Social Media Privacy Risks

Aiyaz A. Alibhai & Alizée Bilbey

Miller Thomson
lawyers | avocats

Social Media Privacy Risks

1. Social Media Platforms
2. Risks and Responsibility under Public Law
3. Risks and Responsibility under Private Law
4. Social Media Background Checks

Social Media Privacy Risks

5. Web 3.0 and the Internet Of Things
6. Illustrative Cases
7. Behavioural Advertising and Privacy
8. Conclusions and Reflections

Miller Thomson
lawyers | avocats

12th Managing Privacy Compliance Course

November 6, 2015

Miller Thomson
lawyers | avocats

Social Media Platforms

Social Media Platforms

Social Media = a form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content

Social Media and Web 2.0

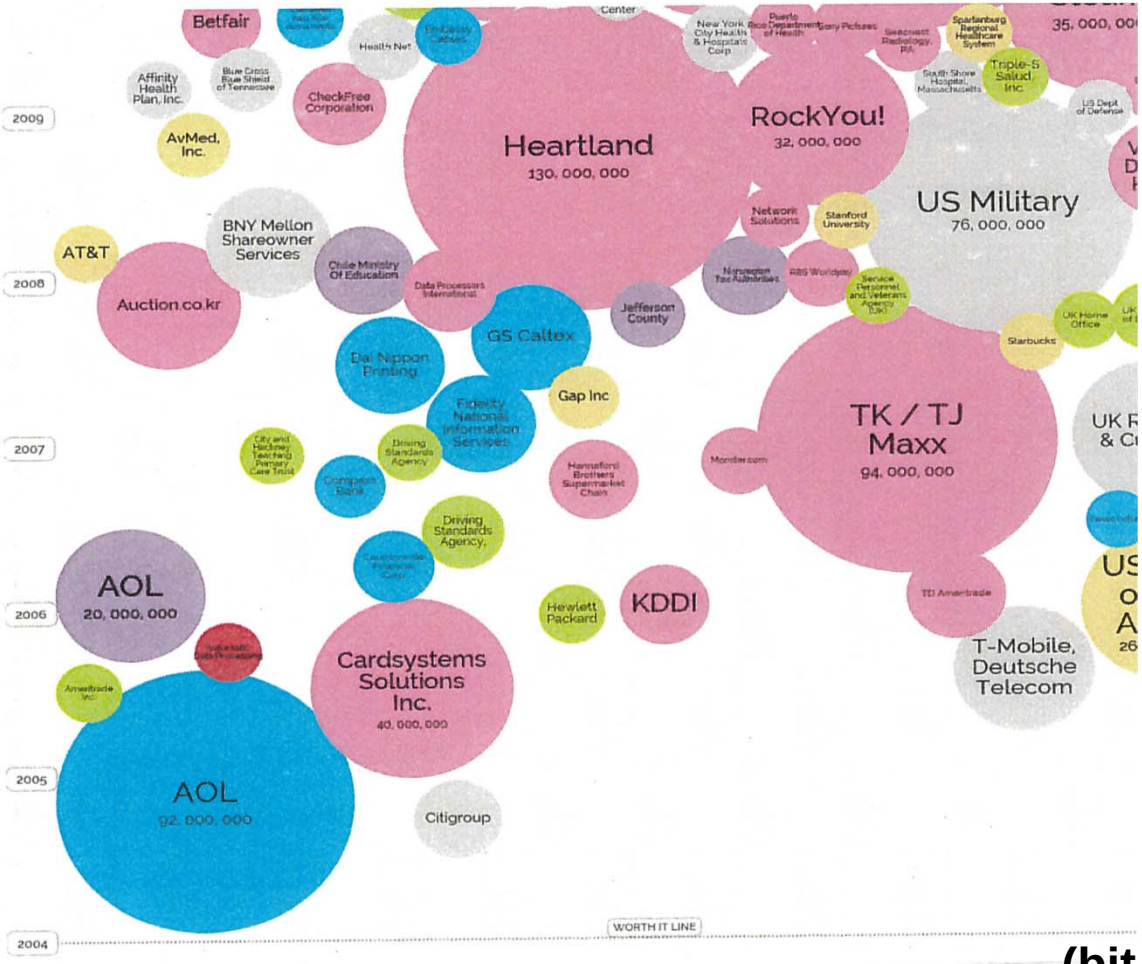
- Traditional World Wide Web (1.0) was static.
  - Data was posted on Web sites, and users simply viewed or downloaded the content.
- Web 2.0 is the current state of online technology.
  - Characterized by greater user interactivity and collaboration, more pervasive network connectivity and enhanced communication channels.
  - Users have more input into the nature and scope of Web content and exert real-time control over it.

