

employment and labour law SEMINARS | 2010

On-Line Social Networking Forums:	(Un)Welcome to the Workplace
J. Geoffrey Howard Jonathan Van Netten	
	

## On-line Social Networking Forums

Reaching Out
Reeling 'Em In
Reining 'Em In


- On-line social networking forums are a force for good and evil in the workplace:
  - Hugely expanded marketing opportunities
  - New and complex workplace risks
  - Costly distractions
  - Workplace policies lag behind the needs of the modern workplace



## On-line Social Networking Forums


Reaching Out
Reeling 'Em In
Reining 'Em In

- What, then, should today's employer know and do:
  - If using social media as a tool for recruitment
  - If using social media as a tool for marketing/promotion/selling
  - When social networking becomes social **networking**
  - When social networking is or is harmful to the employer




## Reaching Out: Recruiting and Screening Employees

- Cyber-recruiting or old-fashioned recruiting - the same issues and rules apply:
  - Information must be up-to-date and accurate
  - Must not explicitly or implicitly impose conditions that would violate human rights requirements
  - Privacy laws only permit requesting or assembling information reasonably related to prospective employment




## Reaching Out: Recruiting and Screening Employees

- Cyber-screening (formal or informal) is more problematic:
  - Potential human rights issues: knowing things you should not know about candidates can support inference of discrimination
  - Potential privacy law issues (collecting, using and retaining/destroying personal information)
  - Plain old-fashioned fairness issues, because the on-line world is inherently unreliable, often out of date
  - Taking into account any unique needs of your workplace and industry, weigh the **value of the information** to be obtained against the **risks associated with having (or not having) it**, and make a conscious choice about which risks to assume, and how to control them



## Recruiting and Screening (cont'd)

- Audit and assess current cyber-screening practices (both formal and informal)
- Establish clear protocols for the future, regarding "who, what, when, why and how" you will deal with on-line information for screening:
  - What on-line information will be accessed?
  - For what purpose (limits on use)?
  - At what stage(s) or upon what events in the hiring process?
  - Who can access it?
  - Who can it be shared with?
  - To what extent, for how long, and in what form (with what security) will it be retained, if at all protected and destroyed?



## Recruiting and Screening (cont.)



- Red light:
  - Personal information (even if relevant to character or "fit") relating to protected human rights grounds (e.g., affiliations with religious or political groups)
- Yellow light:
  - Irrelevant information that is safe to consider from a human rights perspective but not necessarily wise to collect from a privacy perspective (e.g., membership in a Jonas brothers fan club)
- Green light/yellow light:
  - Professional information (related to education, work history, work output, or experience) if relevant to the position and safe to consider or to verify C.V. information (e.g., LinkedIn)
  - Personal information (hobbies, certain personal interests, certain community involvements, "personal style" or professionalism) if relevant to character, "fit" and suitability for the job and safe to collect/consider



7

## Recruiting and Screening (cont.)

- Disclose early and upfront if you will search on-line – either ask for consent or make it clear that it will happen, so candidates can withdraw or "tidy up"

*Sample statement on recruiting Facebook page or employment application:*

**Please be aware that if you apply for a job with us, we will review all publicly available on-line information, to learn more about you**  
**Or: Check here to confirm we may review all publicly available on-line information, to learn more about you**

- Be consistent –follow the same approach for everyone, every time and have a rationale
- Only access publicly available information; never hack accounts or use subterfuge, e.g. posing as "friend"



8

## Recruiting and Screening (cont.)

- Keep personal information including internet sourced information which was freely available secured and confidential: once you have it, Personal Information Protection Act (or other privacy law) protection obligation applies
- Follow normal rules for retention, protection and destruction as required by PIPA
- PIPA requires all personal information used to make a decision (i.e. to hire/not hire) to be kept for 1 year



9

## Reeling 'Em In: Marketing, Promoting and Selling via Social Media

- **What should today's employer know and do:**
  - if using social media to market to customers and prospects (e.g., "friending" customers)
  - if employees are allowed or encouraged to blog or Twitter for or about the organization
  - about subterfuge (e.g., doing a "Guergis": posing as an uninterested party when posting on-line rave reviews about your company's latest product launch; posing as a potential customer of a competitor for industrial espionage purposes)



10

## Marketing, Promoting and Selling via Social Media cont.

- Audit and assess current practices (both formal and informal)
- Establish (and update!) clear protocols for the future, regarding "who, what, when, why and how" you will deal with on-line marketing/promotion/selling activities:
  - When can customers and prospects be contacted via on-line social networking forums?
  - When, if ever, can staff pose as outsiders or deliberately fail to disclose their relationship with your organization?
  - For what purposes?
  - Via what accounts?
  - Who can do this?
  - Who, can blog/post/tweet on behalf of the company and/or on company time, and with what limits?



11

## Marketing, Promoting and Selling via Social Media cont.

- Never allow staff to hack accounts or use subterfuge
- Require staff who link to customers/prospects via social media for work purposes to use stand-alone work-dedicated accounts
- If staff can blog or Twitter for or about your organization, be clear:
  - Whether and when they can use company time and systems to do this
  - What topics are off-limits
  - That both common sense and common courtesy must be observed in their posting
  - That content must still comply with all company policies, particularly confidentiality, public statement and harassment policies



12

## Marketing, Promoting and Selling via Social Media *cont.*

- Consider and co-ordinate branding and intellectual property protection strategies

- Make it your business to know and control what your staff say and do on-line when they are marketing, promoting and selling for your business
- Internet monitoring services are available

**gowlings**  
Law - Business - Technology

13

## Marketing, Promoting and Selling via Social Media *cont.*

**What your staff say and do on-line  
(wherever and whenever they do it) affects  
your business.**

**So, what they do is your business!**

**gowlings**  
Law - Business - Technology

14

## Reining 'Em In

- **What should today's employer know and do:**
  - About social *networking* (abstinence vs. safe sex)
  - About on-line (over)sharing of information and criticisms
    - Confidentiality and public statements
    - Reputation issues
  - About cyber-harassment and cyber-bullying of co-workers
  - About cyber-spying on employees (even if you can, should you?)

