Social Media and Privacy at Work: Five Things You Need to Know

IAPP Canadian Privacy Symposium 2012
May 10, 2012

Andrea York
Partner
Blake, Cassels & Graydon LLP
What issues can employers face with social media?
Social Media & Privacy @ Work
Five Things You Need to Know

1. What is the scope of an employee’s right to privacy (the legal framework)?
2. Do you know what your employees are doing online? Employee use of social media may increase risks for employers.
3. Social media provides insight into off-duty conduct, and may have on-duty consequences.
4. The data mining of social media and employee monitoring – is it permissible?
5. Background checks can be minefields.
1. Legal Framework

- Legislation
  - Federal – PIPEDA
    - provides privacy protections for federally regulated employees
    - commercial activities
  - Provincial privacy legislation
    - limited application to employees outside of AB, BC and QC

- Common law

- Arbitral jurisprudence
1(b) Legal Framework: What is the scope of employee right to privacy?

- **Jones v. Tsige** (Ontario Court of Appeal, 2012)
  - New tort of “intrusion upon seclusion”
  - “Employment” identified as a sensitive matter
  - Potentially wide implications

- **R. v. Cole** (Ontario Court of Appeal, 2011)
  - Employees may have a limited right to privacy in personal use of workplace resources (e.g., laptop)

- Arbitrators in the unionized context have recognized privacy rights on different bases:
  - Legislation (e.g., *Doman Forest Products Ltd. v. International Woodworkers, Local 1-357; B.C., 1990*)
  - Collective agreements (e.g., *Canadian Timken Ltd. v United Steelworkers of America, Local 4906; Ont., 2001*)
  - Independent right stemming from arbitral case law (e.g., *Teamsters Local Union 647 v. William Neilson Dairy; Ont., 2009*)
2. Do you know what your employees are doing online?
2(b) Employee use of social media may increase risks

• Vicarious liability
  – *Bazley v. Curry* (S.C.C.)
    • Liable for employee actions during the course of employment
      – Authorized acts
      – Unauthorized but sufficiently connected to duties
  – Intrusion upon seclusion - *Jones v. Tsige*
    • Can actions of a “rogue employee” lead to vicarious liability?
2(c) Vicarious Liability: Risks on the increase?

- e.g.: *Chatham-Kent (Municipality) v. CAW*
  - Caregiver posted pictures online of residents and information and insensitive comments about medical conditions
  - Could give rise to claims
- Defamation?
- Possible human rights concerns?
- Negligence?
3. Social Media insight into off-duty conduct

“Vancouver rioters got rowdy, then got fired”
– The Toronto Star, January 23, 2011
3(b) Social Media: Off-duty Conduct with On-duty Consequences
3(c) Social Media: Off-duty Conduct with On-duty Consequences

• “atta boy vancity!!! show em how we do it!!!”
3(d) On-duty consequences have limits

- Employers have the onus to prove just cause whether for on or off-duty conduct – high burden

- Consider:
  - Is the conduct wholly incompatible with employment duties such that the employment relationship breaks down?
  - Does the conduct result in real or likely prejudice to the employer?
  - Have other employees been treated consistently?
  - Is a warning a more proportionate response?
3(e) On-duty consequences – Cause for termination

- **Chatham-Kent (Municipality) v. CAW Canada, Local 127**
  - Cause termination justified because:
    - blogger/grievor breached her confidentiality agreement
    - she made public insubordinate remarks about management, workplace procedures, managerial decisions, and the general running of the home
    - the comments demonstrated a disregard for the residents’ need for care and conduct inappropriate and unbefitting of an employee in her position
    - posted the comments on a public website that was accessible to anyone with Internet access
3(f) On-duty consequences – Cause for termination

- *Re Lougheed Imports Ltd. (c.o.b. West Coast Mazda)*
  - Cause termination justified
    - Employees posted derogatory remarks about management and workplace on Facebook, promoted a competitor, posted threatening statements
    - Vice Chair found the posts to be “offensive and egregious”, “expressed contempt for and ridiculed the manager and supervisors in such a manner that there was proper cause”.
    - Compounding the misconduct was the fact that the employees had been untruthful during the employer’s investigation of the issue
3(g) On-duty consequences – Cause for termination

- *West Coast Mazda*
  - Posts visible to many Facebook friends
    - Employees could “not have a serious expectation of privacy”
  - Friends included co-workers and managers
    - Comments were “akin to comments made on the shop floor”
3(h) On-duty consequences – No cause for termination

- **Wasaya Airways L.P. v. Air Line Pilots Assn., International**
  - Pilot posted derogatory remarks about First Nations people
  - Did not identify employer by name
  - “where the internet is used to display commentary or opinion, the individual doing so must be assumed to have known there is potential for virtually world-wide access to those statements”
  - Termination not justified, but employment relationship damaged beyond repair
3(i) On-duty consequences – No cause for termination

- **Groves v. Cargojet Holdings Ltd.**
  - “Joked” about kicking superior in the genitals with steel-toed boots and spitting in his face
  - Called the workplace a “high school” where everyone gossiped
  - Did not identify her workplace or denigrate its business
  - Termination not justified
Off-Duty Conduct and Privacy

