Social Media in the Workplace

Employer Liability Issues

Aiyaz A. Alibhai
Sarah G. Fitzpatrick

Miller Thomson
lawyers | avocats

Social Media in the Workplace

1. Risk Management & Sources of Liability
2. Claims involving Potential Employees
3. Claims involving Employees
4. Claims involving Former Employees
5. Privacy Issues
6. Claims involving Third Parties
7. Conclusions

Miller Thomson
lawyers | avocats

Social Media

Miller Thomson
lawyers | avocats

Social Media Video 2013

Erik Qualman · 38 videos

Subscribe 23,292

460,498

3,765 55

http://www.youtube.com/watch?v=QUCfFcchw1w

Miller Thomson
lawyers | avocats

Risk Management

- Social media has created new problems in the workplace
  - More than 14 million Canadians check Facebook every day
  - More than 400 million tweets are sent daily
  - LinkedIn has over 8 million Canadian users
- Employers can face claims from potential employees, employees, contractors and third parties
- Employers need to take proactive steps to manage risks through employment contracts and implementing policies

Sources of Liability

- Human Rights Legislation
- Personal Information and Privacy Legislation
  - British Columbia: *Personal Information and Protection Act* and *Privacy Act*
  - Federal: *Personal Information Protection and Electronic Documents Act*
- Labour Codes
- Workers' Compensation Legislation

Sources of Liability

- Intellectual property claims
  - Breach of confidence
  - Copyright infringement
  - Trade-mark infringement
- Defamation
- Inadequate contracts or policies

Claims involving Potential Employees

Miller Thomson
lawyers | avocats

Claims involving Potential Employees

"I need your Facebook password before I can hire you. If you're not on Facebook, I need you to join and post a bunch of personal stuff you don't want me to know about."

Miller Thomson
lawyers | avocats

Social Media Background Checks

- 90% of recruiters are using Web search engines to research candidates
- Interviewees are being asked to provide their social media passwords
- Interviewers are looking for information that could damage the business's reputation or illegal behavior
- But, the business may be exposing itself to liability

Social Media Background Checks

- What if the employer finds out information about a candidate that it cannot ask in an interview?
- The employer may face a human rights complaint for discrimination
- British Columbia *Human Rights Code*:
  - "A person must not … refuse to employ … a person … because of the race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical or mental disability, sex, sexual orientation or age of that person …

Social Media Background Checks

- If the employer obtains personal information during a social media background check, it may face an investigation by the Privacy Commissioner
- *Personal Information Protection Act*:
  - Personal information is information that can identify a person (e.g. name) or about identifiable individual attributes (e.g. educational qualifications)
  - Generally, an organization must obtain a person's consent before collecting, using or disclosing personal information
  - Employee personal information may be collected, used or disclosed without consent provided that it is reasonably required for the establishment, management or termination of an employment relationship and as long as notice is given to the person
  - Personal information may only be collected, used and disclosed for purposes that a reasonable person would consider appropriate in the circumstances

Social Media Background Checks

- “While we haven’t yet investigated a complaint involving surreptitious social networking background checks, my feeling is that [the legislation] would prevent this kind of collection of personal information”
  - Elizabeth Denham, BC Assistant Privacy Commissioner in 2010 (current Privacy Commissioner)

Social Media Background Checks

- The BC NDP was investigated by the Privacy Commissioner for requiring leadership candidates to provide their social media passwords
  - Consent was obtained
  - But, the information was not used for purposes that a reasonable person would consider appropriate in the circumstances:
    - Large amounts of personal information were collected that may be outdated, irrelevant or inaccurate;
    - Passwords are particularly sensitive information; and
    - Information was collected about third parties who did not give consent

(BC OIPC Investigation Report, 2011)

