ibid.*, para. 70.
[5] *Ibid.*, para. 71.
[6] *Ibid.*, para. 87.
[7] *Ibid*., para. 65.

> protected for hundreds of years by the common law under various guises and that, since 1982 and the *Charter,* has been recognized as a right that is integral to our social and political order.[8]

(b) *R v Cole*

The second important development in privacy law in 2012 was the Supreme Court of Canada's decision in *R. v Cole*, [9] released in October 2012. In this case, a high school teacher was caught with child pornography on his work-issued laptop. The data was found through a routine IT maintenance check. The high school copied the data, provided a copy to the police and conducted its own internal investigation. Based on its clearly worded, regularly reviewed workplace policies on appropriate computer use, the teacher was terminated from employment.

The crown pressed criminal charges, and the court decision at issue speaks to whether the police had a *Charter* right to obtain the data without a warrant. The court held that the police had violated the employee's *Charter* right to be free from unreasonable search and seizure (section 8), but that the breach was justified in the circumstances and would not bring the administration of justice into disrepute (section 24). The court ordered the evidence to be admitted in a new trial.

The three key employer take-aways from the *Cole* decision are:

(a) that an employer cannot waive an employee's consent regarding privacy rights by handing material over to the police without the police having a search warrant;
(b) an employee has an expectation of privacy in the workplace, that can be diminished, but not eliminated by a workplace policy[10]; and
(c) an enforceable and well used workplace policy will keep employers out of hot water when attempting to discipline or terminate someone based on their inappropriate computer use.

While *Cole* is not a social media case *per se*, it speaks to the issue of the expectation of privacy on a work-issued computer. The case represents a clear message from the highest court: employers cannot eliminate an employee's expectation of privacy on a workplace computer.[11] A workplace policy can articulate the parameters of computer use, and the breach of such use can

[8] *Ibid.*, paras. 67-68.
[9] 2012 SCC 53, [2012] 3 S.C.R. 34, http://www.canlii.org/en/ca/scc/doc/2012/2012scc53/2012scc53.html
[10] *Ibid.*, paras. 1-3.
[11] *Ibid.*

amount in termination of employment, but there is now a finding from the highest court that there remains a residual expectation of privacy in the workplace.

This is in contrast to privacy law in the US, where employers generally have more latitude to eliminate expectations of privacy. It is also in contrast to much of Europe, where employee privacy rights are strong and sometimes seemingly untouchable. Canada falls somewhere in between.

If there was any ambiguity about where the law stood in Canada, *R v Cole* and *Jones v Tsige* together have clearly established that there is an expectation of privacy in the workplace, albeit one that can be significantly altered – but not eliminated - through effective workplace policies.

2. BYOD – The Continued Blurring of Our Personal and Professional Lives

The result of this articulation in our privacy law that employees have an expectation in the workplace is that our personal and professional lives continue to be blurred. The blurring only further reinforces the disconnect that often exists between Gen-Y and their managers. When a younger worker asserts a right to privacy in their personal social media content on a work-issued device, they are shaping the evolution of privacy that increasingly agrees with them.

The "bring your own device" (BYOD) development in many workplaces is a natural extension of this blur between our personal and professional lives – and it is being driven largely by the role of social media in peoples' personal *and* professional lives. Many workers want the ease of staying in touch with friends, colleagues and family on their device, while plugging into their employer's system to be able to also stay on top of work emails and documents.

Additionally, for those engaging in any social media in their professional lives – whether directly as a term of employment, or indirectly as a method to network and stay on top of industry news – it is cumbersome and inefficient to handle various devices.

The demand for BYOD programs is coming from all corners of the organization, including both tech-savvy young workers as well as C-Suite employees[12] who want the convenience and efficiency of a seamless electronic infrastructure.

(a) ***Benefits of BYOD***

There are a number of benefits to permitting a BYOD program in the workplace, including:

i. **EMPLOYEE REQUESTS:** The most obvious benefit to embracing BYOD is employee engagement and retention. If you are in an industry full of creatives, Gen-Y or tech savvy employees, a BYOD program may already be a non-starter. On the other hand, if you are in a necessarily conservative industry such as the military equipment manufacturing industry, it is likely also non-starter that security issues may outweigh any potential benefits. For the many companies in between these two extremes, employee engagement and retention may be one of a number of benefits to consider.

ii. **CLIENT OPTICS:** Certain clients in certain industries may have a preference for one type of device over another. If one of your employees regularly works with a Blackberry dependent tech client in Waterloo, the BB10 may be the preferred device for that employee. For other employees regularly travelling to Cupertino, the iPhone may be smarter. A BYOD program gives employers the flexibility to match business and marketing needs.

iii. **INCREASED PRODUCTIVITY:** BYOD may positively impact employee productivity. Letting people connect their tablet to the company email and document system may facilitate convenient and more frequent after hours work. Rather than lugging a cumbersome laptop home, employees can use their tablet to finish up a document or clear out their email after the kids go to bed. Business travellers, trade show attendees and salespeople on the road all may find BYOD a critical piece to maintaining productivity out of the office.

