

# Canada's Privacy Law Goes Abroad

**PIPA 2.0 Conference 2008  
November 18, 2008**

**Julio Arboleda Ramirez**

**With Special thanks to Curtis Marble and Scott Cedergren,  
both of BLG, for their research assistance**



**BORDEN  
LADNER  
GERVAIS**



# Why is this important?

## Legislation:

Alberta and British Columbia *Personal Information Protection Acts* (each a “PIPA”) – govern the collection, use and disclosure of personal information in those provinces

Federal *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) – Federal Legislation that governs the the collection, use and disclosure of personal information, and applies to:

- cross border flows of personal information;
- businesses in Provinces without substantially similar legislation; and
- Federal Works, Undertakings and Businesses (e.g. banks, airlines, interprovincial trucking) (a “FWUB”)



BORDEN  
LADNER  
GERVAIS



# But why really?

- ... **privacy in Canada is governed by the regulation of the collection, use and disclosure of personal information**
- ... **privacy is believed to be of sufficient importance that it has been deemed to be a human right**
- ... **and in the future, regulation of privacy may be the regulation of an important element of our identities**



BORDEN  
LADNER  
GERVAIS



## Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario in "Privacy in the Clouds"

***“Our digital footprints and shadows are being gathered together, bit by bit, megabyte by megabyte, terabyte by terabyte, into personas and profiles and avatars – virtual representations of us, in a hundred thousand simultaneous locations [...] At the same time, novel risks and threats are emerging [...] Identity fraud and theft are the diseases of the Information Age, along with new forms of discrimination and social engineering made possible by the surfeit of data.”***

**Dr. Cavoukian also raises the probability that as the internet develops and more applications are able to converse, concepts like reputation and identity on the internet will be transferable between applications and follow the user.**



BORDEN  
LADNER  
GERVAIS



# Incremental importance?

**I suggest to you that it is foreseeable that to the extent that individuals self - identities are informed by their interaction with their communities, including digital communities, digital personas and profiles may take on even more importance as both representative of, and a validation of, a person and their self identity.**



BORDEN  
LADNER  
GERVAIS



# What will we and won't we cover?

- **This presentation will use a case study to explore Canadian privacy legislation and how it follows personal information going abroad**
- **This will not explore public or health information legislation, as these are different topic areas**
- **We will cover some recent developments in private sector privacy law**



BORDEN  
LADNER  
GERVAIS



# Outline

1. **Case Study**
2. **Basic Jurisdiction Matters**
3. **Consent Provisions**
4. **Safeguards**
5. **Employees and Contractors**
6. **Extra-jurisdictional Reach**



BORDEN  
LADNER  
GERVAIS



# 1. Case Study – The Company

**A consumer transaction company, located in Alberta, with offices belonging to affiliates and subsidiaries in British Columbia, and Ontario. It has a small sales office in Europe.**

**The company contracts out certain data collection functions. It uses a call center in India.**



BORDEN  
LADNER  
GERVAIS



# 1. Case Study – The Information Collected

**In general, personal information is collected on:**

- ◆ Customers (products purchased, financial transaction information)
- ◆ Employees of the company (H.R. functions)
- ◆ Contractors of the company (background checks, sales performance)



BORDEN  
LADNER  
GERVAIS



# 1. Case Study - Where the information goes

- Information is transferred to the United States for employee (H.R.) management and financial transaction processing
- Sales information is collected from the EU
- Sales information is transferred to the EU for customer relations management and strategic analysis
- Information is transferred to India for processing and customer support



# 1. Case Study – This is about Personal Information

- For the rest of the presentation “information” refers to “personal information” as defined under the relevant legislation
- It is possible to “anonymize” personal information and remove it from the scope of privacy legislation – This can be a practical solution to data flow issues



BORDEN  
LADNER  
GERVAIS



## 2. Jurisdiction - Alberta

**Information collected, used and disclosed in Alberta by non FWUBs is subject to Alberta PIPA**

**Alberta PIPA does not apply to health information under the *Health Information Act*, to certain “not for profit” organizations, or to information subject to the public sector privacy legislation**



BORDEN  
LADNER  
GERVAIS



## **2. Jurisdiction – B.C.**

**Information collected, used and disclosed in B.C. by non FWUBs is subject to B.C. PIPA**

**B.C. PIPA does not apply to information subject to the public sector privacy legislation**



**BORDEN  
LADNER  
GERVAIS**



## 2. Jurisdiction – Incidental cross between B.C. and Alberta

Information that only crosses the provincial border “incidentally” may still only be subject to the PIPA of the disclosing province