Negligent Hiring

- At the same time, employers need to do their homework on potential employees
- If an employee has history that indicates he or she may be violent or untrustworthy, the employer may be liable if he or she harms someone during their employment
- *Wilson v Clarica Life Insurance Co*, (2002, BCCA)
  - Company was liable for an agent who sold life insurance policies and defrauded a widow out of $260,000
  - The court found, among other things, that the employer was negligent in hiring the agent
    - The employer had not checked the references with the agent's previous employers
    - The agent had had committed theft and fraud in previous employment

Claims involving Employees

Harassment and Cyber-Bullying

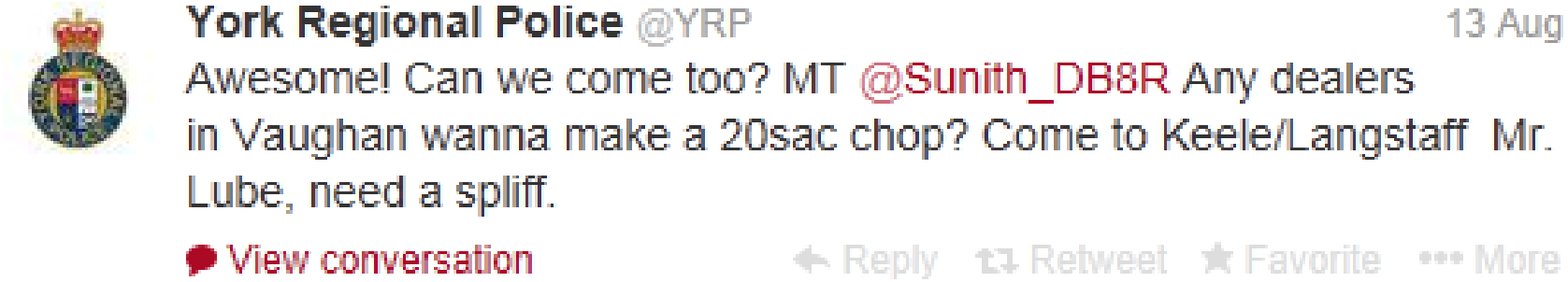
- The rise of social media has created a number of new avenues for bullying
- Bullying by e-mail, internet and social media use during work hours or after work hours may be considered harassment in the workplace
- *Perez-Moreno v. Kulczycki* (2013, HRTO)
  - An employee made Facebook comments and sent messages to co-workers calling her manager a “dirty Mexican”
  - The tribunal found that workplace-related postings on the Internet was harassment in employment under the Code
  - As the employer was not named in the proceeding, the tribunal could not order the employer to provide any remedies

Harassment and Cyber-Bullying

- Employers can be vicariously liable for harassment and discrimination by employees in the workplace
- In November 2013, WorkSafeBC implemented new policies that require employers to take steps to prevent and address bullying and harassment including:
  - Developing a policy statement
  - Developing and implement procedures for reporting incidents and complaints

At Work Behavior

- Can employees be disciplined for inappropriate online behavior during work hours?
- In August, a Mr. Lube employee asked for a marijuana dealer to come to the shop on Twitter
  - The York Regional Police tweeted in response and notified his employer
  - Mr. Lube fired the employee