Social Media Platforms

- Includes:
  - Social networking sites
  - Blogs and micro-blogs
  - File sharing sites

- Web 2.0 – dynamic, interactive

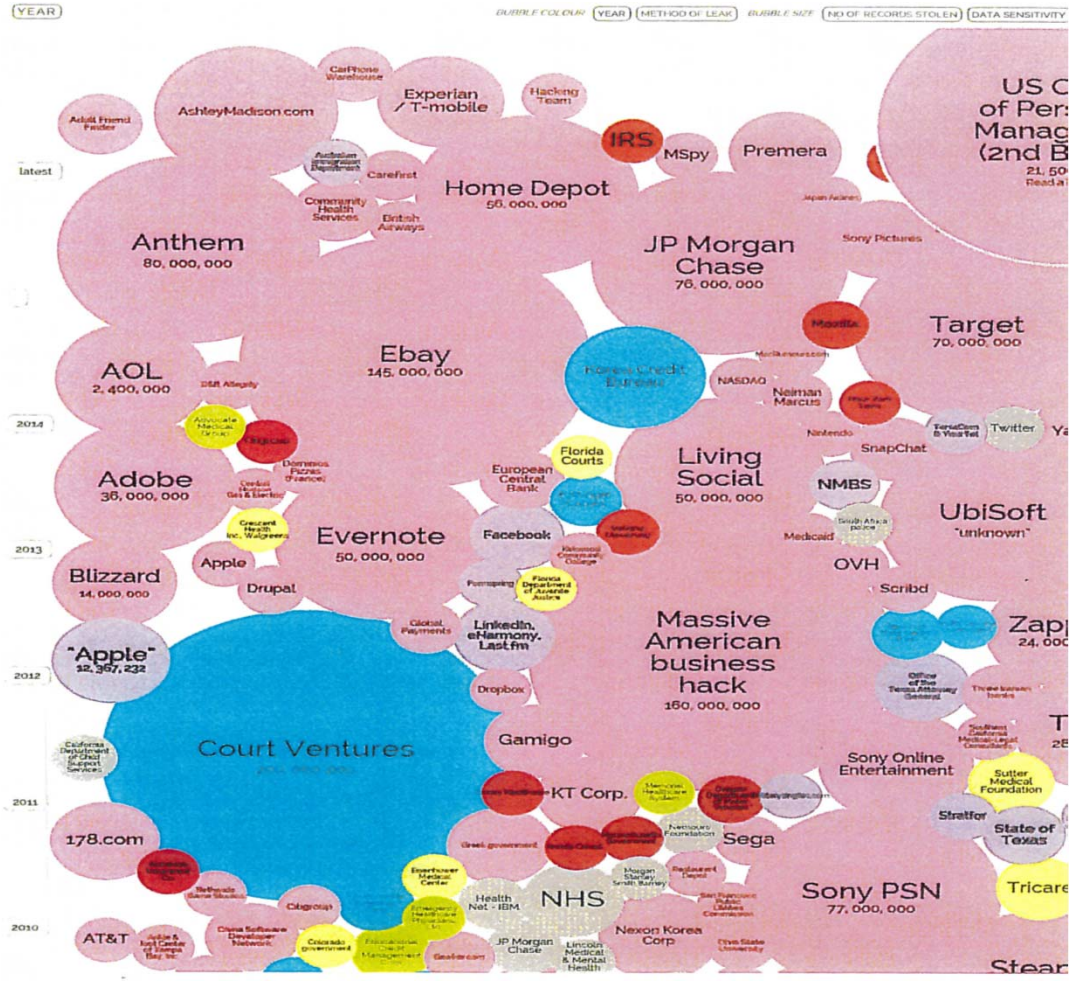
Data Breaches Worldwide, 2004-2009



(bit.ly/bigdatabreaches)

Miller Thomson
lawyers | avocats

Data Breaches Worldwide, 2010-2015



Miller Thomson
lawyers | avocats

Statutory Framework

Statutory

- British Columbia
  - *Privacy Act*
  - *Personal Information Protection Act*
  - *Freedom of Information and Protection of Privacy Act*
- Federal
  - *Privacy Act*
  - *Personal Information Protection and Electronic Documents Act*

