The MEARIE 2018 Conference

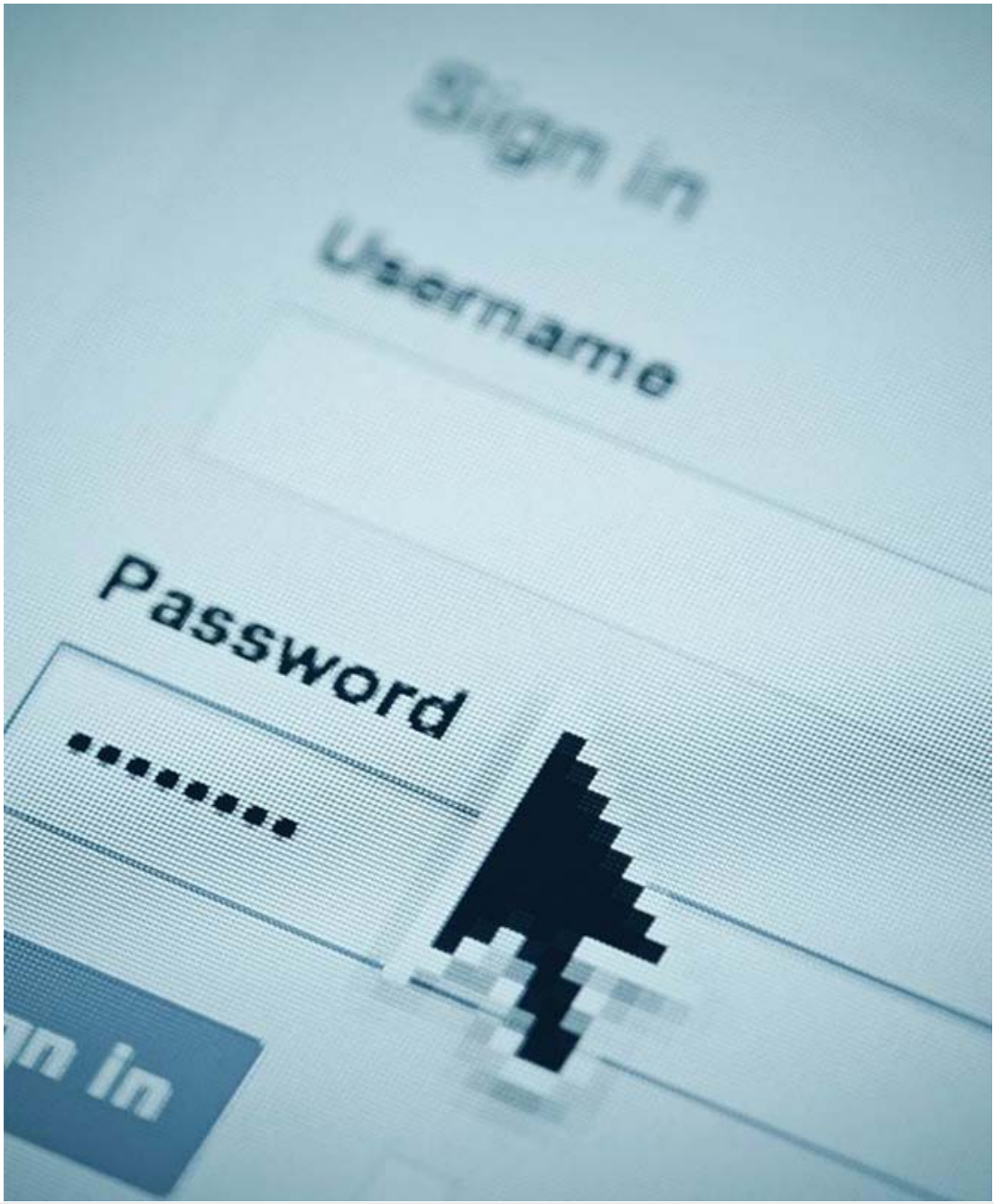
Canada’s new privacy breach reporting law

Karl Schober
Dentons Canada LLP

22 June 2018

This morning

1. Legal landscape
2. Reasons and ramifications
3. Canada's new data breach requirements
4. Class actions
   - Home Depot
5. Lessons + insights