• **Cargojet Holdings**
  – Employee expectations of privacy?
  • “Many subscribers, in particular young persons, regard Facebook as conduct engaged in on personal time, unconnected to the workplace, analogous to sharing a beer with colleagues and friends, or getting together with friends to confide details about their jobs.”
4. Social Media and Data Mining

Forbes
Kashmir Hill, Forbes Staff
Welcome to The Not-So Private Parts where technology & privacy collide TECH 1/24/2012 @ 2:07PM | 14,171 views

#McDStories: When A Hashtag Becomes A Bashtag

A crowd-sourced campaign turns on McDonald's

Here’s a cautionary tale for the corporate social media consultants of the world. Last week, McDonald’s launched a Twitter campaign using the hashtag #McDStories; it was hoping that the hashtag would inspire heart-warming stories about Happy Meals. Instead, it attracted snarky tweeps and McDonald’s detractors who turned it into a #bashtag to share their #McDHorrorStories.

Sample tweets:
- Dude, I used to work at McDonald’s. The #McDStories I could tell would raise your hair. (via Twitter)
- One time I walked into McDonalds and I could smell Type 2 diabetes floating in the air and I threw up. #McDStories (via Twitter)

communities, comments, tweets, reviews, likes…
4(b) Social Media and Data Mining

- Social Media as a Marketing Tool
  - Twitter recently sold rights to 2 years’ worth of tweets
4(c) Data Mining – A cautionary tale

Profiles created by data mining may include the following about an individual:

- Name
- Location
- Email address
- Blogs on which individual participated
- Average circulation
- Link counts
- # of posts per month
- Followers
- Updates
- Age
- Sex
- Religion
- Number of children

Your social media footprint…
4(d) Data Mining – Is it legal?

• Risks
  – Infringement of privacy law and rights?
    • Consent for collection, use, and disclosure?
    • What are the purposes for collecting the information?
    • Are social media postings public information? Does compiling postings and other information available online into a profile change that?
    • Sensitive personal information (*Jones v. Tsige*)
    • Extraterritorial reach of the Internet
4(e) What about monitoring employee use?

• Legitimate business purposes
  – Workplace relationships
  – Relationships with suppliers and customers
  – “Time theft”
  – Breaches of workplace rules
  – Employer reputation
  – Breaches of the law
  – Loss of confidential information
4(f) Monitoring Employee Use

- Is it permissible at the workplace
  - Are there any privacy statutes that apply?
  - *Jones v. Tsige* — “personal correspondence”
  - *R. v. Cole* — limited right to privacy in workplace computer

- Is it permissible for “off-duty” activities
  - Consent?
  - Questionable if employees can be disciplined for off-duty conduct
4(g) Monitoring Employee Use: Reducing the risks

1. Limit monitoring and collection of personal information
2. Aggregate data if this is consistent with the purposes
3. Notify employees of the monitoring and advise them of purposes
4. Obtain consent for sensitive collections
5. Implement a good social media policy to supplement:
   - confidentiality agreement
   - information technology use policy
   - privacy policy
6. Train employees so they understand the policy
7. Enforce the policy consistently and update it regularly
Social Media Policy – Checklist

- What to include in your social media policy?
  - ✓ Explain social media and its nature
  - ✓ Explain the employer’s approach to social media
  - ✓ Include non-work use that affects the employer
  - ✓ Remind employees that their use may affect the employer
  - ✓ Prohibit the violation of laws
  - ✓ Prohibit the violation of company policies
  - ✓ Prohibit speaking on behalf of the company without authorization
  - ✓ Require that work time be respected
  - ✓ Advise of monitoring (e.g., collection, use, and disclosure)
  - ✓ Warn of consequences (i.e., disciplinary action)
  - ✓ Tell employees where to go for answers
5. Background Checks are Minefields

- Privacy & Human Rights Concerns
  - Alberta – *Mark’s Work Wearhouse*
  - Is there a privacy gap in Ontario?
  - Can employers request access to social employee media sites?
  - Social media use as “public”?
  - Does common law now provide employees with enhanced protections
  - BC Guidelines (to be discussed next)
Case Law References

- *Jones v. Tsige*, 2012 ONCA 32
- *R. v. Cole*, 2011 ONCA 218
- *Lougheed Imports Ltd. (c.o.b. West Coast Mazda) v. United Food and Commercial Workers Int’l Union, Local 1518*, 2010 CanLII 62482 (BC LRB)
Guidelines for social media background checks

May 10, 2012
Caitlin Lemiski, Policy Analyst
If it’s publicly available online, what’s the problem?
“public” has a *limited meaning*
- PIPEDA and Alberta’s PIPA have similar limits
- Employers must have the authority to collect
- Examples include: phone book, newspaper
What about other employment laws?
PERSONAL INFORMATION PROTECTION ACT
[SBC 2003] CHAPTER 63

Application

3 (1) Subject to this section, this Act applies to every organization.