British Columbia: *Privacy Act*

- It is a tort, actionable *without proof of damage*, for a person, wilfully and without a claim of right, to violate the privacy of another
- It is a tort, actionable without proof of damage, for a person to use the name or portrait of another for the purpose of advertising or promoting the sale of property or services, unless consent is provided

British Columbia: *PIPA* vs *FIPPA*

Personal Information Protection Act

- Private sector
- "Personal information" means information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information

Freedom of Information and Protection of Privacy Act

- Public sector
- "Personal information" means recorded information about an identifiable individual other than contact information (includes name, position/title, business address/email/fax number)

Miller Thomson
lawyers | avocats

British Columbia: *PIPA* vs *FIPPA* (cont'd)

Personal Information Protection Act

- Organization must:
  - obtain consent or authorization by the Act to collect, use or disclose personal information
  - disclose the purpose for collection
  - consider what a reasonable person would consider appropriate in the circumstances

Freedom of Information and Protection of Privacy Act

- A public body may collect personal information in certain circumstances, including:
  - expressly authorized by FIPPA
  - relates directly to and is necessary for a program or activity of the body
  - individual has consented and a reasonable person would consider collection appropriate

Canada: *Privacy Act* vs *PIPEDA*

Privacy Act

- Public sector
- "Personal information" means information about an identifiable individual that is recorded in any form
- Includes:
  - Race, ethnic origin, religion, age, etc;
  - Educational or medical history
  - Any identifying number, symbol
  - Address, fingerprints, blood type
  - Personal opinions or views

Personal Information Protection and Electronic Documents Act

- Private sector
- "Personal information" means information about an identifiable individual

Miller Thomson
lawyers | avocats

Canada: Privacy Act vs PIPEDA (cont'd)

Privacy Act

- No personal information shall be collected by any government institution unless it relates directly to an operating program or activity of the institution
- Shall inform the individual of the purpose for which the information is being collected (exceptions apply)
- May be disclosed in limited circumstances

Personal Information Protection and Electronic Documents Act

- An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances
- Knowledge and consent of the individual required for collection, use or disclosure, except where inappropriate
- May collect information without knowledge and consent in certain circumstances

Miller Thomson
lawyers | avocats

Risks under Private Law Actions

Risks under Private Law Actions

- Defamatory Statements
  - disparaging comments by employees and others on social media platform about third parties
- Slander of Title
  - untrue statements about a person, property or their business made with malice that causes damage
- Tort of intrusion upon seclusion (Ontario)
  - up to $20,000 for deliberate and significant invasions of personal privacy (financial or health records, sexual practices and orientation, employment, private correspondence)

Miller Thomson
lawyers | avocats

Risks under Private Law Actions

- Infringement of Intellectual Property Rights
  - unlawful linking or use of third party trademark
  - unauthorized reproduction or transmission of material covered by copyright
- Unauthorized disclosure of confidential information and trade secrets
  - secrecy of confidential information lost
  - loss of patent rights by disclosure prior to filing

Risks under Private Law Actions

- Disclosure of Corporate Information contrary to securities laws
  - under Canadian securities laws, material information must be publicly disclosed immediately through a broadly disseminated news release
  - obligation to protect clients from the use of misleading and false statements
    - Canadian Securities Administrators (CSA) Staff Notice 31-325 – Marketing Practices of Portfolio Managers
    - S. 11.5(1) of National Instrument 31-103 – *Registration Requirements and Exemptions* (NI 31-103)

Risks under Private Law Actions

- Employment and Workplace Management
  - restriction of personal freedom vs employers' right to manage workplace and corporate resources
- Disclosure of Personal Information
  - breach of personal information of third parties held by organization
- Breach of Privacy of Users
  - unauthorized collection and use of personal information of users

Social Media Background Checks

Miller Thomson
lawyers | avocats

Social Media Background Checks

- In March 2015, Workopolis (online job site) surveyed 355 Canadian employers:
  - 63% look up potential candidates online and check out their social media profiles before making a hiring decision
  - 48% have seen something on a social media profile that moved them to not hire a candidate

Social Media Background Checks (cont'd)

- Statutory limitations:
  - PIPEDA: organization is required to consider what a reasonable person would consider appropriate in the circumstances
  - Privacy Act:
    - PI collected by government institution must relate directly to an operating program or activity of the institution
    - Institution inform the individual about whom the PI is collected (with exceptions)
    - Institution must not disclose the PI without the consent of the individual, except in accordance with the Act

Social Media Background Checks (cont'd)

- Human Rights Legislation
  - Canada Human Rights Act (RSC, 1985, C H-6)
  - Human Rights Code (RSBC, 1996, Ch 210)
- Employer may face human rights complaint if the employer obtains information about personal characteristics such as race, religion, or sexual orientation if perceived to be a factor in the decision-making process

Social Media Background Checks (cont'd)

"It is a discriminatory practice, directly or indirectly,

(*a*) to refuse to employ or continue to employ any individual, or

(*b*) in the course of employment, to differentiate adversely in relation to an employee,

on a prohibited ground of discrimination."

