What's New? Key developments in privacy law

Tony Morris, Partner
Kateri-Anne Grenier, Partner
Theresa Kim, Associate

Norton Rose Fulbright Canada LLP
May 6, 2015
Bill S-4: "Digital Privacy Act"

Tony Morris, Partner
Norton Rose Fulbright Canada LLP
May 6, 2015
PIPEDA Revisited

• Personal Information Protection and Electronic Documents Act S.C. 2000, c.5 ("PIPEDA")

• CSA's "Model Code for the Protection of Personal Information"

• establishes rules for how private sector organization can collect, use or disclose personal information in the course of commercial activities

• January 2001 applied to PI about customers or employees in federal works, undertakings or businesses in the course of commercial activities

• January 2004 applied to all private sector organizations except those in provinces with substantially similar legislation

• does not apply to employees in the private sector only federal works, undertakings or businesses
PIPEDA Revisited

• Key factors:
  – 10 fair information practices
  – consent to the collection, use or disclosure of PI needed, with limited exceptions
  – use and disclosure of PI only for the purposes for which consent given
  – collection, use and disclosure purposes must be reasonable, even with consent
  – individual access to PI and corrections
  – Privacy Commissioner of Canada's (PCC) oversight

• 5 year review obligation

• Road to amendment:
  – May 2010: Bill C-29
  – September 2011: Bill C-12
  – May 2013: PCC Report
  – April 2014: Bill S-4
PCC Report: "The Case for Reforming PIPEDA"

• "The environment in which personal information is collected, used and disclosed has undergone a dramatic reshaping since PIPEDA was passed at the turn of the 21st century"

• Advances in computer power and storage and massive expansion in the scale of personal information that organizations collect, use and disclosed has caused an explosion in the role and value of personal information to the digital economy.
Pressure Points: Challenges in Enforcing PIPEDA and Recommendations to Ensure Compliance

• Pressure Point #1: Enforcement
  – The national and international context
  – The risk of falling behind
  – Recommendation: strengthen enforcement and encourage greater compliance:
    o statutory damages
    o order-making powers
    o administrative monetary penalties (AMPs)

• Pressure Point #2: Breaches and the lack of mandatory reports
  – Recommendation: shine a light on privacy breaches
Pressure Points: Challenges in Enforcing PIPEDA and Recommendations to Ensure Compliance

• Pressure Point #3: "Lawful authority" disclosures and lack of transparency
  – Recommendation: lift the veil on authorized disclosures

• Pressure Point #4: Demonstrating accountability
  – Proactive compliance and implementing recommendations
  – Recommendation: "Walk the Talk"
    o demonstrating privacy priorities
    o enforceable agreements
An Overview of the Amendments

a) Provides more specifics regarding the elements of valid consent for the collection, use or disclosure of PI

b) Permits the disclosure of PI without knowledge or consent of the individual:
   - to identify an injured or deceased person or communicate with their next of kin
   - preventing, detecting or suppressing fraud
   - protecting victims of financial abuse

c) Permits organization to collect, use and disclose PI without knowledge or consent:
   - contained in insurance claims witness statement
   - produced in the course of employment, business or profession
An Overview of the Amendments

d) Permits organizations to use and disclose PI without knowledge or consent, related to prospective or completed business transactions

e) Permits federal sector to collect, use and disclose PI without knowledge or consent, to establish, manage or terminate employment relationships

f) Requires organizations to notify individuals and organizations of certain breaches of security safeguards that create "a real risk of significant harm" and report them to the PCC

g) Requires organizations to maintain a record of every breach of security safeguards involving PI under their control

h) Creates offences for contravening certain obligations regarding security safeguard breaches
An Overview of the Amendments

i) Extends period to apply to Federal Court regarding a privacy complaint

j) Providing for the PCC to enter into "compliance agreements" with an organization to ensure compliance with PIPEDA; and

k) Modifies the information the PCC may make public relative to a complaint
Key Change #1: Notification of Breach

- New Sections added to address "breaches of security safeguards":

Definition:

"breach of security safeguards" means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards.
Key Change #1: Notification of Breach

• New Section 10.1:
  
  (1) Report to Commissioner

  An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

  (2) Notification to individual

  Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.
Key Change #1: Notification of Breach

• Report to PCC: as prescribed and "as soon as possible"

• Report to individual: to allow the person to understand the significance and to take steps to reduce the risk, in the prescribed manner, directly or indirectly

• Definition for "significant harm" and enumerated factors to determine "real risk of significant harm"
Key Change #1: Notification of Breach

- New Section 10.2:
  Notification to organizations

  10.2(1) An organization that notifies an individual of a breach of security safeguards under subsection 10.1(3) shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm or mitigate that harm, or if any of the prescribed conditions are satisfied.

