Canadian Cyber Liability: Looking back on 2015 and what 2016 presents

A presentation to

The Casualty Actuarial Society

October 28, 2016

What legal remedies exist in Canada as of 2015?

- In 2012 developed tort of intrusion upon exclusion for provinces with no Privacy Act
- Provincial Privacy Acts 5 provinces
- The statutory cause of action for damages under PIPEDA

What legal remedies exist in Canada as of 2015?

- Publicity given to private life (new cause of action – 2016)
- Breach of contract
- Negligence
- Breach of confidence
- Breach of fiduciary duty

What new legal remedies are emerging in Canada?

July 1, 2014 enactment of Canadian anti-spam legislation

- Deals with spam, botnets, phishing and host of cyber problems
- Damages awarded as of July 1, 2017
- Up to $1.0 m per day for "compensatory damages"
- Cases heard before CRTC- expensive to defend

Canadian cyber claims take a differing route than U.S. cyber claims

- In U.S. automatic breach notification laws in 47 states – notify affected parties
- In Canada duty to notify Privacy Commissioner – he or she directs whether notify affected parties
- Under PIPEDA claimant needs a ruling from Privacy Commissioner then claimant sues in Federal Court or provincial Court for damages

Canadian cyber claims take a differing route than U.S. cyber claims

- In U.S. once notified the claimants can commence a class action
- In Canada start a class action if use the Privacy Act/tort "route" – Facebook certified June, 2014
- Privacy Act protects all aspects of privacy: tort only protects "person" "your home" and "your data"

Canadian cyber claims take a differing route than U.S. cyber claims

- PIPEDA only governs personal information collected in business setting
- Privacy Act/tort protects your personal life and information
- Choice: let Privacy Commissioner do the investigation or sue using Privacy Act/tort of privacy

Damages for breach of privacy differ from the U.S.

- In U.S. requirement of "injury in fact" – *Clapper* decision of U.S. Supreme Court – Article 3 of U.S. Constitution
- Problem in U.S.: significant defence costs resisting certification but no damage exposure
- In Canada "actionable without proof of damages" – gist of the cause of action differs from U.S. – no need to prove actual damage – nominal damages
- Result: easy to certify class action in Canada since "common issue"

How do cyber claims in the U.S. differ from Canada?

- U.S. Plaintiff bar uses consumer protection legislation – claim based on misrepresentation
- In Canada have "purpose built" legislation:
  - PIPEDA – whether loss of data accidental or done with intent it is a breach and actionable
  - Privacy Act and "Judge made" tort – it is the disclosure that makes it actionable; no need for actual damages

How do cyber claims in the U.S. differ from Canada?

- Difference: PII in U.S. is limited "shopping list" – in Canada every aspect of your life in PII

Which legal remedy do claimants resort to in Canada?

- Single claimant affected: PIPEDA – investigation done by Privacy Commissioner and then go to Court
- Group of claimants: tort and Privacy Acts – suitable for class action – damages awarded if no pecuniary loss

What is the damage trend for loss of personal information?

- 2010 – Federal Court awarding $5,000 to $6,000 per claimant without proof of actual pecuniary loss
- 2014 – Federal Court awarding $15,000 to $20,000 per claimant if evident breach was culpable (*Chitraka v. Bell*)

How do you avoid mandatory breach notice?

When will need arise?

- Your insured is obligated to report to Privacy Commissioner,
- the insured self-reports to Privacy Commissioner, or
- someone loses data and complains to Privacy Commissioner

How do you avoid mandatory breach notice?

- Being able to determine what data has been hacked or destroyed
- Having a forensics expert identifying who took the data and how quickly a "firewall" can be erected around the compromised data
- Assurances that no further disclosure or harm from disclosure

How quickly does a cyber insurer have to respond to the Privacy Commissioner?

- As soon as practical
- Problem if you don't cooperate: subpoena/formal hearing
- A formal Order increases the likelihood of ensuing litigation

How does the role of a breach coach differ in Canada from the US?