At Work Behavior

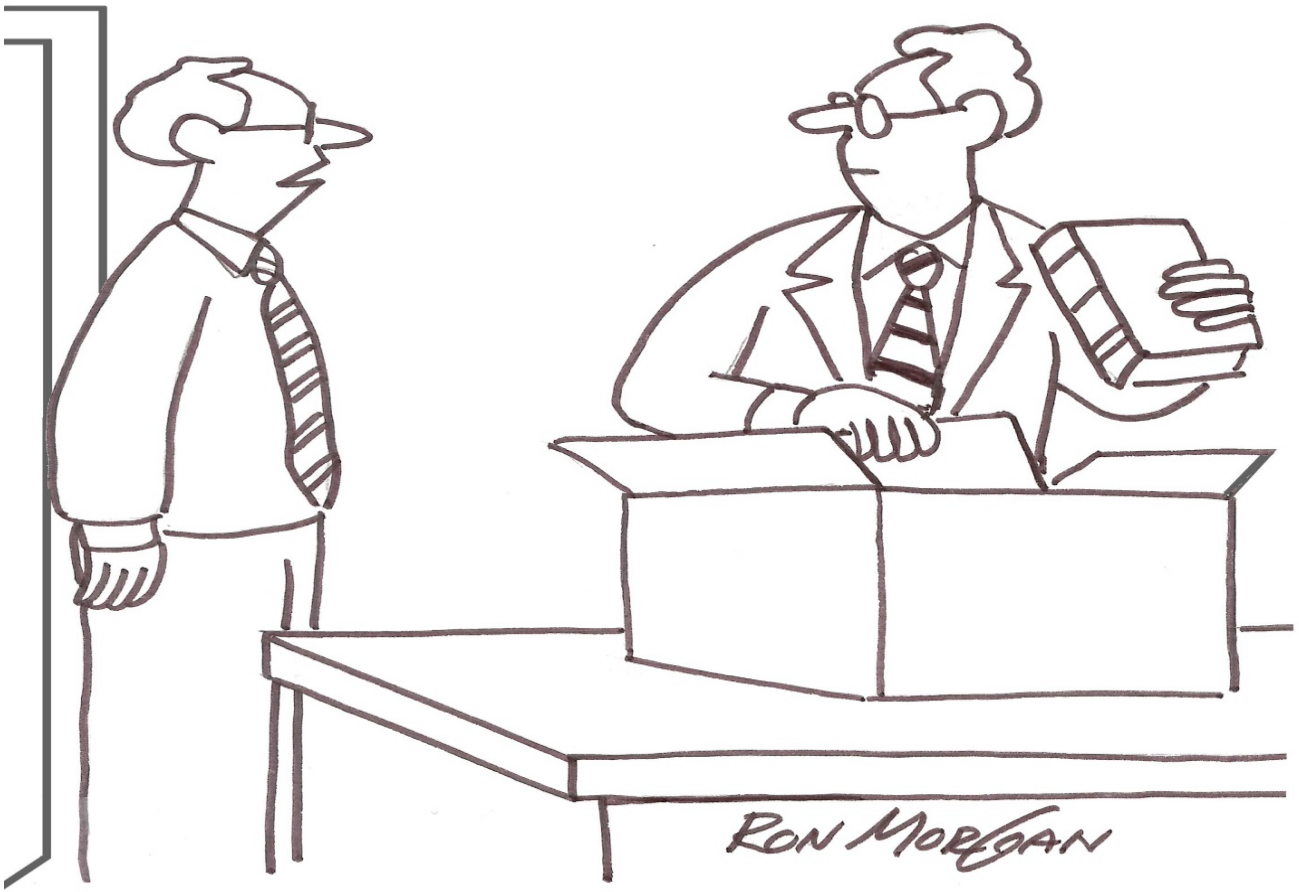
- The employee's conduct has to be sufficiently egregious for the employer to have cause to terminate their employment
- *Health Employers' Assn. of BC v. Health Sciences Assn. Of BC* (2011, BCCAAA)
  - Vic Cheema was terminated for excessive internet use
  - Employer argued Cheema committed "time theft"
  - Arbitrator found no time theft because Cheema attended work, responded to demands and was prompt and efficient
  - Arbitrator found Cheema breached the Electronic Communication Policy by using the internet for personal use during work hours and substituted a suspension of 15 working days

Breach of Confidentiality

- Social media sites are places where information is easily exchanged
- What if employees inadvertently disclose confidential information about the employer and clients?
- *Chatham-Kent v National Automobile, Aerospace, Transportation & General Workers Union of Canada* (2007, OLAA)
  - A nursing home terminated an employee who published information and pictures of residents and made inappropriate comments about residents on a public blog
  - The arbitrator found that the posts constituted a serious breach of confidentiality in circumstances where there is an elevated duty to ensure privacy
  - The arbitrator found the employee breached her confidentiality agreement and upheld the termination

Claims involving Former Employees

Claims involving Former Employees



"Before you leave, we have to do a brain scan to see if you're taking any intellectual property with you."