- Does the substance of the transaction stay in the province? What is the customer’s perspective?
- If there is a contracting out, and the terms of the contract are clear that information is in the control of the discloser, then it is possible that the PIPA continues to apply.
- The B.C., Alberta and Federal Privacy Commissioners coordinate their activities



BORDEN  
LADNER  
GERVAIS



## 2. Jurisdiction - PIPEDA

- Information that crosses an international or provincial border is subject to PIPEDA
- Information collected, used and disclosed by FWUB's
- Includes outsource contracts on behalf of FWUB's
- Both the PIPAs and PIPEDA may apply, and it is necessary to know the specific flow of data



BORDEN  
LADNER  
GERVAIS



# 3. Consent

**Consent may be needed, but consider the variations:**

- **BC PIPA**
  - requires consent prior to collection, use and disclosure
  - requires notification of the individual that information will be collected
- **AB PIPA**
  - requires consent prior to collection, use and disclosure
  - also allows for deemed notice based consent
- **PIPEDA**
  - Specifies that consent may be opt-in or opt-out depending on the sensitivity of the information

**Note: Outsourcing may require additional consent**



BORDEN  
LADNER  
GERVAIS



### 3. Consent - However...

- In both Alberta and BC, there has been a consideration of requiring under PIPA that organizations notify individuals of international trans-border flows of their personal information
- The resulting recommendation from Alberta was to require notification
- In BC this recommendation was rejected, but the BC report instead recommended using contractual safeguards as in PIPEDA



BORDEN  
LADNER  
GERVAIS



### 3. Consent – anticipate flow and disclosure

- Anticipate where the information will go and who will receive it
- If it is going to the U.S. consider disclosure under PIPEDA that such information may be subject to US laws including the U.S. Patriot Act (*CIBC Decision*)
- If it is going for third party processing consider disclosure, especially if to a third country such as the US or India
- If management of H.R. information by US based affiliates consider disclosure (and safeguards – more later under employee matters)



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards – obligations on the home organization

- In each of PIPEDA, BC PIPA and AB PIPA, an organization remains responsible for the information that it collected after it is disclosed for processing
- See PIPEDA Schedule 1, s. 4.1.3, requirement to provide a comparable level of protection using contractual or other means (CIBC)



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards – obligations on the home organization

### BC PIPA s. 4(2):

- An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization.

### AB PIPA s. 5(1) and (2):

- (1) An organization is responsible for personal information that is in its custody or under its control; and
- (2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards – the future?

**Based on respective committee representations:**

- **Alberta PIPA might require merely notice when sending to a third party service provider**
- **BC PIPA might contain specific language indicating responsibility for information transferred to third parties, and require comparable protection**



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards - Information flowing to the U.S.

- **U.S. has sectoral privacy protection**
  - know your industry
  - May be quite sophisticated in certain areas e.g.:
    - ◆ Sarbanes Oxley security requirements
    - ◆ California financial sector regulation
    - ◆ FTC oversight
  - Alternatively, might be a void
  - Watch re-transmission of E.U. information



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards - Information flowing to India

- **For data processing and call center functions in case study**
- **A robust consideration of safeguards required**
  - What contractual mechanisms are available?
  - Background checks on parties and organizations
  - System checks and balances and audits
  - Remember if call center collects information need to ensure consents cover this



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards - Information flowing *into* Europe

- **Directive 95/46/EC does not create requirements for information flowing *into* the EC**
- **There are requirements for information *leaving* the EC**



BORDEN  
LADNER  
GERVAIS



## **4. Safeguards - Information flowing *out* of Europe – EU Law applies**

- **Information collected in Europe is subject to European Community requirements**
- **This should be discussed with European counsel, however there is a requirement that certain standard contractual clauses be used for countries not deemed to provide adequate protection.**



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards - Information flowing *out of Europe* - Countries deemed to provide an adequate level of privacy protection

- Switzerland
- Canada
- Argentina
- Guernsey
- Isle of Man
- US Department of Commerce Safe Harbour Privacy Principles
- Transfer of Name Record to the United States' Bureau of Customs and Border Protection



BORDEN  
LADNER  
GERVAIS



# 4. Safeguards - EU Form Contractual Requirements

- **Requirements include:**
  - Obligations of the data exporter include
    - ◆ Review of safeguards and security measures
    - ◆ For special categories of data, an obligation to notify subject of transfers to third countries
  - Obligations of the data importer include
    - ◆ Safeguards and security measures
    - ◆ Certification that national law does not prohibit compliance
    - ◆ Notice to exporter of disclosure requests and breaches
    - ◆ Grant an audit right
  - A termination clause, including obligations as to treatment of the data after data processing is complete