- New Section 10.3:
  Records

  10.3(1) An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.
Key Change #2: Expanded Offences

• Amended Section 28:

Offence and punishment

Every person who organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or who 27.1(1) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of

(a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or

(b) an indictable offence and liable to a fine not exceeding $100,000.

• Alberta's PIPA has a similar consequence, for failing to notify with an express reasonability test based on the circumstances. But no offence if relying on the Commissioner's direction.
Key Change #3: Disclosure of PI Without Knowledge or Consent

- Additions to Section 7(3) expands the right to disclose if:
  
  (d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;

  (d.2) made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;
Key Change #3: Disclosure of PI Without Knowledge or Consent

(d.3) made on the initiative of the organization to a government institution, a part of a government institution or the individual’s next of kin or authorized representative and

(i) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse,

(ii) the disclosure is made solely for purposes related to preventing or investigating the abuse, and

(iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;
Key Change #3: Disclosure of PI Without Knowledge or Consent

(d.4) necessary to identify the individual who is injured, ill or deceased, made to a government institution, a part of a government institution or the individual’s next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure;

• Privacy Commissioner's submission to the Standing Committee on Industry, Science and Technology (February 2015)
  – challenges the removal of the "investigative body" regime due to accountability and transparency concerns
  – challenges the current wording of Section 7(3)(c.1) in light of the Supreme Court of Canada's powerful decision in *R v. Spencer* (June 2014) that narrows the field of warrantless searches and "lawful authority"
Key Change #3: Disclosure of PI Without Knowledge or Consent

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or the province; or

(c.2) made to the government institution mentioned in of the as required by that section;

(iv) the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual:
Key Change #4: Business Friendly Disclosures Without Consent

- New Section 7.2 regarding both proposed and completed "business transactions"

- New Section 7.3 regarding federal sector employer right to collect, use and disclose an employee's personal information if needed to "establish, manage or terminate" employment

- New Section 4.01 excluding PIPEDA's application to the new definition of "business contact information"

- Variations of these concepts have formed part of Alberta's PIPA since 2004.
Key developments: “Internet tracking, behavioral/targeted advertising and remarketing”

Kateri-Anne Grenier, Partner
Norton Rose Fulbright Canada LLP
May 6, 2015
What do we mean exactly when we refer to “Internet tracking, behavioral/targeted advertising and remarketing”? 

Some examples:

• collection of data about individuals’ web activities by means of such technology as cookies, web beacons, super cookies, zombie cookies, device data;

• use of the collected data for the purposes of online behavioural advertising (OBA);
  – The Office of the Privacy Commissioner of Canada (OPC) defines OBA as “tracking consumers' online activities, across sites and over time in order to deliver advertisements targeted to their inferred interests”;
What do we mean exactly when we refer to “Internet tracking, behavioral/targeted advertising and remarketing”?

- OBA may involve building profiles based on: geographic location; purchase habits; gender; age range; payment patterns; postal code; language. Some organizations classify URLs addresses into categories of interests;

- the profiles built are used to serve advertisements based on the profile. In some cases these profiles are shared with affiliates, third parties, or are used to send publicity at the request of third parties who have targeted the same profiles;

- in other cases, the profile is coupled with other personal information already detained by the organization;

- remarketing allows an advertiser to build a custom list of users to which to target ads, based on user visits to that advertiser’s website, its customer lists, or other advertisers’ determined criteria.
What privacy issues are raised by these practices?

Privacy concerns that have been raised in the past years include:

- whether some of the information collected and used (IP, URLS address; device identification number; browser-generated information (capabilities, time zone, plug-in data and screen size); geographic location etc.) constitutes “a personal information” under applicable laws;
- if these practices are a legitimate business purpose under PIPEDA;
- if, and how, individuals should be made aware of these practices when purchasing goods and services or visiting a website.
What is the position taken by the Office of the Privacy Commissioner (OPC)?

- The OPC issued Guidelines on Privacy and OBA in 2012.
- The Guidelines were developed to ensure that OBA is performed in a fair, transparent way and in compliance with PIPEDA. The Guidelines focus on the following principles:
  
  1. Although not necessary, OBA may be considered a reasonable business purpose under PIPEDA, provided it is carried out under certain parameters, and is not made a condition of service for accessing and using the Internet, generally;
  
  2. The information involved in online tracking and targeting for the purpose of serving behaviourally targeted advertising to individuals will generally constitute personal information;
What is the position taken by the Office of the Privacy Commissioner (OPC)?