[12] For example, see an industry study on the increased BYOD demand from the C-Suite at http://www.avanade.com/us/about/avanade-news/press-releases/Pages/global-survey-companies-enable-employee-use-of-consumer-technologies-report-positive-impact-on-sales-page.aspx

iv. **COLLABORATION:** Linking up devices may encourage people to connect together more frequently, leading to more collaboration and more effective communications. This will especially be true with Gen-Y employees who have a greater comfort around developing and nurturing meaningful relationships through technology.

v. **COMPANY COST SAVINGS:** An obvious bottom line benefit is that the company is no longer on the hook to pay for the hardware. Employees insisting on their own type of device who want to simply connect what they already have can eliminate a line item in the company's technology budget.

(b) Risks and Costs of BYOD

While there are a number of benefits, there are just as many risks and costs, each of which will impact an organization differently, depending on the industry and workforce demographics. The risks and costs include the following:

i. **INCREASED TECHNOLOGY COSTS:** While BYOD may eliminate some hardware costs, your IT team now has to be up to speed on more than one system. This may involves costs for more than one security regime, as well as ongoing training of your IT team to support different software and hardware requirements.

ii. **OVERTIME EXPOSURE:** Overtime claims are a significant risk for employers of salaried employees. Although an hourly employee generally has clearly defined work and easy to track parameters, many salaried employees are compensated and expected to simply get the job done. Thus, after-hours productivity may create exposure for unapproved and unintended overtime pay. The slow death of the 9-5 work day and increasingly blurred lines between work and play require clarity around expectations for after-hours work. BYOD could mean more non-work related activities by day and more work related activities by night.

iii. **CONFIDENTIALITY:** Not every position is BYOD appropriate. For positions that involve particularly sensitive information or in a smaller company where there are not

sufficient technical resources to let one employee have their own technological infrastructure, the risks and costs may outweigh the benefits.

Weighing the risks, costs and benefits of embracing BYOD will vary from industry to industry, and company to company. The reality is most employees already have some sort of device in their pocket, already putting the company at risk of inadvertently (or deliberately) tweeting, posting or emailing out confidential information during or after work hours. Pulling that device into workplace and setting up transparent and engaging policies may help mitigate the risks of a phenomenon that will likely continue to gather speed, with or without workplace blessing.

(c) Workplace BYOD Policies

If implementing a BYOD program, it will be important to set out policies that speak to the company's expectations of use in the workplace. The following is a list of provisions to consider including in a workplace policy:

- exactly what devices are permitted;
- that specific security programs should remain updated;
- that work-related content developed on a personal device is the intellectual property of the company;
- that the security of the company server will prevail when determining when to remote wipe a lost device;
- that the employee should have no expectation of privacy in any device plugged into the company system (in an attempt to diminish, not eliminate the expectation of privacy);
- clear articulation of expectations for use after hours to deal with potential overtime claims head-on;
- that the BYOD program is a privilege of which the employer reserves the right to revoke should an employee abuse the BYOD program; and
- a termination protocol that sets out a checklist should an employee resign or be terminated, including the steps IT will take in advance of any terminations.

BYOD is the manifestation of many employees' willingness to forego some privacy in the workplace in exchange for convenience, potential cost savings and the use of her or his preferred device. We are in a period of legal flux around these issues. Workplace policies that clearly articulate the parties' expectations in the face of this quickly evolving reality will greatly assist the negotiation of disputes that may arise in the future.

3. Who Owns Social Media Content?

Determining the ownership of social media content is another prevalent way in which social media has blurred the line between our personal and professional lives. When using social media to promote one's company, employer or business venture, our personal and professional lives continue to intertwine, and a person's brand may often become the company. Where would Virgin be without Richard Branson? Apple without the late Steve Jobs? Microsoft without Bill Gates? Facebook without Mark Zuckerberg? As people increasingly become their own brand and an ambassador of the company, it becomes increasingly difficult to separate individual social media commentary from commentary on behalf of the company.

(a) Eagle v Morgan et al

In the Pennsylvania case *Eagle v Morgan et al*,[13] Dr. Linda Eagle sued her former employer for taking over her LinkedIn account[14] for nearly a month after she was terminated from the company. Dr. Eagle had co-founded Edcomm, and built up a successful banking education business through various tools, including an active LinkedIn account. Certain company employees maintained the LinkedIn account and had open access to her password.