Miller Thomson
lawyers | avocats

Ownership of Social Media Accounts

- Employees may manage social media accounts for their employers as part of their responsibilities
- These social media accounts can be valuable because of the number of followers
- Who owns a social media account set up during the employee's employment?

Ownership of Social Media Accounts

- *Eagle v Morgan* (2013, E.D. Pa)
  - The company changed the password to a former employee's LinkedIn account, removed her name and picture from her profile
  - Court found the company had illegally taken control of the account and committed an unauthorized use of the former employee's name
  - But, the former employee was awarded $0 in damages because she could not point to a single contract, client, prospect or deal lost as a result of her lack of access
- *PhoneDog LLC v Kravitz* (2011, N.D. Calif.)
  - Employee kept his Twitter account after leaving the company which had 17,000 followers
  - The company sued for illegally using trade secret
  - The parties settled out of court

Confidential Information

- Confidential commercial information and trade secret is information that derives value from being kept a secret.
- The law of confidence and contract protects the confidential information and trade secret from unlawful disclosure so long as the confidential information or trade secret is actively protected by the organization.
- Confidential Information is information that relates or pertains to matters of finance, commerce, science or technical matters as those terms are commonly understood.
- Confidential Information need not have an inherent value, such as a client list might have, however, the value of information is *dependent upon the use that may be made of it*, and its market value will depend upon the market place, who may want it, and for what purposes, a value that may fluctuate widely over time
    - *Merck Frosst v. Canada, (2012, SCC)*

Miller Thomson
lawyers | avocats

Customer Lists

- A business has proprietary interest in its customer lists as long as they are kept confidential
- What happens if a customer list is the same as the subscribers to a social media account?
- *Eagle Professional Resources Inc v MacMullin* (2013, ONSC)
  - The company sued former employees for allegedly breaching restrictive covenants in their employment agreements and soliciting the company's clients
  - The Court dismissed the case, finding that the company had no proprietary information at stake because the customer information was available through social media websites

Claims involving Consultants and Contractors

- The same issues that apply between employers and employees apply to businesses and their consultants and contractors
- The business may be vicariously liable for the actions of its contractors depending on whether they are employees or independent contractors
  - *67112 Ontario Ltd v Sagaz Industries Canada Inc* (2001, SCC)

Privacy Issues

Privacy Issues

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."

Privacy Issues

- Employers have the right to monitor and control business operations
  - But, this right has to be balanced with employees' right to privacy
- Monitoring may be done through video surveillance, drones, GPS or other tracking systems
- Technology can be misused if it is collecting personal information

Personal Information Protection Act

- Employee personal information is information that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate employment relationships
- Employee personal information may be collected without the employee's consent where the collection is reasonable and for the purposes of establishing, managing or terminating the employment relationships
- An organization must notify an individual that it will be collecting the employee's personal information

GPS and Monitoring Cases

- *KONE Inc* (2013, PIPA)
  - KONE collected data from GPS in cell phones issued to service mechanics after notifying them
    - Purpose: ensure accurate client invoicing, client invoice disputes, act as a time clock for employees, optimize response times and locate employees in event of emergency
  - Activity permitted under PIPA and employer had notified employees of the policy
- *Thyssenkrupp Elevator* (2013, PIPA)
  - GPS and engine monitoring in elevator repair vehicles
  - Activity permitted under PIPA but employer failed to notify employees

GPS and Monitoring Cases

- *Schindler Elevator Corporation* (2012, PIPA)
  - GPS monitoring in motor vehicles operated by mechanics
  - Collection of information was permitted because used to manage employees and employees were notified of the collection
- *University of British Columbia* (2013, FIPPA)
  - UBC installed GPS and engine monitoring in campus security vehicles
  - Activity permitted under FIPPA but UBC failed to notify employees as required by the Act