3. Opt-out consent may be adequate in the case of collection and use of non-sensitive information;

In an investigation report issued recently the OPC stated that the context for the OBA Guidelines was targeted advertising in connection with free online websites. When merchants charge consumers for goods and services, a reasonable person could not infer or expect that his/her personal information will be used for OBA as a secondary purpose (whereas, on a free website or free service, one could expect that advertising is the only or primary source of financing;
What is the position taken by the Office of the Privacy Commissioner (OPC)?

4. Opt-in consent must be used for collecting and using sensitive information, and certain information is always off-limits, even with consent (race, religion, health etc.);

5. Even if opt-out is a valid option in the circumstances, the organization must be transparent and make the individual aware of the purposes of the practice and the opt-out options at the time of collection, with tools such as pop-ups, banners etc. Simply explaining the practice in a privacy policy is not sufficient;

6. The opt-out takes effect immediately and is persistent; and

7. Information collected and used is destroyed as soon as possible or effectively de-identified.
How have these principles been applied recently?

- PIPEDA Report of Findings #2014-011: OBA and collection of personal information on a children website
- PIPEDA Report of Findings #2014-001:
  - OPC found that Google’s online advertising service (Google Ad Words remarketing campaign) had wrongfully used sensitive information about an individuals’ online activities to target him with health-related advertisements.
  - the complainant had visited sites offering information about devices used by individuals who suffer from sleep apnea.
  - A cookie was placed in the complainant’s browser and triggered ads for sleep apnea devices to appear on the complainant’s screen when he visited websites that used Google’s advertising services.
  - In this case, it was obvious that the information used was inherently sensitive.
How have these principles been applied recently?

• PIPEDA Report of Findings #2015-001: report on investigation after the OPC received complaints regarding a “relevant ads program” launched by an organization:

  1. the objective of maximizing advertising revenue while improving the online experience of customers is a legitimate business objective under PIPEDA;

  2. with respect to form of consent (opt-in v. opt-out), the OCP makes a clear distinction between free websites and when OBA is performed in the context of a client-customer relationship;

  3. sensitivity of the information may be inherent (e.g., health information) or contextual (through the compilation of identifiers gathered during Internet tracking, coupled with information gathered by the organization for the purpose of selling goods or delivering services);

  4. appropriate safeguards include measures to protect against re-identification of individuals by third party advertisers;

  5. in the case where the individual withdraws his consent to the use of his information for OBA, the profile must be erased and the ads must stop.
How have these principles been applied recently?

• In the UK: *Google Inc. v. Vidal-Hall & Ors*, [2015] EWCA CIV 311 (March 27, 2015).
  
  – The UK Court of Appeal confirmed that UK users of Apple’s Safari web browser could bring a privacy claim against Google for misuse of private information related to its collection, without consent, of browser-generated information (BGI) from Safari users for advertising purposes. Google then would provide the information to advertisers for the purpose of targeted advertising.

  – The claim was allowed to proceed even if the plaintiff did not allege pecuniary loss. The UK Court of Appeal also dismissed Google’s claim that the information collected was not “personal information” and that the US was the proper jurisdiction.
Enforcement of CASL
How long has CASL been in force now?

- The provisions respecting the sending of electronic messages (S. 6) came into force on July 1st 2014. On the 15th of January 2015, the provisions respecting spyware, malware, and the installation of computer programs also came into force. Finally, the provisions respecting the private right of action will come into force on July 1st, 2017.

- With respect to commercial electronic messages, the CRTC (through its website fightsspam.gc.ca) had already received more than 1000 complaints only four days after the date of coming into force. The number of complaints surpassed 100 000 in September 2014.
So far, how have the provisions respecting the sending of electronic messages been enforced?

- 2 cases have caught the public’s attention so far:
  1. The CRTC hit a high note when it issued its first-ever notice of violation under CASL on March 5, 2015.
     - The company was fined $1.1 million in relation to four alleged violations based on commercial electronic messages (CEMs) that were sent to Canadian recipients without their consent, as well as CEMs in which the unsubscribe mechanisms did not function properly.
     - The company’s history contributed to the significance of the penalty. Since 2008, it has been subject to intense criticism for sending unwanted e-mails to unknown recipients.
     - Notwithstanding the entering into force of CASL, the company continued to spam hundreds of recipients daily.
     - The CRTC found that it “flagrantly violated the basic principles of the law by continuing to send unsolicited commercial electronic messages after the law came into force to email addresses it found by scouring websites.”
So far, how have the provisions respecting the sending of electronic messages been enforced?

2. Plentyoffish Media has paid $48,000 for alleged non-compliance with Canada’s anti-spam legislation, following the sending of commercial emails to registered users of its online dating site that did not contain an unsubscribe mechanism compliant with CASL requirements.