Legal landscape

Privacy regime

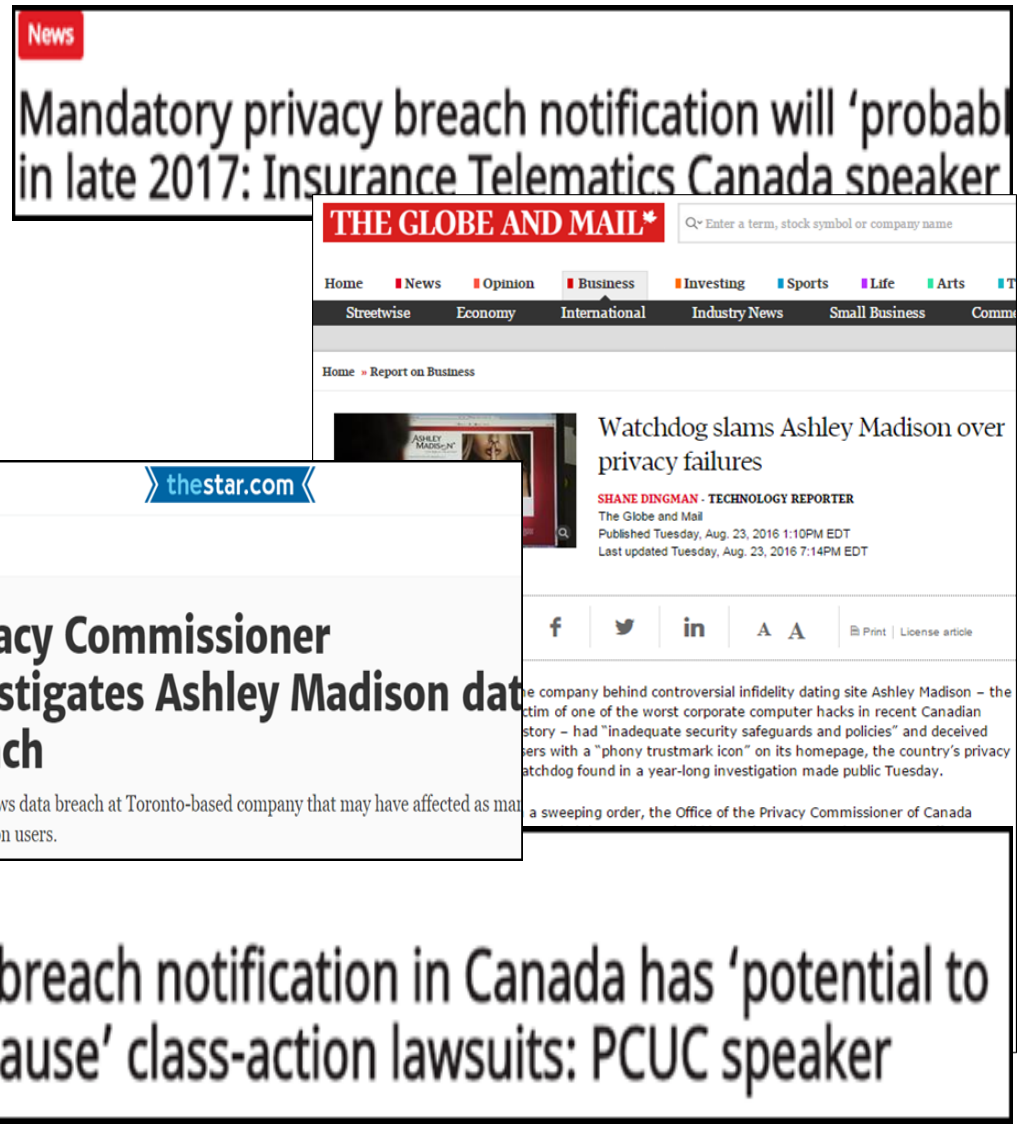
- Alberta's *Personal Information Protection Act*
- Ontario's *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
- Ontario Energy Board
  - New cybersecurity framework
- Common law

- Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA)

Breaches
Reasons and ramifications

Ramifications

- Name and shame
- Power to investigate and issue public findings
  - Commissioner and individuals can then apply to court for monetary damages
- Right now – no statutory penalties
- As of November 1 - Penalties with respect to new PIPEDA data breach obligations
  - up to $100,000
    - Failure to report breach
    - Failure to maintain records for 24 months



