

Privacy Breaches: Are You Ready?

9th Annual Privacy and Security Conference
and Exposition

Presented by Cappone D'Angelo and
Jason Eamer-Goult

February 6, 2008

Who we are

- Jason Eamer-Goult,
Manager, Legislation and Privacy Policy
IM/IT Privacy and Legislation Branch
Ministry of Labour and Citizens' Services
- Cappone D'Angelo, Partner
Technology and Privacy Law
McCarthy Tétrault LLP
Barristers and Solicitors

Today's agenda

- Overview of the business context
- Overview of the legal context
- Responding to a breach
- Post-breach debrief and remediation
- Proactive Steps
- Case study exercises
- Questions

What is Privacy?

- Not defined in any privacy legislation in Canada
- Subjective and Context Sensitive
- Different types of privacy: physical, spatial, informational
- Personal information protection legislation deals only with informational privacy. It sets out rules that must be followed to achieve privacy

What is Personal Information?

- Personal information is [recorded] information about an identifiable individual
- Personal information includes but is not limited to:
 - name, address, telephone number
 - Race, national/ethnic origin, colour, religious or political beliefs or associations
 - age, sex, sexual orientation, marital status
 - identifying number or symbol
 - fingerprints, blood type, DNA prints
 - health care history
 - educational, financial, criminal, employment history
 - anyone else's opinions about individual and individual's personal views/opinions unless about someone else

Access and Privacy Legislation in Canada

Federal

- *Access to Information Act*
- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act (PIPEDA)*

British Columbia

- *Freedom of Information and Protection of Privacy Act (FOIPPA Act)*
- *Personal Information Protection Act (PIPA)*

Privacy Differs from Security

- Privacy is often confused with security
 - Security of personal information necessary to achieve privacy but is only one element
 - Privacy is both broader and narrower than security

Privacy Differs from Security

- “Privacy” is achieved by giving individuals “informational self determination” or control
 - Ensuring that individuals are able to control, to the greatest extent possible, how their information is collected, used and disclosed
 - If individuals can’t control, should at least be aware (with some exceptions)
 - Notice and consent, where necessary, are key

Case study

- Dr. Smith is a psychiatrist who assesses inmates in provincial facilities. Dr. Smith travels to different institutions to do the evaluations. Dr. Smith is a contracted service provider for a public body that is responsible for providing support services for citizens with criminal records.
- On the way to a facility, Dr. Smith stops for lunch at a restaurant. Dr. Smith's work laptop is stolen from the back seat of the car.
- Is this a privacy breach?

What is a privacy breach?

- A privacy breach is a collection of, use of, disclosure of, access to, disposal of, or storage of personal information, whether accidental or deliberate, that is not authorized by the applicable privacy statute.

How are things going?

10. Leaving a filing cabinet on the front lawn of a doctor's office, marked "For Sale", that still contains medical files.
9. Permit motor vehicle insurance records (containing detailed medical information) that were due for destruction to be used as props on a television show.
8. Using a real social insurance number for years in HR training slides and having the slides available for general viewing on the intranet.
7. Store your law firm's personal injury records, awaiting pick up for shredding, in an unlocked storage bin in a back alley, where they are videotaped blowing down the alley.
6. Put a national bank's unwiped hard drives, with detailed financial information on clients, up for sale on E-bay.

How are things going?

5. Post school children's psychological reports on the Internet and leave them there for months.
4. Permit a janitor to dispose of old hospital records by lighting a bonfire on a public beach, at the same time a ferry passes by, sending waves onto the beach that put out the fire and wash the half-burned records down the shoreline of B.C.
3. Hand over thousands of reports containing names, addresses, Social Security numbers, financial information and other details to fraud artists posing as officials in legitimate debt collection, insurance and cheque-cashing businesses.
2. Accidentally email an AIDS patient list, including their addresses, to more than 800 unauthorized recipients.
1. Use faulty IT security that leads to the theft of 46.6 million credit/debit numbers, with costs to the company approaching \$1 billion.