   - Unlike in the previous case, the company entered into an undertaking with the CRTC in order to update its unsubscribe mechanism, which probably contributed in lowering the amount of the administrative penalty.

   - This “after the fact” voluntary undertaking was not sufficient in itself, however, to exempt the company from paying a penalty, which demonstrates that achieving compliance must remain the goal, as well as being able to demonstrate due diligence.

   - The CRTC, at least in the early days, will probably be pursuing the largest and most persistent spammers to send a strong signal that willful disregard for the law will not be tolerated. It will probably be less concerned with those who make honest mistakes and demonstrate that appropriate corrective measures have been taken.
What are the advantages of a voluntary undertaking?

- A voluntary undertaking may be entered into at any time. It can have a preventive goal, because once a person enters into an undertaking, no notice of violation may be served on them in connection with an act or omission referred to in the undertaking.
  - The undertaking must be accepted by the CRTC and is a public acknowledgement of a violation.
  - It contains the conditions under which it is made (such as, the measures that will be put into place to ensure compliance).
  - It may, or not, be accompanied by a requirement to pay a specified amount.
  - A person may also enter into an undertaking once it is served with a notice of violation, in order to put an end to the prosecution.
  - A voluntary undertaking will also have the effect of blocking an application made by a victim of spam before a court, under the CASL provisions respecting the private right of action (s. 47) once this section comes into force on July 1st, 2017.
How are the penalties determined? Does CASL provide for fixed amounts?

- CASL only stipulates that the maximum penalty for a violation is $1,000,000 in the case of an individual, and $10,000,000 in the case of any other person (including a corporation).
  - In the case of a violation, the government has a large discretion in the determination of the appropriate sanction.
  - The goal of the administrative penalties is not to punish but rather, to promote compliance with CASL.
  - Factors that must be considered by the CRTC include: the nature, scope, length of the violation; the person’s history with respect to any previous violation of CASL, the Competition Act or PIPEDA; the person’s history with respect to any previous undertaking; the financial benefit that the person obtained from the commission of the violation; and the person’s ability to pay the penalty.
How is the private right of action a game changer?

• The private right of action will allow a person who alleges that they are affected by a violation of CASL or PIPEDA or certain provisions of the Competition Act to apply to a court of competent jurisdiction for an order against one or more persons who they allege have committed the act or omission or who they allege are liable for the contravention.
  – If, after hearing the application, the court is satisfied that one or more persons have contravened any of the provisions referred to in the application, it may order the payment of a compensation in an amount equal to the actual loss or damage suffered or expenses incurred by the applicant, and monetary penalties set out in section 51 of CASL which, instead of being payable to the government, will be payable to the victim.
  – The private right of action is a huge advantage for the victim, because it allows the payment of penalties without having to demonstrate a tort/fault.
  – Defense of due diligence is available to the person being sued.
  – The application cannot be received if the organization has already entered into a voluntary undertaking with the CRTC for the same act or omission.
Is there more to CASL than spam?

- CASL regulates other IT practices, including the installation of computer programs and the unauthorized electronic collection of personal information and e-mail addresses.
- These provisions (S.7 & 8) came into force on January 15, 2015.
- As for computer programs, it is now prohibited for anyone to install, update or upgrade a computer program (e.g., software, mobile apps, video games, etc) on any computer or device in Canada (e.g., tablet, phone, video game consoles, etc) without first obtaining the express consent of the owner of that computer or device. In very limited circumstances (e.g., cookies, java script), express consent is presumed.
- Express consent is required if the program collects personal information, and in this case, additional consent requirements are set out by CASL and the regulations.
Potential Implications of Bill C-51

Theresa Kim, Associate
Norton Rose Fulbright Canada LLP
May 6, 2015
Bill C-51 – An Introduction

• **Full Title:** AN ACT TO ENACT THE SECURITY OF CANADA INFORMATION SHARING ACT AND THE SECURE AIR TRAVEL ACT, TO AMEND THE CRIMINAL CODE, THE CANADIAN SECURITY INTELLIGENCE SERVICE ACT AND THE IMMIGRATION AND REFUGEE PROTECTION ACT AND TO MAKE RELATED AND CONSEQUENTIAL AMENDMENTS TO OTHER ACTS

• **Short Title:** Anti-terrorism Act, 2015

• **Sponsor:** Minister of Public Safety and Emergency Preparedness
Bill C-51 - Legislative Status

• Introduction and First Reading: January 30, 2015
• Second Reading and Referral to Committee: February 23, 2015
• Committee Reporting the Bill with Amendments in the House of Commons: April 2, 2015
• Concurrence at Report Stage in the House of Commons: May 4, 2015
• Third Reading at House of Commons: May 5, 2015
Bill C-51 - Brief Overview