Ramifications cont'd

Class actions

- Breach of contract
- Negligence
- Breach of confidence and violation of privacy
- Breach of fiduciary duty
- Intrusion upon seclusion
- Breach of statutory duty (i.e. PIPEDA)

Other

- Public relations
- Loss of consumer confidence
- Operational disruption
- Financial costs
  - Notification
  - Free credit monitoring
  - Resources
- Opens door to investigations and audit

Canada’s new data breach requirements

Evolution of incident response

- From sending letters out to strategic disclosure
- Investigation
- Remediation
- Disclosure

General framework of response

Record

Keep records of breaches of security safeguards

Report

Report breaches to the OPC if the risk of harm threshold is met

Notify

Notify affected individuals if the risk of harm threshold is met

Mitigate

Notify third parties if they could mitigate the risk of harm

What is a breach of security safeguards?

- the loss of, unauthorized access to or unauthorized disclosure of personal information
- resulting from a breach of an organization's security safeguards
- or from a failure to establish those safeguards

Report

- report to the OPC if it is reasonable in the circumstances to believe that the breach [of security safeguards] creates a real risk of significant harm to an individual
- report as soon as feasible

What is…

“real risk”

- the sensitivity of the personal information involved in the breach;
- the probability that the personal information has been, is being or will be misused

“significant harm”

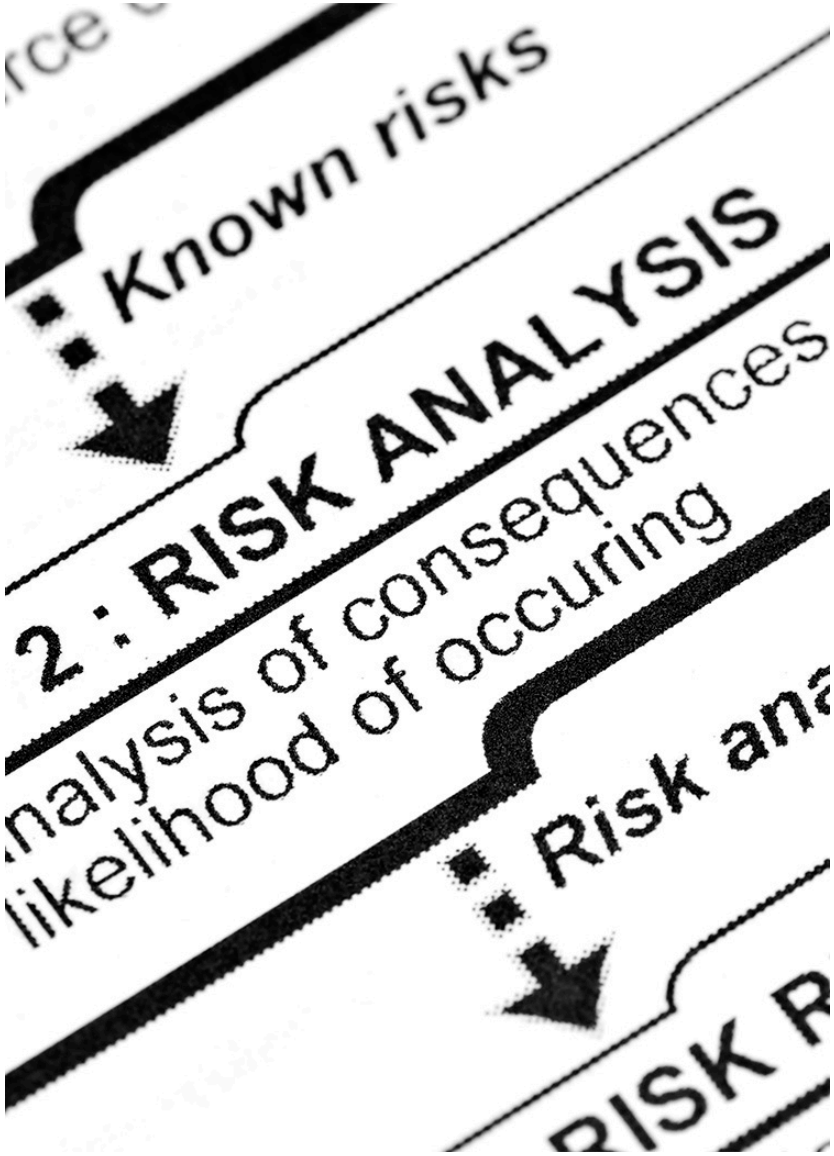
- includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Contents of the report