**Don't be an ostrich. Implement a practical social media/Internet policy that:**

- balances employer/employee interests, recognizes the realities of human behaviour;
- warns of employer access and/or monitoring of business devices (not just computers); and
- imposes reasonable rules and consequences.

**gowlings**  
Law - Business - Technology

15

## Next Steps

- HR, IT and management all need to be involved
- Audit and assess your workplace to:
  - identify specific risks and problems (or particularly problematic employees)
  - identify what you want or need to accomplish with any policy
  - understand the available options for addressing problems
  - then, update (or establish) clear policies/protocols for the future
- Consider:
  - Different rules for internal (intranet, wiki) vs. external forums?
  - How much time/resources do you want to spend on monitoring?

A safe sex model allows limited, reasonable personal use and access

**gowlings**  
Law - Business - Technology

16

## Social Networking and Abuse of Social Media

- **Social Networking**
  - As with any time-management issues, use practical policies, reasonable monitoring, consistent enforcement and, where necessary, progressive discipline
- **Confidentiality/Public Statements/Criticisms**
  - Requires a broad, multi-prong strategy, via some or all of written:
    - Confidentiality policies and confidentiality agreements
    - Public statement policies
    - Social media policies
    - Technology systems and equipment use policies
    - Harassment policies

**gowlings**  
Law - Business - Technology

17

## Social Networking and Abuse of Social Media (*cont'd*)

- **Confidentiality/Public Statements/Criticisms *cont'd***
  - Requires active and ongoing (re)conditioning so that staff (especially younger staff) understand:
    - All employees have a duty of loyalty that operates 24/7
    - Their freedom of expression is limited by this duty, even off-site and off-hours
  - On-line statements are *public* statements
  - Courts and arbitrators say: if their on-line conduct could affect workplace relationships or business reputation, then it is potentially disciplinable;

**gowlings**  
Law - Business - Technology

18

## Social Networking and Abuse of Social Media (cont'd)

- **Confidentiality/Public Statements/Criticisms cont'd**
  - Requires active and ongoing (re)conditioning so that staff understand:
    - Risks of both deliberate and inadvertent on-line disclosures (e.g., Facebook status reads “Am trapped in due diligence hell”)
    - They can have **no reasonable expectation of privacy**
      - (i) using the employer’s technology systems and equipment, on or off hours;
      - (ii) making publicly accessible on-line postings



19

## Social Networking and Abuse of Social Media (cont'd)

### Sample Policy

- “When you are on-line (for example, Tweeting, or blogging or participating in a chat room or in any on-line social media forum such as Facebook or MySpace), you must refrain from discussing the Company, its products, its pending or planned major changes or transactions, and its relationships, including offering opinions or speculation about our staff, customers, products, services, strategies or performance. You must also ensure that your personal views are not presented as being those of the Company.



Please understand that these rules apply whether or not you are using the Company’s systems and equipment to go on-line, whether or not you believe your statements to be “private” and/or you are using privacy settings, and whether or not your on-line activities are during working hours.”



20

## Cyber-Monitoring

- Audit and assess current practices (both formal and informal)
- Monitoring use of your organization’s systems is permissible, but notice should be given in policies and/or “on screen” under PIPA
- Monitoring “public” Internet postings also permissible:
  - if not targeting employees, but rather firm name; regular random trolling for information may be considered breach of privacy
  - or if done after receiving information supporting concern or suspicion



21

## Cyber-Monitoring (cont'd)

- Get a screen shot when you find it! Internet evidence is fragile
- Establish clear protocols for the future, regarding “who, what, when, why and how” you will deal with on-line information about current employees
- Remember to ask for the perpetrator’s side before acting, because the on-line world is inherently unreliable



22

## Summary

- Social media is here to stay, and in the on-line world, employers cannot afford to be passive
- Social media can be a superb new recruiting, marketing and engagement tool

Take the time now to:

- ✓ Conduct a careful audit and assessment of your current practices, policies and problems
- ✓ Evaluate your workplace’s culture, needs and concerns
- ✓ Make a conscious decision about what activities should (or not) and must (or not) be addressed, allowed, controlled or prohibited
- ✓ Then create, update and harmonize your policies and practices, so that they are clear, reasonable, practical and effective
- ✓ Reevaluate, adjust and update frequently
- ✓ Educate and (re)condition your staff, frequently



23

And remember...  
when things go wrong at work,  
cry over your beer,  
and not into your Twitter account.



24

**For further information:**

**J. GEOFFREY HOWARD**  
Direct Tel: (604) 891-2279  
Email: [geoffrey.howard@gowlings.com](mailto:geoffrey.howard@gowlings.com)

**JONATHAN VAN NETTEN**  
Direct Tel: (604) 443-7609  
Email: [jonathan.vannetten@gowlings.com](mailto:jonathan.vannetten@gowlings.com)

**GOWLING LAFLEUR HENDERSON LLP**  
Barristers & Solicitors  
Suite 2300 – 550 Burrard Street  
Vancouver, British Columbia V6C 2B5  
Fax: (604) 683-3558



618707

Montréal • Ottawa • Toronto • Hamilton • Waterloo Region • Calgary • Vancouver • Moscow • London