- Enacts the Security of Canada Information Sharing Act
- Enacts the Secure Air Travel Act
- Amends the Criminal Code
- Amends the Canadian Security Intelligence Service Act
- Amends the Immigration and Refugee Protection Act
Bill C-51 – Potential Implications for Businesses

Data Sharing by Government Departments

Canadian businesses holding foreign customer data

Canadian companies holding Canadian customer data

Data Sharing between Government Departments

Discussion from critics:
• Potential chill on Canadian businesses.
• Reputational impact on Canada.
• Any “relevant” information captured
Bill C-51 – Potential Implications for Businesses

Data Sharing by Government Departments

"We work with international clients, and we fear that this proposed legislation will undermine international trust in Canada's technology sector, thereby stifling the kinds of business our respective technology companies can generate when that level of trust is high."


"If adopted in its current form, the Security of Canada Information Sharing Act would make available to 17 federal departments and agencies, which hold some responsibilities in relation to national security, potentially all personal information that any department may hold on Canadians. … [The] language used in SCISA to confer information is extremely broad. For instance, all the tax information held by the Canada Revenue Agency, which historically has been highly protected information, would be broadly available if deemed relevant to the detection of new security threats."

(Bill C-51, the Anti-Terrorism Act, 2015, Submission to the Standing Senate Committee on National Security and Defence (by the Office of the Privacy Commissioner of Canada), April 16, 2015 (website: https://www.priv.gc.ca/parl/2015/parl_sub_150416_e.asp))
Bill C-51 – Potential Implications for Businesses
Communications, Speech, Writings, Signs, Visuals, Audio

Section 83.221(1) Every person who, by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general – other than an offence under this section – while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed, as a result of such communication, is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years.

Seizure and deletion of “terrorist propaganda”

"Terrorist propaganda" means means any writing, sign, visible representation or audio recording that advocates or promotes the commission of terrorism offences in general — other than an offence under subsection 83.221(1) — or counsels the commission of a terrorism offence.
Bill C-51 – Potential Implications for Businesses

Communications, Speech, Writings, Signs, Visuals, Audio - Examples:

• Statements – public statements, private statements, emails, text messages
• Websites available to the public with controversial material
• Social media
• Advertisements, marketing media and campaigns
• Journalistic speech, interviews and articles
• Linking to certain websites
• Demonstrations
Bill C-51 – Potential Implications for Businesses

No Fly List

- Travel for business and leisure
- Domestic and international travel
- CBSA assistance in administration and enforcement
- Disclosure of the list to air carriers and operators of aviation reservation systems
- Minister of Transport can have agreement with foreign states to share the list
- Judicial review available
Recent Privacy Breaches and Lessons Learned
Recent Privacy Breaches – Federal Government

2013-2014 Annual Report to Parliament, Office of the Privacy Commissioner of Canada

- OPC received reports of 228 data breaches across the federal government, more than double the 109 from the previous fiscal year. Accidental disclosure (i.e. human error) accounted for just over two-thirds of those breaches. (Office of the Privacy Commissioner of Canada, 2013-14 Privacy Act Annual Report to Parliament)

Canada Revenue Agency

- In November 2014, the CRA accidentally disclosed a document to the CBC containing confidential taxpayer information, such as home addresses, and value of tax credits.
- In March 2013, the CRA had accidentally mailed confidential personal information to the wrong recipient. The package contained the recipient’s information, but also the confidential information of five other Canadians.

Veterans Affairs Canada

- Annual Report on the Administration of the Privacy Act for the 2013-2014 fiscal year reported 87 privacy breaches impacting 101 individuals.
Recent Privacy Breaches – Federal Government

Employment and Social Development Canada

– In November 2012, a loss of an external hard drive containing the personal information of 583,000 student loan recipients was reported. The OPC investigation reported that the hard drive was left unsecured for extended periods of time, not password protected and held unencrypted personal information.

– In November 2012, the ESDC lost a USB key containing the personal information of 5,045 people appealing their disability entitled under the Canada Pension Plan was missing.

Health Canada

– In 2013, Health Canada mass mailed to 40,000 people involved in a marijuana medical access program. The mail contained he individual’s name and that the individual was part of the program.
Recent Privacy Breaches - Ontario's Health Sector

- **Hopkins v. Kay, 2015 ONCA 112**
  - Approximately 280 patients of the Peterborough Regional Health Centre were inappropriately accessed and disseminated to third parties by several hospital employees without the patients' consents.
  - Plaintiffs claimed damages under the tort of intrusion upon seclusion. The hospital unsuccessfully brought a motion to strike the claim arguing that the claim fell under the *Personal Health Information Protection Act* (PHIPA) and as such the court does not have jurisdiction to hear the claim.
  - The court held that the claim for intrusion upon seclusion should be permitted to proceed in Ontario.
Recent Privacy Breaches – By Year

2015

January 2015: Newfoundland and Labrador Motor Registration Division breach by inappropriate access of personal information by an employee who revealed the information of 28 people to another individual who is not an employee.