The cost of a privacy breach to an organization

- Hard costs
 - loss of current business
 - time and resources committed to breach
 - loss of assets, including data
 - financial exposure
 - risk to public health or public safety
 - resources committed to mitigation, repair, and damage control
 - regulatory scrutiny and penalties, contractual damages, possible lawsuits

The cost of a privacy breach to an organization

- Damage to reputation:
 - Bad publicity
 - Loss of trust / public confidence
 - Loss of prestige
 - Loss of future business

The cost of a privacy breach to an individual

- Risk of identity theft or fraud (usually if SIN, banking information, identification numbers, etc. have been compromised)
- Security risk or risk of physical harm (through stalking or harassment) or psychological harm (for example, by reopening closed issues)
- Risk of hurt, humiliation or damage to reputation (for example, through medical or disciplinary records)
- Loss of business or employment opportunities

Legal Context

- Express Legislative Reporting Obligations
 - *Ontario Personal Health Information Protection Act (PHIPA)*
 - foreign legislation
 - PIPEDA? BC and Alberta PIPA?

Legal Context

- Legislative Safeguarding Obligations
 - obligation to safeguard may include an obligation to report breaches in the appropriate circumstances
- Contractual Obligations
- Mitigation of Damages

Responding to a breach: Detection and Escalation

- **Detection**:
 - all employees of an organization should be trained to identify a breach
 - technological solutions
 - processes (including electronic and manual auditing)
- **Escalation**: all employees of an organization should know how (*i.e.*, to whom) to **escalate** once a breach is suspected

Responding to a breach: Initial Assessment and Containment

- Initial Assessment:
 - has there been a breach?
 - what personal information is involved?
 - has there been unauthorized use or disclosure of the information?
 - what is risk of further misuse?

Responding to a breach: Initial Assessment and Containment

- Containment
 - “stop doing that”
 - “disconnect that network connection”
 - “disable that ex-employee’s access”
 - “call the locksmith”
 - “request the return of the information”
 - “reminder that our policy is”

Responding to a breach: Notifying Regulator(s)

- which regulators have jurisdiction?
 - not always obvious, especially in BC and Alberta
- threshold for notification
 - legislative requirements
 - regulator may be able to provide advice on next steps (including whether to notify individuals)
 - sometimes a multi-party decision

Responding to a breach: Notifying law enforcement

- Police should be contacted when a theft or crime is suspected
- In some cases, police may request that other notifications be delayed so as not to impede the police investigation
- It might be appropriate to seek legal advice or to consult within your organization prior to contacting law enforcement

Responding to a breach: Notifying affected individuals

- Key consideration is whether notification is necessary to avoid or mitigate harm to an individual
- Consider if harm would come to a third party from the notification of the individual

Responding to a breach: Notifying affected individuals

- Other considerations:
 - Legislative requirements for notification
 - Contractual obligations require notification
 - The individual is at risk of identity theft or fraud
 - The individual is at risk of physical harm
 - The individual is at risk of hurt, humiliation or damage to reputation

Responding to a breach: Notifying affected individuals

- Notification should occur as soon as possible following the breach
- Notify individuals directly by phone, letter, or possibly email whenever possible
- Indirectly notify by website or newspaper notices, media, etc. when direct notice causes harm, contact information is not available

Responding to a breach: Providing breach notices

Breach notices should include:

- A description of the breach, including date and information compromised
 - Steps taken to mitigate the breach and next steps planned
 - Long term plans to prevent future breaches
 - Steps the individual can take to further mitigate the harm
- ...