- a description of the circumstances of the breach and, if known, the cause
- the day on which, or the period during which, the breach occurred
- a description of the affected personal information
- an estimate of the number of affected individuals
- a description of the steps taken to reduce the risk of harm or to mitigate that harm
- a description of the steps that the organization has taken or intends to take to notify affected individuals
- contact information

Contents of notification

- a description of the circumstances of the breach and, if known, the cause
- the day on which, or the period during which, the breach occurred
- a description of the affected personal information
- a description of the steps taken to reduce the risk of harm or to mitigate that harm
- what the affected individual could do to reduce the risk of harm or to mitigate that harm
- a toll-free number or email address to obtain further information about the breach
- information about the organization's internal complaint process and the right to complain to the OPC



Direct notification

- email or any other secure form of communication if the affected individual has consented to receiving information from the organization in that manner
- by letter delivered to the last known home address of the affected individual
- by telephone
- in person

Indirect notification

- direct notification would cause further harm to the affected individual
- the cost of direct notification is prohibitive for the organization
- the organization does not have contact information for the affected individual or the information that it has is out of date

- by a conspicuous message, posted on the organization's website for at least 90 days
- by means of an advertisement that is likely to reach the affected individuals

Records

- keep and maintain a record of every breach of security safeguards involving personal information under its control
- retain for 24 months after determining the breach occurred
- must contain information pertaining to the breach that enables the OPC to verify compliance with the breach reporting and notification provisions
- content is not prescriptive
- will need to ensure service providers who have custody of personal information cooperate
- a report to the OPC of a breach containing the prescribed information can be used as a record

Class actions

Movement in data incident litigation

Developments

Some background and trends

- increased litigation in last 5 years
- rapid increase of class actions since 2016
- significant number of class actions involve incidents caused by malicious actors
- courts recognizing inconvenience and upset sufficient to certify?

Developments and trends

My not-so-scientific, scientific study

Causes

1. Malicious actors
2. Employee snooping and misuse by authorized users
3. Loss of devices
4. Accidental

Industries

1. Tech
2. Health
3. Public Bodies (Government)
4. Financial
5. Retail (online + point of sale)

Cybersecurity incidents

Private sector

- Equifax
- Uber
- Ashley Madison
- Yahoo!
- Target
- Home Depot
- Walmart
- Eddie Bauer
- Etc.

Energy sector

- American Electric Power (2016)
- Board of Water & Light (2016)

Non-commercial

- Increase in Doxing

Home Depot

Background

- custom-built malware on point of sale systems (self-checkout)
  - Stripe only
- April - September 2014
- obtained payment information of 500,000 customers
- harm test met
- engage its response plan
- none of the regulators found Home Depot had violated privacy law
- Offered premium package to affected individuals

Home Depot cont'd

Class actions

- British Columbia, Saskatchewan, Ontario, Quebec, Newfoundland
- was there actual harm suffered?
- issues with claim, class lead and their experts
- Parties move to settle, class counsel value settlement at $1 million

Settlement

- court approved national settlement agreement, but reduces value of claim
- $250,000 settlement fund, down from over $1 million
- Agreed to pay credit monitoring, up to $250,000
- Counsel fees, $120,000 down from over $400,000

Home Depot cont'd

"There comes a point when the litigation should be abandoned, discontinued, or settled," - Justice Perell

"…that despite utmost diligence and efforts to prevent data breaches, companies remain vulnerable because hackers continually develop new malicious code and the game of cat and mouse continues," - Justice Perell

Lessons

- Still a developing area in Canadian litigation
- Push that class members must demonstrate actual harm
- The need for a governance framework
- Data breach response playbook
- Vendor risk management
  - Arguably the weakest link
  - Organizations cannot coast
- Litigation risk
  - Voluntarily offer credit and identify theft?
  - Difficulty for courts to quantify harms

Thank you

Karl Schober
(416) 863 4483

Dentons Canada LLP
77 King Street West
Suite 400
Toronto, Ontario M5K 0A1
Canada

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.
www.dentons.com