

**From Panic to Practice:  
The Privacy Obligations of Information  
Technology Providers and Strategies for  
Effectively Addressing Them**

J. Fraser Mann and Bonnie Freedman

Presentation to the  
Toronto Computer Lawyers Group  
February 22, 2005

**2004  
Privacy Law  
Developments & Amendments**

**WASHINGTON, Oct 2001** – The **United States Department of Justice** maintains that The USA PATRIOT Act is “Preserving Life and Liberty” by “Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”

**VANCOUVER, Oct 2004** – The **B.C.** government passed a law aimed at preventing U.S. authorities from examining information about British Columbians held by private U.S. companies. Commissioner Loukidelis concludes the sweeping powers of the Patriot Act will triumph over any legislation approved in Canada.

**TORONTO, Nov 2004** - The **McGuinty government** passed legislation that protects the privacy of Ontarians' personal health information. Ontario will have the toughest regulations ever on how health information is used and protected according to Minister of Health and Long-Term Care, George Smitherman.

**Developments: Ontario**

- Nov '04 sees introduction of PHIPA = law protecting personal health information
- Imposes requirements on IT providers who sell to most health care providers (HICs)

**Ontario**

- Prohibitions & requirements apply respectively to providers of services that enable:
- 1 or more HICs to use electronic means to manage personal health information (“Providers”)
- 2 or more HICs to use electronic means to disclose phi to one another (“Network Providers”)

**Providers are prohibited from ...**

- Using phi accessed in the course of providing services (except as necessary to provide services)
- Disclosing phi accessed in the course of providing services
- Permitting employees or agents to access phi unless they are bound by restrictions

### In addition to being subject to the prohibitions ...

- Network Providers are required to:
  - Report incidents
  - Provide description of services & safeguards to HICs & public
  - Track & record access to/transfers of phi
  - Provide “threats, vulnerabilities & risks” assessment

### Network Provider Requirements

- Ensure that 3<sup>rd</sup> Ps comply with restrictions & conditions necessary for network provider compliance with PHIPA
- Have a written agreement with each HIC
  - □ □
- Some requirements entail changes to established industry practices

### Impact on Industry

- Threats, vulnerabilities & risk assessment
  - Cost, potential for security breaches
- 3<sup>rd</sup> Ps
  - Pushing down obligations & liability, compelling powerful vendors
    - Immunity - where good faith and reasonable exercise of duties
    - \$10,000 limit – damages for mental anguish

### Impact on Industry

- Written agreements
  - Requirement w/ all subcontractors
  - What was good practice is now a regulatory requirement

### Amendments: British Columbia

- USA PATRIOT Act amends Foreign Intelligence Surveillance Act (FISA)
- In response - BC amends Freedom of Information and Protection of Privacy Act (“FOIPPA” = public sector privacy law) in Oct ‘04

### Public Sector Service Providers

- Under amendments, prohibitions & requirements relating to personal information (“PI”) management apply to service providers, their employees, associates & subcontractors, to the extent they manage PI in the custody or under the control of prescribed public bodies (“Public Bodies”)

## Prohibitions & Requirements (Principal)

- **Storage & access of PI restricted to Canada**
  - Unless obtain consent or FOIPPA expressly permits disclosure outside of Canada
- **Permitted disclosure inside Canada**
  - Public Bodies & service providers may disclose PI in Canada
    - for purpose for which PI was obtained or consistent purpose
    - to comply with a subpoena, warrant or order issued in Canada

## Permitted Disclosure

- Public Bodies & their service providers may disclose PI inside or outside of Canada
  - with consent
  - where permitted or required by law of BC or Canada, arrangement or agreement made under such law, or treaty
  - to a Minister & the AG under defined circumstances
  - to collect a debt owed to BC gov't or a Public Body

## Reporting Foreign Demands

- Public Bodies & their service providers (& those providers' employees & associates), must report if they
  - receive a subpoena, warrant, order, demand or request from a foreign court, state or other authority for the disclosure of PI ("Foreign Demand")
  - receive a request for PI that they know or believe is in aid of responding to a Foreign Demand
  - have reason to suspect that unauthorized disclosure has occurred in response to a Foreign Demand

## Impact on Industry

- Practice was to require service providers and subcontractors to comply with all applicable law
- Now require compliance with applicable BC or Canadian laws only
  - Unintentional effect may be breach of foreign law

## Impact on Industry

- Feds & Alberta reviewing legislation and public sector outsourcing agreements – will they & other provinces follow BC?
- Some Public Bodies and their Service Providers going beyond requirements in FOIPPA in outsourcing agreements