Responding to a breach: Providing breach notices

Breach notices should include:

- Steps the organization can take to assist the individual in mitigating harm (context dependent)
 - paying for credit watch services
 - providing counselling services
 - paying other costs
- Contact information of someone who can answer questions or give further information
- That individuals can complain to the Office of the Information and Privacy Commissioner

Responding to a breach: Providing breach notices

Breach notices should **NOT** include:

- personal information about others
- information that could be used to circumvent security measures
- information that could prompt a misuse of the lost or stolen information
 - for example, if hardware was stolen for simple 'wiping and resale' but the breach notification prompts someone to realize that personal information is on the hardware and only then do they try to access the data

Responding to a breach: Informing other parties

- Communications office of your organization
- Organization's IT and/or physical security offices
- Insurers, lawyers, etc.
- Professional or other regulatory bodies
- Office of the Information and Privacy Commissioner:
 - Consider relevant factors in deciding to report to the Commissioner
 - Complete the Privacy Breach Notification Form on the Commissioner's website: <http://www.oipc.bc.ca/>
 - The OIPC may choose to do a further investigation. ²⁹

Case study

- The files on Dr. Smith's laptop contain the psychological assessments of offenders some of whom have significant psychological issues dealing with paranoia, as well as anger management. In some cases the files also contain information about the offences that could identify victims or other offenders.
- The laptop is password protected but the files are not encrypted.
- The laptop contains current files, and files from 2006 and 2007, that are backed up on his desktop at Dr. Smith's office.
- Who should or should not be notified? What information would you need to determine this?

Communications Issues

- Be proactive (both for internal and external communications)
- Ensure that relevant individuals are “in the loop” (internal and external)
- Staff, affiliates, unaffected customers, advisors and suppliers (including insurers), media
- Information sheet for anyone who may receive questions

Post-breach Debrief and Remediation

- Thoroughly investigate the cause of the breach:
 - Physical and technical security audits
 - How personal information is administered
- Develop a remediation plan to address deficiencies
- Examine policies and processes:
 - Are revisions necessary to reflect lessons learned from the breach and to prevent potential breaches?
 - After an appropriate period, review the effectiveness of the new policies and procedures
 - Develop long term standards and safeguards against further breaches

Post-breach Debrief and Remediation

- Assess the response to the breach
 - Did staff quickly recognize the breach and act/escalate commensurate to its seriousness?
 - Was the breach contained quickly and effectively?
 - Were harms mitigated to the greatest extent possible?
 - Were 1. affected individuals and 2. the public satisfied with how the organization dealt with the breach?
 - Were breach protocols properly followed?
 - What improvements can be made to the breach response process?

Case study

- Dr. Smith's boss is getting pressure from the public body that wants to know how this happened. What could have been done to avoid this breach?
- What role does the public body (in this case) as the contract holder have to ensure privacy breaches do not occur?

Proactive steps

- Articulate a **breach reporting policy** for your organization
 - **Regulatory regime**: what laws apply to your organization (and which **regulators** administer those laws)? Don't waste time doing this once a breach occurs – know the answers in advance.

Proactive steps

- **Breach reporting policy (con'd)**
 - **Notification**: what **criteria** will the organization consider in determining whether to notify and whom to notify - both general considerations that apply in all circumstances but also considerations specific to your organization (such as **contractual** obligations to notify)

Proactive Steps

- **Breach Reporting Policy (con'd)**
 - **Information Gathering Team**: which **individuals** will be involved in **gathering the relevant information** regarding the suspected breach?
 - **Decision Making Team**: which **individuals** will be involved in **assessing the breach** and **deciding whether to notify** individuals and or regulatory authorities (**CPO, legal counsel** (internal and/or external), other **sr. management, communications/marketing, IT** (if it's an IT issue), **HR** (if it relates to employees), **external advisors** (for example, to assess risk of unauthorized access)?

Proactive Steps

- **Breach Reporting Policy (con'd)**
 - **Process Checklist**: what is the **process for notifying individuals** and/or regulators (what order, what medium)?
 - **List of Resources**: keep a collection of resources – again, don't waste time doing this once a breach occurs.