Privacy Torts

- Some provinces have enacted legislation which create a civil action for violation of privacy
- British Columbia *Privacy Act*
  - Violation of privacy is a tort actionable without proof of damage
  - Damage awards under the BC *Privacy Act* range from $100 to $60,000

Privacy Torts

- Ontario Court of Appeal recognized a new common law tort of intrusion upon seclusion
- *Jones v Tsige* (2012, ONCA)
  - An employee of the Bank of Montreal snooped on the personal financial records of another employee 174 times over 4 years
  - Reasons for the new tort included that the pace of technological change has accelerated exponentially and there is a pressing need to preserve privacy
  - The Court noted that there was no economic loss, damages would ordinarily be measured by a modest conventional sum (i.e. up to $20,000)

Recent Developments

- *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401* (2013, SCC)
  - Alberta PIPA which tracks BC PIPA
  - Union was video-tapping and photographing individuals crossing a picket line
  - General rule: organizations cannot collect, use or disclose personal information without consent
  - Purpose: enhance individual's control over personal information
    - Related to individual's autonomy, dignity and privacy
  - Entire statue declared invalid because did not balance union's right to freedom of expression with interests protected by PIPA

Reasonable Expectation of Privacy

- PIPA protects personal information that is publicly disseminated. Personal information does not lose its character if it is publicly known.
- PIPA has not been reconciled with an individual's "reasonable expectation of privacy" protected by s. 8 of the *Charter*
- An individual's reasonable expectation of privacy may be diminished where personal information was stored on a work computer and the employer had a policy that data on the computer belonged to the school

R v Cole (2012, SCC)

Data Protection

- If an employer's security is breached, the employer may be liable for disclosing personal information of employees and clients
- January 7, 2012 – University of Victoria
  - a USB flash drive containing personal information and bank numbers relating to over 11,000 current and former employees was stolen
  - The privacy commissioner found that the University failed to prevent an unauthorized disclosure of personal information

(2012, FIPPA)

- A business can be liable for breach of information under the BC PIPA or the Federal FIPPA or PIPEDA
  - European Comm. recognizes Federal PIPEDA as providing adequate protection for personal data transferred between EU and Canada
- A business may also be contractually liable to clients or third parties for the breach in data protection

Claims involving Third Parties

Miller Thomson
lawyers | avocats

Claims involving Third Parties

**"A customer on the internet criticized our technology!
Twitter his blog and Flickr his Google until he Netscapes an apology!"**

Claims involving Third Parties

- Third parties may post harmful comments about a business on social media websites
- These comments can have significant reputational risks as comments on the internet are always speaking
- Remedies available include defamation and trademark and copyright infringement actions
- Before starting a lawsuit, the business should give notice to the third party and ask them to remove the comments

Copyright

- Copyright protects expression of ideas for literary, artistic, dramatic or musical works (including computer programs), performance, sound recording and communication signals
- To be considered “original”, a work must be the result of “an exercise of skill and judgment”
- Copyright is automatic on creation and fixation of the work
- A copyright means the sole right to produce, reproduce perform or publish the work or any substantial part thereof in any material form for a period of the author’s life plus fifty years

Trade-marks

- Protect and distinguish the sources of products and services
- It can be a word, symbol or design, including colours, smells, sounds and package designs, look and fell of product or service
- A trade-mark allows its owner exclusive use of that mark to be identified with certain goods or services
- Common law affords some trade-mark rights protection for trade-marks which are not registered with the Trade-mark Office provided they have acquired reputation
- Initial registration period is 15 years which can be renewed for consecutive 15 year periods indefinitely

Defamation

- The elements of defamation are:
  - That the words were defamatory, in the sense that they would tend to lower the plaintiff's reputation in the eyes of a reasonable person;
  - That the words in fact referred to the plaintiff; and
  - That the words were published, meaning that they were communicated to at least one person other than the plaintiff