## Offences

- Service providers & their employees or associates commit an offence where they
  - Store PI outside or allow access to PI from outside Canada
  - Fail to report a Foreign Demand for disclosure
  - Take action against a whistle-blower
  - Make an unauthorized disclosure

## Penalties

- Fine of up to \$25,000 where individual service provider (or partnership) commits offence & up to \$500,000 where corporate service provider
- Exercise of due diligence is a defence
- Service provider deemed to have committed an offence if holding PI in course of providing services & employee or associate commits an offence

## Implications of New Legal Requirements for Agreements with Information Technology Providers

## Analysis

Recommendations for custodians of personal information:

- Review agreements to determine whether on-side with new legal requirements and effect changes as required.
- Review any changes in policies and procedures regarding privacy, confidentiality and security with staff.

## Analysis

- Should examine the following areas:
  - Vendor Information
  - Access to Information
  - Removal/Storage of Information
  - Non-Disclosure and Restricted Use
  - Governing Law/Jurisdiction
  - Disclosure Permitted by Law
  - Return of Personal Information

## Analysis

- Audits and Reviews
- Cooperation
- Assignment
- Safeguards to Protect Personal Information
- Remedies

## Vendor Information

(Issues)

- Is the vendor a Canadian company?
- Does the vendor have offices in other countries?
- Does the vendor have any affiliates (including parents and subsidiaries) located outside of Canada?
- Does the Agreement permit the customer to require the vendor to remove or replace subcontractors?

## Vendor Information

(Provisions to Consider)

- *Customer reserves right to approve all vendor subcontractors (including affiliates).*
- *Subcontractors of the vendor (including affiliates) must be Canadian entities.*
- *Customer reserves right to approve vendor personnel in key positions (i.e., any person having potential access to personal information).*

## Access to Information

(Issues)

- Based on the nature of services being provided by the vendor, might the vendor obtain access to personal information held by customer?
- Is access required to enable the vendor to provide goods or services?
- Is it possible to segregate systems so that personal information is not accessible?

## Access to Information

(Issues)

- How will the vendor obtain access (through on-site services; remote access; reports)?
- Is it possible personal information may be accessed from outside Canada?
- Is the vendor required to track and log accesses and transfers of personal information?

## Access to Information

(Provisions to Consider)

- *Any information used by the vendor for non-production purposes (e.g., application testing, development or training) must be non-personally identifiable data.*
- *Any subcontractor access to information must be from a physical location within Canada.*

## Access to Information

(Provisions to Consider)

- *Vendor must require any authorized persons entering into secured premises to declare any devices in their possession that may be used to record/store any information.*
- *Vendor is required to prohibit such devices unless consent is obtained from customer or device is necessary to carry out duties.*

## Access to Information

(Provisions to Consider)

- *Vendor is required to prevent any US subcontractors from gaining access to the information, unless specifically approved in advance by the customer.*
- *Vendor is required to implement tools to trace and audit data access and copying.*

### Removal/Storage of Information (Issues)

- Is it necessary for the vendor to remove personal information from a customer's site for any reason (i.e., off-site storage)?
- What is the location to which personal information may be removed to?
- Is the vendor required to disclose the location(s) where it keeps personal information?

### Removal/Storage of Information (Provisions to Consider)

- *Any off-site storage by the vendor must be approved by the customer.*
- *No storage outside of Canada.*
- *Vendor must use security measures.*

### Flowing Down Restrictions (Issues)

- Is the vendor required to cause its employees, consultants, agents or other representatives to abide by the vendor's obligations?
- Is the vendor required to have written non-disclosure agreements with its representatives?
- Is the vendor required to cause its representatives to enter into non-disclosure agreements directly with the customer?

### Flowing Down Restrictions (Issues)

- Is the vendor required to provide the customer with reports and with any information, cooperation and assistance as reasonably requested by the customer?
- Do the reports and obligation to cooperate extend to information about services provided by vendor relevant to threats, vulnerabilities and risks of services provided by customers to its clients/end users?

### Flowing Down Restrictions (Provisions to Consider)

- *Vendor must cause all of its representatives to execute non-disclosure agreements directly with the customer.*
- *All non-disclosure agreements must be up-dated annually.*

### Flowing Down Restrictions (Provisions to Consider)

- *Vendor and its representatives are required to notify the customer of any actual or potential unauthorized accesses, uses or disclosures of personal information.*
- *Canadian vendor is prohibited from disclosing personal information to an affiliate.*

## Disclosure Permitted by Law

(Issues)

- Does the Agreement permit the disclosure of personal information when required by law?
- What is the scope of disclosure permitted under this provision?
- Is the vendor required to notify the customer of any subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for the disclosure of personal information?