(Canada Human Rights Act, s. 7)

Miller Thomson
lawyers | avocats

Web 3.0 and the Internet of Things

Internet of Things

- A term used to describe how everyday objects can send and receive information to and from the internet (*David Sweet, M.P., Submission to the House of Commons Standing Committee on Industry, Science and Tech, June 18, 2015*)
- Includes: home automation systems, health devices connected to a mobile application, wearable technology (i.e. Fitbit, Google Glass)

Internet of Things (cont'd)

- Evolution to Web 3.0
- Machine-classified, data sharing world creates a basis for ubiquitous computing.
- Pervasive computing, is a scenario in which embedded processing in everyday objects enables intercommunication and unobtrusive data sharing throughout the user's environment.

Internet of Things (cont'd)

- In 2008, the number of things connected to the internet was greater than the number of people on the planet
- By 2020, anticipating 50 billion objects connected to the internet (Cisco)
- "Internet of Everything" (Cisco)

(Daniel Caron, speaking at the Information Security Rendez-Vous in 2014)

Miller Thomson
lawyers | avocats

Internet of Things (cont'd)

- Wearable computing
  - The use of miniature, body-borne computer or sensory device worn on, over, under or integrated within, clothing
  - Includes: body-worn cameras and technologies
  - "The wearable era compounds and amplifies privacy risks in the mobile environment by gathering additional, and intimate, personal information"

(Canada Privacy Commissioner)

Internet of Things (cont'd)

- Vast collection of personal information at low costs:
  - Intruder compromising mobile devices, televisions
  - tracking locations
  - constant surveillance at vey low costs
- Physical safety:
  - intruder hacking medical devices (pacemaker),
  - vehicle braking systems

("Internet of Things: Privacy & Security in a Connected World", US Federal Trade Commission, January 2015)

Miller Thomson
lawyers | avocats

Risks with Automatic Collection of Data

- What data is collected?
- Is it personal information? (likely)
- Where is it stored?
- What uses are intended for data?
- Who has access to data?

Illustrative Cases

Privacy Risks

- Breach can be small- or large-scale
- Consequences of a large-scale breach can be devastating
- Consider Facebook:
  - 1.49 billion monthly active users as of June 30, 2015
  - 1.31 billion mobile monthly active users as of June 30, 2015
  - 968 million daily active users on average for June 2015

Miller Thomson
lawyers | avocats

Privacy Risks (cont'd)

- Breach of one platform may result in contamination of another
- Consider the social media platforms that ask you to sign in using your Facebook account
- Risks:
  - To user
  - To third parties
  - To the business/employer

Privacy Risks: "Bring Your Own Device" and Big Data

- Greater move towards cloud-based big data storage solutions
- Risk created by:
  - Employees using personal devices in the workplace, and
  - Employees using personal e-mail addresses to connect to employer-provided devices
- Transmission of information across forums

(Source?)

Miller Thomson
lawyers | avocats

Privacy Risks: *Eagle v Edcomm* (Pa, US)

- Plaintiff Linda Eagle founded Defendant Edcomm Inc
- Eagle's employees managed her LinkedIn account
- Edcomm Inc sold, new owner locked Eagle out of her account

(Source?)

Miller Thomson
lawyers | avocats

Privacy Risks: *Eagle v Edcomm* (cont'd)

- Eight causes of action:
  - Unauthorized use of name (successful)
  - Invasion of privacy by misappropriation of identity (successful)
  - Misappropriation of publicity (successful)
  - *Identity theft (unsuccessful)*
  - *Conversion (unsuccessful)*
  - *Tortious interference with contract (unsuccessful)*
  - *Civil aiding and abetting (unsuccessful)*
- Damages = $0
- Outcome in Canada?

(Source?)

“Once conversations that should be private are undertaken in a public forum, they become theater – meant for the onlookers more than the participants.”