Grant v Torstar Corp (2009, SCC)

- What constitutes publication on the internet is a live issue
- Hyperlinking to a website with defamatory content, without adopting the content is not publication
  - *Crookes v Newton* (2011, SCC)

Damage to Reputation

- Social media sites are public and have high traffic
- Harmful posts may damage a business's reputation
- Newspaper articles may be written about the incident
- Businesses and employers need to implement safeguards to protect themselves

Miller Thomson
lawyers | avocats

Claims involving Third Parties and Employees

- If employees make harmful posts about another business on social media websites, the employer may be liable for damages
- The employer may face defamation or trade-mark or copyright infringement actions
- Employers are vicariously liable for the actions of their employees
  - Normally restricted to actions done in the course of employment

    Bazley v Curry (1999, SCC)
  - But, employers have been found to be vicariously liable for actions of employees off-duty

    Jacobi v Griffiths (1999, SCC)

Miller Thomson
lawyers | avocats

Development in other Jurisdictions

Development in other Jurisdictions

- Nova Scotia has amended its Labour Standards Code
  - prohibits employers from demanding passwords, account information or access to employee and applicant social media accounts
- United States does not have umbrella privacy legislation
  - State legislatures are enacting industry specific legislation
  - In 2013, over 24 privacy laws have been passed in more than 10 states
  - Vary from limiting how schools can collect student data to deciding whether police need a warrant to track cell phone locations

Development in other Jurisdictions

- "Right to be Forgotten"
  - The European Union is proposing to enact regulation on data protection that would create a right to be forgotten
  - The regulation would grant individuals greater control over personal information held by any company or agency
  - Any person would have the right to have their personal data erased and no longer processed where:
    - the data is no longer necessary for the purposes for which it was collected or used,
    - The person has withdrawn his or her consent for having the data used, and
    - The person objects to the use of his or her personal data.

Conclusions

Social Media Policies

- Establish a policy for social media use
  - Define social media
- State what constitutes appropriate and inappropriate use of social media
  - Is the employee prohibited from mentioning information about the business's employees or customers without prior approval?
  - Is the employee permitted to use social media during work hours?
- If employee uses social media for the employer, state the procedures for the use and who owns the account
- State that the employer monitors use of social media
- State the consequences for not following the policy

Anti-Bullying and Harassment Policies

- Assess whether business is in compliance with WorkSafeBC policies on bullying and harassment in the workplace
- Establish a policy to prevent and address inappropriate behaviour in the workplace
- State what constitutes appropriate and inappropriate behaviour
- Outline how use of social media relates to bullying and harassment
- Develop and implement reporting procedures
- Develop and implement procedures for dealing with incidents and complaints

Confidential Information

- Establish a confidentiality policy
- Define confidential information:
  - The information must have a quality of confidence about it; and
  - The information must have been imparted in circumstances giving rise to an obligation of confidence
- Information must be treated as being confidential
  - Create a process for disclosure
  - Authorize a group of permitted persons to control information
- State the consequences of breaching the policy

Managing Privacy Rights

- What personal information about customers, employees and third parties does the business collect?
- Has the impact of *Personal Information and Protection Act* on the business been assessed?
- Is there a policy with respect to the collection, use and disclosure of personal information?

Reflections

1. Social media websites are increasingly affecting businesses
2. Social media websites pose new challenges and stretch existing issues into new areas
3. Without proper contracts and policies, employers are exposing themselves to liability and reputational harm
4. Employment contracts and policies must be developed to ensure proper use
5. Interaction between personal information, reasonable expectation of privacy, employer's duties and obligations to take care (monitor and supervised) is not settled

Thank You

Aiyaz A. Alibhai

aalibhai@millerthomson.com

604.643.1233

Miller Thomson
lawyers | avocats

www.millerthomson.com

Added experience. Added clarity. Added value.

Follow us...

Miller Thomson
lawyers | avocats