(2) This Act does not apply to the following:

(5) If a provision of this Act is inconsistent or in conflict with a provision of another enactment, the provision of this Act prevails unless another Act expressly provides that the other enactment, or a provision of it, applies despite this Act.

- You must always consider PIPA
- Alberta and PIPEDA have the same rule
- The authority to collect is often overlooked
REJECTED!
Social Media Consumer Report

Client: Gizmodo

Subject Name: Mathew (Mat) Honan

Information Provided

Address Information
AddressLine1: Not Provided
City: San Francisco
State: CA
PostalCode: Not Provided

Contact Information
HomePhone: Not provided
CellPhone: Not provided
OtherPhone: Not provided
EmailAddress: honan@gizmodo.com

Social Intelligence runs a search based on resume data like your name, address, phone number and email. Setting up a new email address just for your job search will help “clean” your results.

Summary

An extensive review of Mat Honan’s online presence and activity was conducted by Social Intelligence Corp. A number of items found were identified as negative based on the client’s pre-defined criteria.

My report returned several negative hits.
I'll tell you one thing about Wired that I really appreciate: we don't assume our readers are idiots. I've written for a lot of publications, and you'd be amazed at how many think you're fucking stupid. Apparently, the New York Times shares that sentiment.

Look, here's the thing: meth can help you focus and accomplish menial and creative tasks—just as is true of other amphetamines. It boosts dopamine output. Plain and simple. Does that mean it's worth doing? No.

Amphetamine has a long and storied history as a tool that has helped people, well, amp up their brainpower. Jack Kerouac is one famous case. His drug of choice for cranking out page after masterful page was Benzedrine. Benzedrine's active ingredient is dl-amphetamine, which is, of course, a close cousin to meth.

Now, that doesn't mean you should use it. Certainly long term use makes you dumb and crazy. I've watched friends ruin their lives on meth. It's a horrible drug that's less likely to turn you into the next Kerouac than it is this guy.

Why, this may shock you, but here's the thing: Cocaine is exceptionally fun. LSD? It genuinely alters your perception. I'm not suggesting that you do either of these. Both conspired, unsuccessfully, to kill me and I would no more try either today than I would attempt to put a rattlesnake in my anus. I am older and wiser and recognize that the benefits are not worth the risks. Despite my swinging-dick persona on Twitter, I'm more this guy than that guy. Drugs, especially highly addictive ones like speed or cocaine or heroin or ones with powerful psychological components like LSD, tend to not be worth the price you pay for their use.

But the viewpoint that illegal drugs are purely bad and have no positive contributions whatsoever to offer is simply nonsense, and we should put it to rest. We'll never solve society's problems if we can't at least speak honestly about them.

The bottom line is if you use meth, you're very likely to ruin your life. Which I noted. In fact, one reason I wanted to include meth was to help make the point that every drug has its cons.

But that does not mean the cons are the entire story. And as long as we're shaming, maybe the New York Times should be ashamed of itself for assuming we are a nation of six year olds who can't be spoken to honestly or trusted to make rational decisions.
Blumenthal, Franken Call on Social Intelligence Corp to Clarify Privacy Practices

Monday, September 19, 2011
(Washington, DC) – Senator Richard Blumenthal (D-CT) and Senator Al Franken (D-MN) recently wrote to the CEO and President of Social Intelligence Corporation, Max Drucker, pressing the firm on concerns that their business practices relating to personal privacy were unfairly detrimental to prospective employees. Social Intelligence Corporation is an online provider of employment screening and monitoring services that pulls information about job-seekers from various social media sites such as Facebook and Flickr.

In the letter, Blumenthal and Franken write, “According to sample background reports published in the media, information is collected from applicants’ profiles on social networking sites like Facebook and LinkedIn, among others. It is then sold for prospective employers to use in hiring decisions. This type of surveillance can potentially harm a job-seeker’s ability to gain employment. It could also deter people from seeking employment opportunities if they believe their privacy will be invaded.”
Do treat viewing as collection

- At home, at work, on a smartphone
- Even if you don’t save it
- Even if you don’t print it
- Order P10–01(2010 BCIPC No. 7)
- Jones v. Tsige, 2012 ONCA 32
Do not assume they can’t find out

- **IP addresses** are unique numbers assigned to each device connected to the internet.
- **Web analytics** measure internet traffic using IP addresses and cookies.
- Bloggers could run web analytics to ID visitors.
- Individuals **have a right to find out** how an organization has used their information (if it is under their control) – see s. 23 of PIPA.
Do a privacy impact assessment
Do not assume you are meeting your legal obligations

- **Accuracy**: Consider imposter and hacked accounts
- **Reasonableness**: Plenty of fish versus LinkedIn
- **3rd party information**: Like a dragnet, social media checks can catch much more than intended.
Final thoughts

- Determine if what you are doing is legal
- Be prepared for an information access request
- If in doubt, find a less privacy-intrusive alternative
- Train your staff, and have penalties for not complying
- Treat social media checks like any other kind of check
- Ask yourself if what you are doing is reasonable
- Be transparent with your hiring process
Thank you.

May 10, 2012
Caitlin Lemiski, Policy Analyst