Dr. Eagle sold her company in October 2010, and by the following June 2011, she and two other original employees were terminated from employment. Upon termination, Edcomm immediately changed the password to Dr. Eagle's LinkedIn account, replaced her photo with the new employee who took over her position, and changed most but not all content. The connections

[13] *Eagle v. Morgan*, 2013-11-4303 (E.D. Pa. 2013), http://www.gpo.gov/fdsys/pkg/USCOURTS-paed-2_11-cv-04303/pdf/USCOURTS-paed-2_11-cv-04303-4.pdf
[14] http://www.linkedin.com/in/lindaeagle

remained, and Edcomm asserted that they were company property that Edcomm had the right to "mine" for business.

Dr. Eagle immediately objected to her LinkedIn being "hijacked" by Edcomm, and had LinkedIn take over the account when Edcomm refused to return the account to her. Within approximately a month, Dr. Eagle had regained control of her account, although she claimed she lost inbox messages during that period and over the subsequent number of months.

Dr. Eagle sued Edcomm in Pennsylvania for the following causes of action:

(a) unauthorized use of name

(b) intrusion upon seclusion by appropriation of identity

(c) tort of misappropriation of publicity

(d) crime of identity theft

(e) tort of conversion

(f) tortious interference with contract

(g) civil conspiracy to gain access to account

(h) civil aiding and abetting.

In March 2013, Dr. Eagle received the bittersweet decision in her case against her former employer, Edcomm, Inc. She won on the first three above noted claims, and failed to make out a case in the remaining five claims. Edcomm did indeed use her name in an unauthorized manner, appropriated her identity and misappropriated her publicity.

Dr. Eagle failed, however, to prove that she suffered any actual monetary losses. She could not quantify a business deal lost or not acquired during the period, or any other tangible negative impact on her reputation. As a result, while she did establish that Edcomm committed three of the eight claims made, the court awarded her $0 in damages.

Employers should be cautious in drawing any comfort from this decision. The court was rather critical of Dr. Eagle's failings as a self-represented plaintiff. Had she hired a good lawyer, she

may have better established the damages she suffered, which no doubt would have led to a different decision on the quantum of damages.

The case clearly sets out that she had some sort of property in her LinkedIn account, even though it was developed and maintained by the company's employees.

Furthermore, one of the three successful claims in the Eagle case is the tort of the intrusion upon seclusion, the new tort established in Ontario through the *Jones v Tsige* case. While this is a US case with no direct precedential value in Canada, it will no doubt be persuasive, particularly given our Court of Appeal's specific adoption of the US tort in issue.

LinkedIn promises to be the most likely battleground for precedent-setting litigation on the ownership of social media content. Unlike many other social media platforms, LinkedIn's primary purpose is the development of business. This, by definition, is often intimately connected to an individual's workplace. While each LinkedIn account is a contract between the individual and LinkedIn (ie. the company/employer is not privy to the contract), the overlap with one's employer's customer/client list is inevitable.

To the extent that a party can establish a monetary value in LinkedIn content and connections, there will be value in litigating over who owns the content and connections. While we may not quite be ready for a specific quantification of social media content, it is no doubt right around the corner.

(b) PhoneDog Noah

The *Eagle* case is one of the few cases that have gone to trial and about which we have a final disposition. Most cases settle, such as the @PhoneDog_Noah[15] case that attempted to quantify the value of Twitter followers. In that case, an employee named Noah Kravitz set up a Twitter account and amassed 17,000 followers while tweeting about his US employer's business in between various personal tweets.

[15] See my blog post on PhoneDog Noah, that includes a copy of the pleadings in the case: http://www.canadaemploymenthumanrightslaw.com/articles/social-media/

After four years at PhoneDog, Noah moved to a competitor, changed his Twitter handle to @NoahKravitz, and took his followers with him. PhoneDog sued him for:

(a) misappropriation of trade secrets;

(b) intentional interference with prospective economic advantage;

(c) negligent interference with prospective economic advantage; and

(d) conversion.

Based on "industry standards" which involved questionable metrics, PhoneDog valued each follower at $2.50. The parties settled in December 2012 and the agreement remains confidential, although we do know that Noah kept his Twitter account and continues to do so to present.

Although this case settled, it did generate a lot of online discussion about the value of social media content, as well as the often strong views on who owns social media content. Employers generally view work product developed in the course of business as their own product, as does traditional caselaw on work product and customer lists.

However, in our modern world of the mobile employee who expects to work for many employers over the course of her or his career, it seems unseemly to have one's online personality be "owned" by anyone. Such is the dilemma of collapsing our personal and professional lives into one Twitter account.