Proactive Steps

- **Detection**: what processes are in place to ensure that breaches are detected?
 - having a clear policy (“**all employees must report breaches to CPO**”)
 - employee education
- **Escalation**: what processes are in place to ensure that breaches are escalated to the appropriate individuals

Proactive Steps

- **Security Policies**: ensure that your organization's security policies provide **appropriate safeguards** (including IT security policies)
 - the applicable legislation generally requires only that an organization implement appropriate safeguards, it generally does **not** require an "absolute guaranty of security"

Proactive Steps

- Security Policies (con'd)
 - even though a policy itself may not **prevent** breaches, it's better that the policy was **in place** and **adequate** (even if breached by an employee or circumvented by intruders)
 - increasing **guidance from Commissioners, industry** regarding what levels of security are appropriate, and organizations need to be aware of this guidance

Proactive Steps

- Compliance with Security Policies:
 - ensure that employees know which policies apply to them and their job duties
 - ensure that employees understand the applicable policies
 - ensure that employees comply with the applicable policies
 - ensure that business processes are compliant with the applicable policies

Proactive Steps

- ensure that retention policies are being followed
 - **deleting** personal information that is no longer required for the purposes for which it was collected
 - **scrubbing** electronic devices and media, **shredding** paper documents
 - **collecting/retaining** only the information that it is reasonable to retain
- ensuring that protections extend to service providers (including obligation to notify your organization of a **known, suspected, or anticipated** breach)

Case study

- The media and the public have raised concerns. The public body is considering terminating the contract. The OIPC is doing an investigation. What should be done to prevent future breaches?

Resources

B.C. Government

- **Privacy Helpline**
Email: CPIAADMIN@gov.bc.ca; Phone: (250) 356-1851
- **Privacy Breach Guidelines (under review)**
<http://www.lcs.gov.bc.ca/privacyaccess/>
- **The FOIPPA 'Policy and Procedures Manual'**
<http://www.mser.gov.bc.ca/privacyaccess/manual/toc.htm>
- **The Core Policy and Procedures Manual, Chapters 12 and 15, and Chapter 12 Supplemental**
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm and
<http://www.cio.gov.bc.ca/prgs/cpm12.pdf>
- **Information Security Policy**
<http://www.cio.gov.bc.ca/Security/ISP/>
- **The General Incident or Loss Report**
<http://www.min.fin.gov.bc.ca/pt/rmb/forms/0597FILL.pdf>

Resources

Office of the Information and Privacy Commissioner for British Columbia

- **'Key Steps in Responding to a Privacy Breach'**
[http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches_\(Dec_2006\).pdf](http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf)
- **'Privacy Breach Reporting Form'**
[http://www.oipcbc.org/forms/Privacy_Breach_Form_\(Dec_2006\).pdf](http://www.oipcbc.org/forms/Privacy_Breach_Form_(Dec_2006).pdf)
- **'Breach Notification Assessment Tool'**
http://www.oipcbc.org/pdfs/Policy/ipc_bc_ont_breach.pdf

Resources

- **Office of the Privacy Commissioner of Canada**
 - **'Key Steps for Organizations Responding to Privacy Breaches'**
http://www.privcom.gc.ca/information/guide/2007/gI_070_801_02_e.asp
 - **'Privacy Breach Checklist'**
http://www.privcom.gc.ca/information/guide/2007/gI_070_801_checklist_e.asp

Contact Us

- Jason Eamer-Goult
Manager, Legislation and Privacy Policy
IM/IT Privacy and Legislation Branch
Ministry of Labour and Citizens' Services
Telephone: (250) 387-6403
Email: jason.eamergoult@gov.bc.ca
- Cappone D'Angelo, Partner
Technology and Privacy Law
McCarthy Tétrault LLP
Barristers and Solicitors
Telephone: (604) 643-5906
Email: cdangelo@mccarthy.ca