Privacy Update – What's New, What's Changing and What Consumers Think

Chris Kelly, Navigator Ltd
Barry Sookman, Partner, Technology, McCarthy Tétrault
Kirsten Thompson,Counsel and Co-Lead, National Cybersecurity, Privacy and Data Protection Group, McCarthy Tétrault

Cybersecurity: Preventing and Managing a Breach

Kirsten Thompson
Counsel and Co-Lead, National Cybersecurity, Privacy and Data Protection Group

Cybersecurity Preparedness

Before:

- Governance
- Cybersecurity Response Plan
- Training and Policies
- Third Parties and IT Service Agreements
- IT Security
- Cybersecurity Risk Allocation/Cyberinsurance

After:

- **Cybersecurity Response Plan**
- Team

Cybersecurity Response Lifecycle

Notify/Address

- Notify
  - Notification (oversight authorities)
  - Notification (affected individuals)
- Address
  - Public announcements
  - Call centre/consumer response
  - Privacy complaint handling

Notification (Oversight Authorities)

- Privacy commissioners (provincial, federal, state, global)
- Professional or regulatory (e.g. health professionals, OSFI, IIROC, SEC, securities commissions, stock exchanges, etc.)
- Law enforcement (e.g. federal, global, anti-terror)
- Contractual obligations (especially for indemnification purposes) – review agreements
- Insurers

Privacy Commissioners

Federal (PIPEDA):

- Notification is voluntary…for now

Provincial:

- Alberta has mandatory notification (must notify AB privacy commissioner if personal information under organization's control is lost, accessed or disclosed without authorization, or if organization has suffered a breach where a "real risk of significant harm" to an individual exists as a result of the breach)
- Failure to notify the commissioner of a breach in those circumstances is an offence

United States:

- Most states have mandatory notification requirements

Notification (Affected Individuals)

- Method and manner
  - direct and/or indirect
  - method: letter vs email vs text vs…
- Timing and priorities
  - jurisdictional/time zone issues
  - can't just hit "send" on 75 million emails without breaking the Internet
- Identity theft and credit monitoring services
- Consider in context of other notifications/messages
- CASL compliance

Public Announcements

- Breach website
- Media releases
- FAQs
- Public company disclosure requirements

Call Centre/Consumer Response

- Call centres
  - Scripts
  - Training
  - Handling access/delete requests
- Protection Products
  - What (identity protection vs. credit monitoring)
  - How long? Eligibility restrictions?
  - Jurisdictional differences
- Compensation

Privacy Complaint Handling

- Affected individuals may contact company, or may go straight to privacy commissioners
- Managing multiple individual complaints
- Managing a commissioner-initiated investigation
- Cross border concerns

Contacts

Kirsten Thompson

Counsel and Co-Lead, National Cybersecurity, Privacy and Data Protection Group
(416) 601-7797
kthompson@mccarthy.ca

McCarthy Tétrault *Advance*™
Building Capabilities for Growth

Canada's New Data Breach Rules

Barry B. Sookman
McCarthy Tétrault LLP
bsookman@mccarthy.ca
416-601-7949

April 1, 2015

PIPEDA Amendments in S-4

- (*f*) require organizations to **notify certain individuals and organizations** of certain breaches of security safeguards that create a real risk of significant harm and to report them to the Privacy Commissioner;
- (*g*) require organizations to **keep and maintain a record of every breach of security safeguard**s involving personal information under their control;
- (*h*) **create offences** in relation to the contravention of certain obligations respecting breaches of security safeguards;

What breaches are in scope?

- "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.
- What is covered?

Remedies

- Individuals can file complaints with OPC for violations of any part of the new regime (s11(1)) which can lead to
  - Court applications by individuals for damages (s14(1))
  - Court making an order that the organization correct its practices in order to comply with the security breach regime (s16(a))
- Unprecedented new offenses with fines on organizations that knowingly contravene the obligations to notify the OPC or individuals or for failing to keep proper records. (s28)
  - on summary conviction a fine not exceeding $10,000; or
  - an indictable offence a fine not exceeding $100,000.

Notice to individuals

- 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;
  - **"significant harm"** is *deemed* to include 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;
  - the factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include
    - (a) the sensitivity of the personal information involved in the breach;
    - (b) the probability that the personal information has been, is being or will be misused; and
    - (c) any other prescribed factor.

Notice to individuals

- Notice must
  - be given as *soon as feasible* after the organization determines that the breach has occurred. S10(1)
  - provide enough information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm.
  - be conspicuous and be given *directly to the person*, except in prescribed circumstances
- Questions and implications
  - Over-reporting?
  - Inaccurate information?
  - Jurisdictional issues?

Notice to OPC and others

- 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
  - as soon as feasible after the organization determines that the breach has occurred.
- Notice must also be given to
  - any other organization or government institution
  - if the notifying organization believes that the other organization or the government may be able to reduce the risk of harm that could result from it or mitigate that harm
  - as soon as feasible after the organization determines that the breach has occurred.

Record keeping obligations

- 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.
- on request, provide the Commissioner with access to, or a copy of, a record.
- Problems:
  - Materiality?
  - Harm?
  - Who will be most penalized?

VANCOUVER

Suite 1300, 777 Dunsmuir Street
P.O. Box 10424, Pacific Centre
Vancouver BC V7Y 1K2
Tel: 604-643-7100
Fax: 604-643-7900
Toll-Free: 1-877-244-7711

CALGARY

Suite 3300, 421 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500
Fax: 403-260-3501
Toll-Free: 1-877-244-7711

TORONTO

Box 48, Suite 5300
Toronto Dominion Bank Tower
Toronto ON M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673
Toll-Free: 1-877-244-7711

MONTRÉAL

Suite 2500
1000 De La Gauchetière Street West
Montréal QC H3B 0A2
Tel: 514-397-4100
Fax: 514-875-6246
Toll-Free: 1-877-244-7711

QUÉBEC

Le Complexe St-Amable
1150, rue de Claire-Fontaine, 7e étage
Québec QC G1R 5G4
Tel: 418-521-3000
Fax: 418-521-3099
Toll-Free: 1-877-244-7711

UNITED KINGDOM & EUROPE

125 Old Broad Street, 26th Floor
London EC2N 1AR
UNITED KINGDOM
Tel: +44 (0)20 7489 5700
Fax: +44 (0)20 7489 5777

mccarthy tétrault