## Disclosure Permitted by Law

(Provisions to Consider)

- *Vendor is required to acknowledge that it is solely subject to the laws of a province of Canada and Canada, and will take no steps to become subject to the laws or jurisdiction of the USA or another country.*
- *Acknowledgment by vendor that permitted disclosure means disclosure only under Canadian law.*

## Audits and Reviews

(Issues)

- Does the customer have a right to review or audit vendor's premises/systems/records?
- What is the purpose for which customer may carry out such review or audit?
- Is the customer permitted to use any subcontractor or other third party to exercise review or audit rights?
- Is the customer entitled to make copies of documents or other materials when conducting a review or audit?

## Audits and Reviews

(Provisions to Consider)

- *Customer will have the right to inspect and audit any systems and premises used to provide services and any records relating to the Agreement.*
- *Vendor must maintain all records relating to the Agreement in a particular location in Canada disclosed to the customer.*
- *Customer may use any third party to exercise its review and audit rights under the Agreement provided that such third party has agreed to comply with applicable confidentiality provisions.*

## Audits and Reviews

(by Vendor)

- When acting for a vendor, audit and review rights may be sought.

## Assignment

(Issues)

- Does the Agreement permit the vendor/customer to assign its rights and responsibilities to another party?

### Assignment

(Provisions to Consider)

- *Consent required to ensure no assignment to foreign affiliates.*

### Safeguards to Protect Personal Information

(Issues)

- To what extent does the customer require the vendor's personnel to undergo security screenings?
- Does the Agreement require the vendor to obtain all necessary consents from individuals for security screenings?

### Safeguards to Protect Personal Information

(Issues)

- Is the vendor required to comply with the customer's policies regarding confidentiality, security and privacy?
- Has the customer provided copies of its policies regarding confidentiality, security and privacy to the vendor?

### Safeguards to Protect Personal Information

(Provisions to Consider)

- *The vendor is required to provide the customer with a plain language description of its services and the safeguards that its uses to protect personal information.*
- *The vendor is required not to allow personnel to obtain access to the customer's systems/premises if results of background checks not acceptable.*

### Safeguards to Protect Personal Information

(Provisions to Consider)

- *The vendor is required to replace any of its representatives providing services to the customer if requested by the customer.*

### Remedies

(Issues)

- What remedies does the customer have available to it in the event of an unauthorized use, access or disclosure of personal information?

## Remedies

(Provisions to Consider)

- *Customer may terminate the Agreement and be entitled to recover damages in the event of unauthorized use, access or disclosure of personal information, or any breach of any other applicable provisions of the Agreement relating to personal information.*

## Other Possible Provisions

- *Customer will retain ownership and control over all records and personal information.*
- *Vendor will create a detailed privacy plan and conduct a Privacy Impact Assessment before making any changes to its systems/premises used to provide services.*
- *Vendor will be required to have a dedicated Privacy and Security Officer who oversees compliance.*

## Top 10

Provisions that May Be Over-Reaching

10. Requiring a vendor to provide a higher level of security for personal information than that provided by the customer.
9. Requiring a vendor to implement changes to services at any time to comply with new policies or directions imposed by customer, without recourse to change management process, or right to reimbursement of expenses to reflect new obligations.

## Top 10

Provisions that May Be Over-Reaching

8. Requiring the vendor to take any and all actions the customer deems necessary at any time to prevent any disclosures of personal information by the vendor.
7. Requiring the vendor to confirm compliance by customer of its policy obligations.

## Top 10

Provisions that May Be Over-Reaching

6. Requiring the vendor to provide absolute commitment that no security breaches will occur.
5. Requiring the vendor to provide the customer with a power of attorney which enables the customer to step-in in the event of an anticipatory breach.

## Top 10

Provisions that May Be Over-Reaching

4. Requiring the vendor's Privacy and Security Officer to take direction from the customer.
3. Requiring the vendor to ensure that no remote access is possible from outside Canada or by an unauthorized individual.

## Top 10

### Provisions that May Be Over-Reaching

2. Requiring the vendor to provide the customer with logs generated from any vendor Internet or e-mail activities.
1. Requiring the vendor not to comply with any foreign laws, or with orders or directives of any court or tribunal not having jurisdiction in a province, if such compliance would result in a breach of any obligations under the Agreement or under the laws of such province.