BORDEN  
LADNER  
GERVAIS



## 4. Safeguards – Other Possible Contractual Provisions

Such agreement could set out appropriate contractual safeguards to protect the Information, including:

- (i) restrictions with respect to the use of the Information by the processor;
- (ii) specifying a limited category of individuals within the processor's IT department who will have access to the Information (i.e. only those who need to have access to the Information for the purposes of carrying out the services under the agreement);
- (iii) a prohibition against transferring or disclosing the Information;
- (iv) a prohibition against subcontracting the services;
- (v) an obligation to return or destroy the Information upon termination of the contract;
- (vi) physical and/or technological security measures to be taken by the processors to protect against unauthorized access; and
- (vii) an obligation to notify the organization in the event of a privacy breach.



BORDEN  
LADNER  
GERVAIS



## 5. Employees and Contractors

- Despite being substantially similar, PIPA covers certain things differently, for example “employees”
- “employee” includes volunteers
- PIPEDA applies to employees of FWUBs
- PIPEDA does not apply to employees of provincial businesses
- PIPEDA arguably applies to contractors of provincial businesses



BORDEN  
LADNER  
GERVAIS



## 5. Employees and Contractors

- Is there a regulatory void for information about provincial employees?
- Consider employee's whose H.R. information is managed in the U.S. - U.S. H.R. department required to meet safeguards
- Does this mean that the Provincial commissioner should be able to investigate outside of Alberta where information about employees of provincial businesses are involved?  
We will return to this point when after discussing the *Abika* and *LSAC* cases.



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - *Abika*

**Provides the first instance of Canadian Privacy Law being *enforced* outside of Canada's borders**

- This case was a U.S. based data aggregator collecting data in Canada and selling it from the U.S. to Canadians
- The Privacy Commissioner, in her decision, declined to investigate
- The Federal Court *ordered* the investigation
- This means companies are on notice that the Commissioner must investigate



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - *Abika* – The Original Decision

**It was noted by the commissioner that it is unusual for legislation to allow for extra-territorial application**

- Normally, where extra jurisdictional application is to be permitted, the jurisdiction must be explicitly given. *PIPEDA* gives no such jurisdiction.
- The Commissioner, citing a lack of jurisdiction (but sympathising with the Plaintiff's case) said she would be unable to investigate.



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - *Abika* - The Federal Court's Robust Approach

- The Federal Court parted ways with the Commissioner, stating that there *was* authority for the Commissioner to investigate
- Authority came from the fact that the Commissioner's power was over the subject matter
- The Federal Court in somewhat strained reasoning held that this was not an extraterritorial application



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - LSAC

- In this case the Federal Commissioner held that she could require a US based organization to alter its practice and storage habits
- The *Abika* approach was followed in LSAC where the commissioner determined she could investigate based on a ‘real and substantial connection’



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - Inconsistencies?

In a different decision the Federal Court held that it did not have jurisdiction to issue a warrant to intercept communications in other countries.

Clear legislative intention is required to grant jurisdiction, and this cannot be implied.



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - Which path do we take?

### *Abika*

- Authority of the commissioner is over the *subject matter*
- The commissioner's authority is not being exercised extra-jurisdictionally because it is over subject matter, which remains in Canada.

### *CSIS*

- Legislation does not explicitly provide for extra-jurisdictional application
- The authority is *not* over the subject matter, but over territory or person
- Therefore: cannot legislate abroad



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - What this means at the Federal Level

- We have entered an era where companies should *expect* the attention of the Federal Commissioner if they are moving information across borders
- Companies need to be increasingly aware of how they handle personal information, especially where a Canadian subsidiary may be entrusting the information to a foreign parent



BORDEN  
LADNER  
GERVAIS



## 6. Extra jurisdictional reach - How does this compare at the Provincial Level?

### Provincial regimes are governed by provincial legislation

- Jurisdiction is over the subject matter
- Should a Provincial Privacy Commissioner be able to investigate when issues arise across borders?
  - ◆ What about an area where a Provincial Commissioner has jurisdiction, but the Federal Commissioner does not? Example: “Employees”?



BORDEN  
LADNER  
GERVAIS



# Conclusions:

- **There is a movement towards a more robust protection of personal information**
- **This movement has created a complex statutory system involving both federal and provincial legislation**
- **Questions of jurisdiction remain**



BORDEN  
LADNER  
GERVAIS



**Thank You!**

**Julio Arboleda, LL.B., LL.M**

**(403) 232-9601**

**[jarboleda@blgcanada.com](mailto:jarboleda@blgcanada.com)**



**BORDEN  
LADNER  
GERVAIS**