2014

December 2014: Sony breach by hackers leaked unreleased movies and employee personal information, including 47,000 social security numbers of current and former employees, and posted publicly.

January 2014: Neiman Marcus reported a similar malware breach initially thought to affect 1.1 million credit card and debit card information. Further investigations revealed 350,000 customers were affected.
Recent Privacy Breaches – By Year

2013

2013-2014: Employees of AT&T stole personal information of nearly 280,000 AT&T customers at call centers in Mexico, Colombia and the Philippines, including names, social security numbers and account information. The information was sold to a third party dealing with stolen devices and was used to request unlock codes. The breaches occurred from 2013 and 2014. On April 8, 2015, the Federal Communications Commission fined AT&T $25 million for the breaches.

December 2013: Target security breach over the holidays a couple of years ago of over 110 million accounts, including customer names, emails, mailing addresses, credit and debit card information, numbers, expiration dates and card security codes, were stolen. The security breach was from a malware infected on point of sale devices which transmitted the information to the thieves.

October 2013: Adobe reported 3 million customers' credit card information was stolen. A leak also exposed the login information, such as email addresses and passwords, of 40 million users.
Recent Privacy Breaches and Lessons Learned

Lesson 1: Tips to Prevent the Breach

- Regular audits on systems and processes
- Detect security breaches and flaws through vigilance, safeguards and technological tools
- Use encryption when downloading to external devices
- Use access controls on documents and files containing personal information.
- Establish privacy policies and procedures and update regularly
- Staff training on procedures and policies
- Limit access to personal information by employees whose function do not require it
- Develop employee termination procedures
- Use window envelopes to ensure letters are sent to the correct address - but careful that the window does not show too much information or sensitive information
- Use caution in giving network and building access to contractors and ensure proper controls are in place
Recent Privacy Breaches and Lessons Learned

Lesson 2: Develop a Corporate/Communications Response Plan

– Establish a privacy officer and inform privacy officers in all affected jurisdictions of the security breach
– Establish a incident response team, complete with members, contact information, reporting lines and responsibilities. Depending on the scope of personal information collection and retention, multijurisdictional team may be advisable. Consistency of the response, where possible, is key.
– Identify where personal information is stored, the nature of the information, the affected individuals, who has access and who is responsible
– Identify reporting and notification protocols - internal, regulatory authority and affected individuals.
– Ensure clear "chain of command" in cases of security breach.
– Timelines in breach response plan must be immediate - hours not days
– Have all relevant documents consolidated (including insurance policies and key contracts - particularly where dealing with third-party supplier actions could be at issue).
– Measure that can be taken to minimize the impact.
– PR response to media queries and internal communications strategy.
Recent Privacy Breaches and Lessons Learned

Lesson 3: Responding to the Breach

1. Breach containment and preliminary assessment
   – Immediately contain the breach - activate the breach response plan; notify the members of the response team; stop the unauthorized access

2. Evaluate the risks associated with the breach
   – Investigate the incident
   – Evaluate the cause of the breach and the extent - What data was involved? How sensitive is the information?
   – Identify the individuals affected by the breach - Who was affected and how many individuals are affected?
   – Assess the foreseeable harm from the breach - For example, security risk, identity theft, financial loss, loss of business opportunity, physical harm, humiliation, damage to reputation, legal proceedings, and consider whether public harm could result from notifying the public of the breach
Recent Privacy Breaches and Lessons Learned

3. Notification
   – Reporting obligations to the appropriate regulatory authorities
   – Inform the police if the breach involves criminal activity (e.g. theft)
   – Notify the affected individuals - Assess when and how individuals should be notified, and what should be included
   – Notify your insurer

4. Prevention
Recent Privacy Breaches and Lessons Learned

Lesson 4: After the Breach - Assess

– How or why did the breach happen?
– How could it have been prevented?
– What are the lessons learned?
– What are the repercussions? Review your policies. Review employee training. Review contracts. Are any changes needed?
Alberta's *PIPA* Invalidation by the Supreme Court of Canada

Tony Morris, Partner
Norton Rose Fulbright Canada LLP
May 6, 2015
The Context  - Lawful Strike at West Edmonton Mall

• In 2006, members of the United Food and Commercial Workers, Local 401 (the "Union") were engaged in a lawful strike at the Palace Casino at West Edmonton Mall in Alberta.
  – The strike lasted 305 days.
  – The Union and a security company hired by the Employer video-taped and photographed the picket line near the main entrance to the Casino.
  – The Union posted photos of individuals, including Union members, crossing the picket line on a website.

