



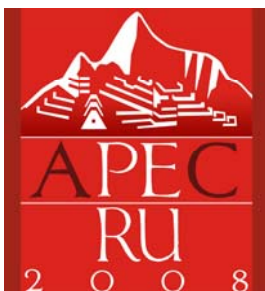
**Asia-Pacific  
Economic Cooperation**

---

**2008/SOM1/ECSG/SEM/014**

## **Outsourcing: A Citizen/Consumer Perspective**

Submitted by: University of Ottawa



**Technical Assistance Seminar on International  
Implementation of the APEC Privacy  
Framework  
Lima, Peru  
19-20 February 2008**



## Outsourcing: A Citizen/Consumer Perspective

Philippa Lawson, Director  
Canadian Internet Policy and Public Interest Clinic  
University of Ottawa, Faculty of Law  
Ottawa, Canada  
[www.cippic.ca](http://www.cippic.ca)

*Technical Assistance Seminar on International Implementation  
of the APEC Privacy Framework, 2008  
Lima, Peru  
Feb. 19 & 20, 2008*



uOttawa  
L'Université canadienne  
Canada's university



## Consumer Concerns

- vulnerability to unauthorized access
  - by ID thieves, fraudsters, org'd crime, disgruntled ee's
    - inadequate security
    - increased risk as a result of transfer
  - by foreign government agencies
    - foreign state surveillance activities
    - inadequate privacy laws
- secondary uses and disclosures
  - by foreign government agencies
  - by other businesses for their own purposes
    - inadequate privacy laws

## Protecting Outsourced Data



- From unauthorized access:
  - Minimize amount/type of data transferred
  - Minimize retention of data by vendor
  - Encrypt, anonymize or pseudonymize data
  - Ensure technical security safeguards
  - Ensure business process/employee safeguards
- From fraudulent use:
  - security breach notification
- From secondary uses/new purposes
  - ensure informed consent (or don't do it)
- From foreign government surveillance
  - avoid jurisdictions that lack due process guarantees

## Canadian Consumer Concerns



### National survey - March 2006

- Transfer of personal data across borders:
  - B2B (customer data)
  - G2B (citizen data – outsourcing to USA)
  - G2G (“to protect national security”)
- Questions:
  - How concerned would you be if...?
  - How important is it for you to be notified?
  - How important is it that the individual's consent be required (B2B transfers only)?

## Canadian Consumer Concerns



### CdnCo transfers customer data to ForeignCo:

- Level of concern:
  - 65% - high
  - 32% - moderate
  - 6% - low
- Customers should be notified:
  - 75% - very important
  - 5% - not important
- Customer consent should be required:
  - 84% - very important
  - 2% - not important

## Canadian Consumer Concerns



### CdnGov transfers customer data to ForeignCo:

- Level of concern:
  - 65% - high
  - 28% - moderate
  - 6% - low
- Customers should be notified:
  - 72% - very important
  - 6% - not important

## Canadian Consumer Concerns



CdnGov transfers customer data to ForeignGov  
“to protect national security”:

– Level of concern:

- 51% - high
- 36% - moderate
- 11% - low

– Customers should be notified:

- 70% - very important
- 8% - not important

## International Consumer Concerns



- 2006 International Survey
  - Canada, USA, Mexico, Brazil, France, Spain, Hungary
  - Ipsos-Reid, for Queen’s University Surveillance Project

Q: “Is it appropriate for companies to share or sell customer data with third parties such as:

– foreign governments?”

- 39%-53%: No (never)
- 19%-25%: Yes, with express consent
- 19%-27%: Yes, if customer suspected of wrongdoing
- 4%-12%: Yes, under all circumstances



## “Country Risk”

- Citizens/consumers don't want their data made available to foreign governments with less oversight/due process:
  - Cdn complaints to Privacy Commissioner:
    - bank, ISP outsourcing to USA
    - SWIFT
  - when given choice, many opt out of foreign outsourcing
    - Cdn security system provider
  - BC govt, Cdn census outsourcing issues



## Cdn. Legislative Response

- Some Cdn laws amended to “block” disclosures of citizen data to foreign govts without Cdn govt authorization:
  - if govt outsourcing to foreign-based vendor:
    - data must be housed in and accessed from Canada
    - no disclosure in response to foreign ct orders/subpoenas
    - notice of any such requests
    - substantial fines for non-compliance
    - whistleblower protection

## Responsibility of Outsourcers



- Canadian law:  
"An organization **is responsible** for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a **comparable level of protection** while the information is being processed by a third party."

## Responsibility of Outsourcers



### APEC IX. Accountability

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual **or** exercise due diligence and take reasonable steps to **ensure that the recipient person or organization will protect the information** consistently with these Principles.

## Comparison: Responsibility



- responsibility/due diligence obligation applies to all outsourcing orgs in Canada
- under APEC, outsourcing orgs may choose to rely on consent instead of taking responsibility for the data
  - meaningfulness of consent?

## Comparison: “Country Risk”



- PIPEDA:
  - requires “a comparable level of protection”; doesn’t exclude protection from foreign govt access under foreign laws
- APEC:
  - “in cases where disclosures are required by domestic law, the personal information controller would be relieved of any due diligence or consent obligations”

## Notice of Foreign Outsourcing



- Canadian law:
  - “An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.”
    - outsourcing orgs must notify customers of foreign outsourcing (but consent not required)
- Quebec privacy law:
  - data collector must inform individual of location where personal data is being kept
- APEC:
  - no notice of foreign outsourcing required

## Data Minimization



- Canada:
  - collect only what is necessary
  - retain only as long as necessary
- APEC:
  - collect only what is relevant
  - no rule limiting retention

## Breach Notification



- Security Breach Notification laws:
  - must notify affected individuals in case of security breach exposing personal data
    - most US states
    - being considered in Canada
    - arguably required under APEC “Preventing Harm” principle
- Dual purpose of law:
  - creates stronger incentives for effective security + data minimization (esp. if via public registry)
  - allows affected individuals to take mitigating action

## Consumer Risk Management



- Consumers should be able to select service providers based in part on exposure to foreign “country risk” + on record of data security
  - notice of foreign outsourcing
  - public notice of security breaches
- Consumers should be able to prevent ID fraud by taking action when their data is exposed
  - individual notice of data security breaches



## **Enforceability**

- Consumers should be able to enforce data privacy laws and commitments against:
  - (a) companies whose data processors fail to protect customer data, and/or
  - (b) data processors who fail to protect the data.
  
- Adequacy of trustmark schemes in providing consumer remedies?



**[www.cippic.ca](http://www.cippic.ca)**