(c) Netflix – Social Media's Impact on the Markets

While there were questionable metrics involved in the @Phonedog_Noah case, and virtually no metrics in the *Eagle* case, there were big, specific numbers involved in the recent issue Netflix encountered with the US Securities and Exchange Commission (SEC). On July 3, 2012, the CEO of Netflix, Reed Hastings, posted the following on his Facebook page to his then 269,595 followers:

> "Congrats to Ted Sarandos, and his amazing content licensing team. Netflix monthly viewing exceeded 1 billion hours for the first time ever in June. When House of Cards

> and Arrested Development debut, we'll blow these records away. Keep going, Ted, we need even more!"[16]

While he was no doubt attempting to be a good cheerleader for his organization, given his role within the company and his known personality in the Valley, his Facebook status update had an immediate and impressive impact on the market: the value of Netflix shares went up 6% in one day.

The SEC immediately sent Mr. Hastings a Wells Notice, notifying him that he would be subject to an investigation because he had violated securities law that requires equal disclosure of key company information to all investors. By posting this key company information on his Facebook page, he had not disclosed equally, as not all investors were his Facebook page "followers".

On April 2, 2013, the SEC released a report[17] on the use of social media for key company information. The SEC concluded that the use of social media outlets to announce key information was in compliance, so long as investors have been alerted about which social media will be used. The SEC's press release described the trigger of this report as follows:

> The SEC's report of investigation stems from an inquiry the Division of Enforcement launched into a post by Netflix CEO Reed Hastings on his personal Facebook page stating that Netflix's monthly online viewing had exceeded one billion hours for the first time. Netflix did not report this information to investors through a press release or Form 8-K filing, and a subsequent company press release later that day did not include this information. Neither Hastings nor Netflix had previously used his Facebook page to announce company metrics, and they had never before taken steps to alert investors that Hastings' personal Facebook page might be used as a medium for communicating information about Netflix. Netflix's stock price had begun rising before the posting, and increased from $70.45 at the time of the Facebook post to $81.72 at the close of the following trading day.
>
> The SEC did not initiate an enforcement action or allege wrongdoing by Hastings or Netflix. Recognizing that there has been market uncertainty about the application of Regulation [Fair Disclosure] to social media, the SEC issued the report of investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934.

While Netflix did not suffer any penalty from the SEC, the case demonstrates how easy it is for a senior executive to get her or himself into deep water. The extent of social media's impact makes every tweet and Facebook update loaded with risk if one represents the company.

[16] https://www.facebook.com/reed1960/posts/10150955446914584
[17] http://www.sec.gov/news/press/2013/2013-51.htm

Whether or not one is the CEO, statements purportedly made on behalf of – or even about – the company may run afoul of the industry's regulator.

(d) Securities & Disclosure in Canada

It is important to note that the Canadian National Policy 51-201 Disclosure Standards[18] does not yet reference or specifically include social media as an acceptable platform to disclose key information. The said policy still requires that dissemination be made by (i) press release; or (ii) press conference with specified notice as follows:

> 3.5 (4) Companies may satisfy the "generally disclosed" requirement by using one or a combination of the following disclosure methods:
>
> (a) News releases distributed through a widely circulated news or wire service.
>
> (b) Announcements made through press conferences or conference calls that interested members of the public may attend or listen to either in person, by telephone, or by other electronic transmission (including the Internet). A company needs to provide the public with appropriate notice of the conference or call by news release. The notice should include the date and time of the conference or call, a general description of what is to be discussed, and the means of accessing the conference or call. The notice should also indicate for how long the company will make a transcript or replay of the call available over its Web site.[19]

At present, social media is thus not an acceptable channel for disclosure, and companies and their more influential or senior employees should remain wary of posting or tweeting anything that may disclose key company information regarding a Canadian company.

Whether or not a senior executive may have any expectation of privacy in the workplace, as long as a single social media post can have such a broader impact on the market – as it did in Netflix, the securities regulator will likely continue to assert its right to intervene and investigate when it deems necessary to do so.

4. Conclusion

The current social media landscape is in a fast-paced state of change, and is unlikely to slow down anytime soon. The next generation's evolving concept of expectations of privacy online, and the intersection of individual "personality" with company social media content will continue

[18] http://www.osc.gov.on.ca/en/SecuritiesLaw_pol_20020712_51-201.jsp
[19] *Ibid.*

to present unique and unprecedented challenges to how we present the company's "voice" to the marketplace. HR and Marketing will together have to figure out how to manage employees and their expectations, while remaining active and effective in the company's increasingly necessary social media space.

~ ~ ~