(Rian Van Der Merwe, “Are we surrendering our privacy too easily?”, Memeburn™, 2010)

Miller Thomson
lawyers | avocats

Privacy Risks: Harassment and Bullying

- Bullying by e-mail and social media during work hours or after work hours may be considered harassment in the workplace: *Perez-Moreno v Kulcyzycki*, 2013 HRTO 1074
- Posting offensive messages on social media may result in termination of employment

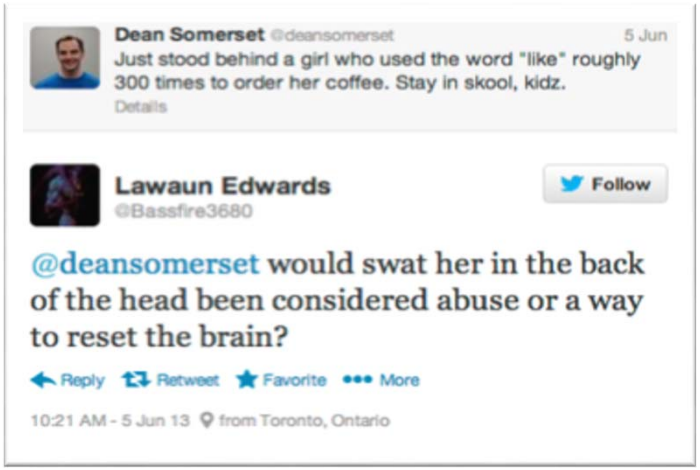
Privacy Risks: Offensive and Threatening Conduct

- In 2012, a California Cold Stone Creamery employee posted racist and threatening Facebook status about President Barack Obama on her private wall
- A contact took a screenshot and shared it on Twitter – post went viral
- Employee was fired

Miller Thomson
lawyers | avocats

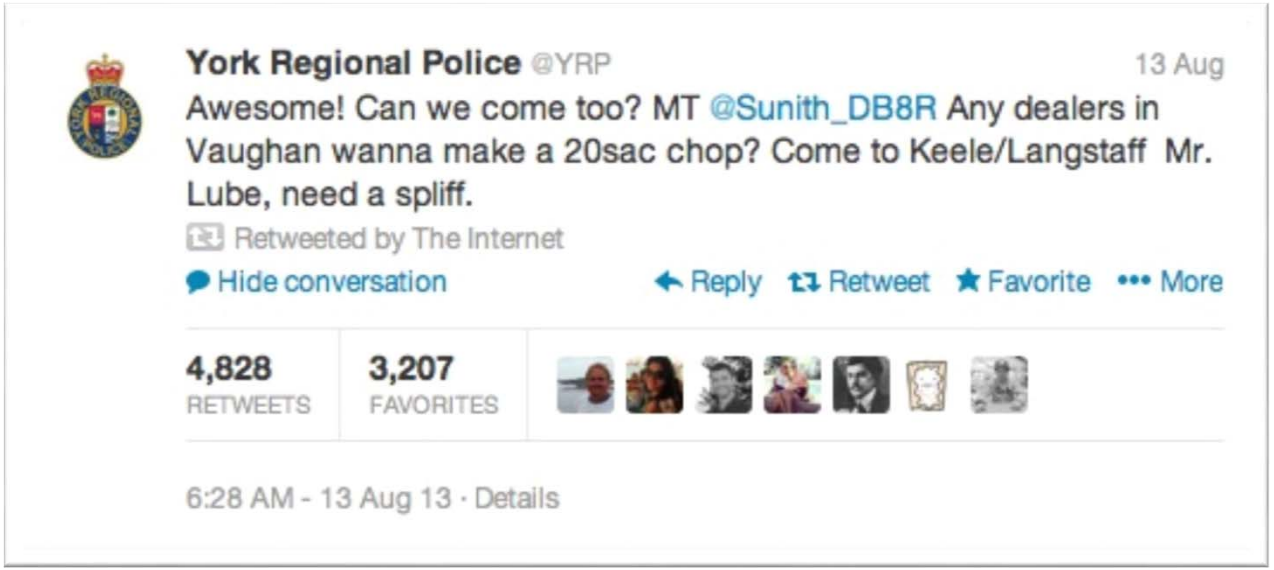
Privacy Risks: Offensive Conduct

- In 2013, two Toronto firefighters were fired after posting misogynistic and offensive tweets
- Both challenged the dismissals – Lawaun Edwards was reinstated



Privacy Risks: Workplace Conduct

- In 2013, a Mr. Lube employee asked a marijuana dealer to come to the shop on Twitter
- York Regional Police tweeted in response and notified his employer