- Identifying the resources needed to address the hacking/loss of data
- Identifying which provincial Privacy Commissioner needs to be notified of loss
- Preparing a defensible case for the Privacy Commissioner
- Efforts to avoid an Order of the Privacy Commissioner
- After the Privacy Commissioner defending the insured in Federal Court (under PIPEDA)

Steps in a typical Canadian cyber claim

First Party

- Forensic investigation
- Internal Investigation
- Re-establish security and functionality
- Indentify assets lost
- Retrieve data and/or prevent further loss
- Quantify BI Loss
- Notify affected individuals
- Crisis management

Regulatory

- Privacy Commissioner gets notified
- Negotiate content and breadth of notice
- Demonstrate due diligence
- Negotiate regarding remedial steps
- Try to avoid an investigation and a ruling
- Respond to investigation
- Corrective steps may be required
- Possible fines

Third Party

- Investigate facts to prepare defence
- Third party gets notified
- May commence lawsuit
- May make complaint to regulator
- Defence expenses
- Settlement/judgment

The biggest practical problems for cyber insurers in Canada?

- Wide range of hourly rates for data restoration firms and varied response times
- Insurers that make statements to Privacy Commissioners before reporting claim to cyber insurer
- Failing to mitigate loss before coverage is confirmed
- Ignoring customer complaints that lead to mandatory Privacy Commissioner Orders
- Knowing how to deal with the Privacy Commissioners and their enforcement staff

Canada moves to mandatory

- Federal legislation: Bill S-4 Digital Privacy Act became law June 1, 2015
- Mandatory breach notification if "real risk" of significant harm
- "Harm" includes:
  - loss of reputation
  - loss of identity
  - financial loss, or
  - harm to credit
  - property damage/bodily injury
  - loss of employment
  - loss of business or professional opportunity

The impact of CASL on cyber indemnity exposure

Became law as of July 1, 2014

- Regulates spam, identity theft, phishing, spyware, viruses, botnets
- Problem: if hacker uses your system to commit an offence – jointly and severally liable with hacker/intruder
- "due diligence" defence available
- Damages up to $1.0 m in compensatory damages as of July 1, 2017
- Expensive to defend before the CRTC

Canadian Certified Class Actions

Hacking/Extortion

- *Bennett v. Lenovo (Canada) Inc.*, Ontario 2015
- *Shore v. Avid Dating Life Inc.* (Ashley Madison), Ontario & Quebec 2015 (and 12 U.S. states)
- *Tucci v. People's Trust*, BC 2015
- *Zuckerman v. Target*, Federal Court, 2015

Canadian Certified Class Actions

Employee Bad Behaviour

- *Evans v. Bank of Nova Scotia*, Ontario, 2014
- *Hopkins v. Kay*, Ontario 2015
- *Broutzas/Taylor v. Rouge Valley*, Ontario 2014

Canadian Certified Class Actions

Big Data/Corporate Profiteering

- *Tocco v. Bell Mobility*, Ontario 2015
- *Douez v. Facebook*
- *Plimmer v. Google*, BC 2012
- *Elkoby v. Google*, Quebec 2011
- *Albilia v. Apple Inc.*, Quebec 2013
- *Ladas v. Apple Inc.*, BC 2014

The Honda Case: A case study

5 Person IT firm contract to update website

Employee steals customer list for personal use

Lawsuits in Canada and US to recover data and seeking damages

Class action settled

Damages

- $185,000 - Computer forensics expenses
- $326,000 - Legal costs in USA to stop spread & misuse of data
- $200,000 - Mailing notice to 120,000 Canadian auto owners
- $450,000 – Manufacturer's legal costs to defend class action and Privacy Commissioner
- $300,000 - IT firm's defence costs in USA and Ontario
- Undisclosed settlement paid to settle class action (Confidential)

- **Disgorgement of profits / waiver of tort** (*Tucci v People's Trust*; *Tocco v Bell*; *Evans v. Bank of Nova Scotia*)
- **What is personal information** (Medical Marijuana)
- **Adequacy of consent** (*Tocco v Bell*)
- **Vicarious liability** (*Ari v. ICBC*; *Evans v. Bank of Nova Scotia*)
- **Stacking of remedies** (*Tucci v. People's Trust*, *Hopkins v. Kay*)
- **Damage requirement for negligence, breach of confidence** (Condon student loan)
- **Punitive damages** (Ashley Madison)

Key Points Emerging in 2016

- Claimants can claim nominal damages for loss of personal information data even if no pecuniary loss
- Not difficult to certify a class action
- Emergence of Plaintiff class action bar specializing in cyber claims
- Privacy Commissioners more aggressive in ordering breach notice (before Bill S-4)
- Securing capable data restoration and forensics firms challenging
- Need to know how to work with Privacy Commissioners to avoid Orders

Questions?

DOLDEN WALLACE FOLICK LLP

Insurance Lawyers