• Complaints were filed with the Alberta Information and Privacy Commissioner under PIPA alleging that the Union had unlawfully collected, used and disclosed personal information without the consent of the individual complainants.
The Decisions Below

• The Privacy Commissioner of Alberta
  – An Adjudicator appointed by the Commissioner found that the Union's actions violated portions of PIPA.

• Judicial Review
  – The Union brought a constitutional challenge alleging that PIPA limited the Union's freedom of expression under Section 2(b) of the Charter.
  – Both the chambers judge and Court of Appeal found that PIPA was overbroad, breached the Union's rights under Section 2(b) of the Charter and could not be saved under s. 1.
The Supreme Court of Canada's Declaration of Unconstitutionality

- The Commissioner and Attorney General of Alberta request that if portions of PIPA are found to be unconstitutional, the Supreme Court of Canada strike down the entirety of the Act.

- The SCC found that the Union's s. 2(b) Charter rights were unreasonably infringed and therefore declared PIPA invalid.
  - the invalidity was suspended for 12 months or until November 15, 2014.

- Constitutional Right - Freedom of Expression
  
  Section 2 of the Charter - Fundamental Freedoms:
  2. Everyone has the following fundamental freedoms:
     
     (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
Balancing Constitutional and Quasi Constitutional Rights

• Quasi Constitutional Right - Individual Right to Privacy

Para 19 of the SCC's decision: "The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as “quasi-constitutional” because of the fundamental role privacy plays in the preservation of a free and democratic society"

• The Balance Between Rights

Para 38 of the SCC decision: "It is enough to note that, like privacy, freedom of expression is not an absolute value and both the nature of the privacy interests implicated and the nature of the expression must be considered in striking an appropriate balance."
Nature, Purpose, Context

• The SCC comments on the balance between freedom of expression and protection of privacy:

[25] The price PIPA exacts, however, is disproportionate to the benefits it promotes. PIPA limits the collection, use and disclosure of personal information other than with consent without regard for the nature of the personal information, the purpose for which it is collected, used or disclosed, and the situational context for that information. As the Adjudicator recognized in her decision, PIPA does not provide any way to accommodate the expressive purposes of unions engaged in lawful strikes. Indeed, the Act does not include any mechanisms by which a union’s constitutional right to freedom of expression may be balanced with the interests protected by the legislation. As counsel for the Commissioner conceded during oral submissions, PIPA contains a general prohibition of the Union’s use of personal information (absent consent or deemed consent) to further its collective bargaining objectives. As a result, PIPA deems virtually all personal information to be protected regardless of context.
The Privacy Commissioner's Letters Government

• There were a number amendments available to the Province following the Supreme Court of Canada's decision:
  – The Narrow Approach:
    confine amendments to labour disputes.
  – The Broad Approach:
    adopt amendments to broader contexts where freedom of expression conflicts with privacy rights.

• Commissioner Clayton writes to the Ministers of Justice and Solicitor General and of Service Alberta advocating for narrow amendments.
  – She recommends adding authorizing provisions to allow the collection, use and disclosure of personal information by unions for expressive purposes without consent during a lawful strike.
The Privacy Commissioner's Letters Government

- Commissioner Clayton writes to the Premier and Ministers of Justice and Solicitor General and Service Alberta after the Alberta Legislature is prorogued until after the date set for PIPA to lapse.

- The government seeks an extension which the Supreme Court of Canada grants just 15 days before the legislation was set to lapse.
The Debate: Narrow v. Broad Amendments to PIPA

**Opposition to the Narrow Approach:**

"These rights of expression, Mr. Speaker, don't just benefit unions. As I said, the major purpose is to address political and social issues of the day and then work for social justice for all Albertans. So the specific work that a union might do to, as I said before, express and talk about health and safety issues but also workplace standards, wages, and so forth indirectly and directly affects positively the larger society as well. Anyway, by denying a key right necessary for individuals or unions to communicate and achieve these objectives, this bill is too restrictive, and we think that the well-being of all Albertans and, in fact, democracy is adversely affected as well." (David Eggenn)

"From the beginning of the process to the end unions need to be able to communicate freely in order to advance their interests and, as I've said, to advocate on behalf of the public good. By extending the right to collect, use, and disclose personal information only in the context of a labour dispute, which is how Bill 3 is currently written, Mr. Speaker, it flies in the face of the Supreme Court findings and advice because of that restriction to gather information only when there is a labour dispute and not when, obviously, there isn't one."