Privacy Risks: Illegal Activity

- In 2015, a woman live-streamed herself driving while intoxicated on app Periscope
- Live stream entitled “Drunk girl driving”
- Multiple viewers contacted Lakeland Police Department
- Police downloaded the app, pinpointed landmarks from the video and located the driver

Miller Thomson
lawyers | avocats

Privacy Risks: Breach of Confidentiality

- Employee has responsibility to respect workplace confidentiality and not to damage the employer's reputation
- An employer may be able to terminate an employee that inadvertently discloses confidential information about the employer and clients

Privacy Risks: Breach of Confidentiality (cont'd)

- *Chatham-Kent v National Automobile, Aerospace, Transportation & General Workers Union of Canada* (2007)
  - Nursing home terminated employee who published information about and pictures of residents
- *EV Logistics v. Retail Wholesale Union, Local 580 (Discharge Grievance)* (2008)
  - Employee posted racist, violent and hateful comments on a public blog

Behavioural Advertising

Behavioural Advertising

- Involves tracking online activities of a consumer, across sites and over time, to deliver advertisements targeted to the inferred interests of the consumer
- The user's actions can be monitored and converted into data
- "Free" services (i.e. Facebook, Google) are based on the currency of trading personal information

Privacy Risks: Behavioural Advertising (cont'd)

- "The information involved in online tracking and targeting for the purpose of serving behaviourally targeted advertising to individuals will generally constitute personal information" (OPCC)
- PIPEDA – the form of consent can vary:
  - Opt-in when dealing with sensitive information (express consent)
  - Opt-out when the information is less sensitive (implied consent)

Bell's Relevant Advertising Program

- August 2013: Bell announces Relevant Advertising Program ("**RAP**"), using opt-out consent model
- OPCC received 170 complaints alleging the RAP contravened the PIPEDA
- April 7, 2015: OPCC released its decision, in which it found that Bell's opt-out model was insufficient to obtain adequate consent for the RAP

AshleyMadison.com Class Action Lawsuit

- July 15, 2015: news begins to circulate that AshleyMadison.com was hacked
- August 18, 2015: media reports that 9.7 Gb of user data was posted online
- August 20, 2015: national class action proceeding filed in Ontario

AshleyMadison.com Class Action Lawsuit

- Notice of action alleges:
  - Breach of contract
  - Breach of the *Consumer Protection Act*
  - Negligence
  - Breach of Privacy and Intrusion upon Seclusion
  - Publicity Given to Private Life

AshleyMadison.com Class Action Lawsuit

- Damages sought:
  - General damages: $750,000,000
  - Special damages: to be determined
  - Punitive damages: $10,000,000

Miller Thomson
lawyers | avocats

Conclusions and Reflections

Conclusions

- Development of Web 2.0 and 3.0 make privacy breaches inevitable from Social Media Platforms
- Consider privacy during the design of Social Media Platforms
- Consider features to minimize damage:
  - Encryption of data
  - Distribution of personal information in separate servers
  - Limiting access to data clusters or servers

Conclusions (cont'd)

- Adoption of best practices for monitoring access to data
- Implement intrusion prevention and detection systems
- Acceptable Use Policy for Social Media Platforms
  - Employees
  - User Terms of Use / Privacy Policy / Community Standards
- Clear Policies for Bringing Your Own Device
  - Complex and variable passwords
  - Ability to wipe missing or stolen devices

Conclusions (cont'd)

- Appropriate Informed Consent
  - Express consent for sensitive information
  - Implied consent for less sensitive information
  - Disclosure of specific use of personal information
  - Disclosure if personal information shared
- Reasonable expectation of user is considered in light of type of services, relationship of parties, etc.
- Generally, retention of personal information after withdrawal of consent and termination not permissible

Conclusions (cont'd)

- Dispute resolution outside the Courts
  - Mandatory Arbitration Provisions
  - Selection of Forum (Substantive Law)
  - Selection of Seat (Place of Arbitration determined procedural laws)
  - Disclaimers and Limitation of Liability provisions
- Terms could prevent class actions in the courts

Thank You

- Aiyaz A. Alibhai, Partner
  604.643.1233
  aalibhai@millerthomson.com
- Alizée Bilbey
  604.643.1220
  abilbey@millerthomson.com

Miller Thomson
lawyers | avocats

www.millerthomson.com

Added experience. Added clarity. Added value.

Follow us...

Miller Thomson
lawyers | avocats