"The unconstitutionality of this legislation stems from its application to all personal information regardless of the organization's purpose in using such information. This piece of legislation may also invite more litigation from unions, political or social groups whose freedom of expression this current bill will continue to infringe upon. The other part, Mr. Speaker, is that it will involve the Privacy Commissioner in labour disputes rather than leaving those issues regarding such disputes to be resolved by the Labour Relations Board, which is an expert tribunal on such matters and where, quite frankly, those decisions should remain." (Deron Bilous)

**Arguments in Support of the Narrow Approach:**

"The proposed changes will ensure that the Personal Information Protection Act authorizes trade unions to collect, use, and disclose personal information for matters related to labour relation disputes. Those amendments will address a trade union's right of freedom of expression under the Charter of Rights and Freedoms while maintaining key protection for Albertans' personal information under the act." (Sohail Quandri)

"Other legislative options are available that would protect expressive activities of unions. For example, a somewhat broader exception could be enacted for expression by unions engaged in legitimate labour relations activities. However, this would go beyond the constitutional question stated by the Court. Even more broadly, union expression in the course of labour relations activities could be added to the exemption provisions that specify certain activities to which the Act does not apply. Finally, unions could conceivably be excluded from the Act altogether. However, in my view, neither of these latter mechanism would permit the appropriate "balancing" called for by the Court. The result would be that expressive activates by unions that caused disproportionate harms, or were otherwise clearly unreasonable relative to the union's purposes, could not be enjoined. As stated in its decision, the Court's conclusion did not mean that it necessarily condoned all of the Union's expressive activities [para. 38].

Further, these alternative solutions would remove the protections in PIPA that ensure that personal information that is collected for a union's expressive labour relations purposes be appropriately secured, or destroyed when no longer needed. It would also remove the ability of individuals to request access to their own personal information collected by unions for such purposes." (Jill Clayton, Information and Privacy Commissioner)
Bill 3 - Personal Information Protection Amendment Act, 2014

• The Balance Adopted by the Legislature
  – Alberta adopts a narrow exception
  – Labour disputes and unions are not excluded from the application of PIPA under Section 4.
  – A trade union is allowed to collect, use and disclose personal information without the consent of the individual, only if:
    o The information is being collected, used and/or disclosed in the context of a labour dispute.
    o The information is for the purpose of persuading the public about a matter of significant public interest and importance relating to a labour relations dispute involving the trade union.
    o The collection, use and/or disclosure of the personal information is reasonably necessary for the purpose of persuading the public about a matter of significant public interest and importance relating to a labour relations dispute.
Bill 3 - *Personal Information Protection Amendment Act, 2014*

- Collection by a trade union relating to a labour dispute
  14.1(1) Subject to the regulations, a trade union may collect personal information about an individual without the consent of the individual for the purpose of informing or persuading the public about a matter of significant public interest or importance relating to a labour relations dispute involving the trade union if
    (a) the collection of the personal information is reasonably necessary for that purpose; and
    (b) it is reasonable to collect the personal information without consent for that purpose, taking into consideration all relevant circumstances, including the nature and sensitivity of the information.

  (2) Nothing in this section is to be construed so as to restrict or otherwise affect a trade union's ability to collect personal information under section 14.

- Similar clauses regarding use and disclosure
Bill 3 - *Personal Information Protection Amendment Act, 2014*

- Other Jurisdictions Follow the Alberta Lead

The same narrow exception is recommended by the Report of the Special Committee to Review the *Personal Information Protection Act* tabled February 6, 2015 to the Legislative Assembly in British Columbia.
What's Next?

• Comprehensive review of PIPA is scheduled to begin in July 2015:

   63(1) A special committee of the Legislative Assembly must begin a comprehensive review of this Act and the regulations made under it (a)by July 1, 2015, and ... 

   (2). A special committee must submit a final report to the Legislative Assembly within 18 months after beginning a review under subsection (1).

• The debate continues...
  – Within the labour dispute context
    o how is "significant public interest" to be defined?
    o how is "reasonably necessary" to be defined
  – Outside the labour dispute context
    o What other political or social groups' freedom of expression are infringed upon under PIPA?
Disclaimer

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

References to 'Norton Rose Fulbright', 'the law firm' and 'legal practice' are to one or more of the Norton Rose Fulbright members or to one of their respective affiliates (together 'Norton Rose Fulbright entity/entities'). No individual who is a member, partner, shareholder, director, employee or consultant of, in or to any Norton Rose Fulbright entity (whether or not such individual is described as a 'partner') accepts or assumes responsibility, or has any liability, to any person in respect of this communication. Any reference to a partner or director is to a member, employee or consultant with equivalent standing and qualifications of the relevant Norton Rose Fulbright entity.

The purpose of this communication is to provide general information of a legal nature. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.