Cross-Border Issues for Privacy Law Compliance in Canada, the US & the EU

- David M.W. Young
  Partner, Lang Michener LLP (Toronto)

- Simon Chester
  Partner, McMillan Binch LLP (Toronto)

- Evelyn L. Sullen
  Staff Counsel, Volkswagen of America Inc. (Auburn Hills, MI)

- David T.S. Fraser
  Associate, McInnes Cooper (Halifax)
Cross-Border Issues for Privacy Law Compliance in Canada, the US & the EU

David M.W. Young
Partner, Lang Michener LLP (Toronto)

Simon Chester
Partner, McMillan Binch LLP (Toronto)

Evelyn L. Sullen
Staff Counsel, Volkswagen of America Inc. (Auburn Hills, MI)

David T.S. Fraser
Associate, McInnes Cooper (Halifax)

Cash machines everywhere
Airline networks
E-mail ubiquitous
High density storage
Multinational businesses
Three Women
How European Courts are Protecting Privacy

Three Poster Women of European Privacy

Campbell v. MSN Papers
Europe Driving Privacy

- European Data Protection Directive
- Mandates action by member states
- By restricting data export
- Forces countries outside European Union
  - To legislate privacy protections
  - To follow European models
- Threat to stop data flow

Where is the call centre?

- Offers consumers 24/7 response
- Cheaper for business
- Enforcement may be problematic
  - Response – beef up security
  - Provide contractual assurance

Legislate adequate protection
The Threat of Data Export

- Blocking statutes have two thrusts
  - Extraterritorial norms
  - Regulation by foreign governmental entities
- Interference with business records
- Early privacy regulation focussed on dangers of data exports
  - Pre-internet world
  - Pre-micro storage at minimal cost
- Prompts European regulatory model
- GM’s Intranet Directory

Europe → United States

<table>
<thead>
<tr>
<th>European Union</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>More trust in private sector</td>
<td>More trust in private sector</td>
</tr>
<tr>
<td>Government will root out and control abuse</td>
<td>Mass media will expose/shame abuse</td>
</tr>
<tr>
<td>Compensatory laws preferable</td>
<td>Sector-specific laws where necessary</td>
</tr>
<tr>
<td>Self-regulation is equivalent to no regulation</td>
<td>Sector-specific laws where necessary</td>
</tr>
<tr>
<td>Broad rules with narrow exemptions</td>
<td>Technology can solve problems caused by technology</td>
</tr>
<tr>
<td>Overprotect consumers rather than under-protect</td>
<td>Empower consumers with information</td>
</tr>
</tbody>
</table>

Europe Moves

- 1995 European Union issued privacy directives
- Fundamental right to privacy with respect to the processing of personal data
  - Applies to public and private sector
  - Applies to automated and non-automated forms of data
  - Personal data defined as any information relating to identified or identifiable natural person
Europe Moves

Mandates certain minimum standards for the collection, disclosure, and transmission of personal data

Imposed condition on all E.U. states that transfer of personal information to a non-E.U. country is permitted only if country ensures an adequate level of protection.

Aims of European law

Legal basis
- Promote internal market
- Free flow of personal data (Art 95 Treaty)

Object
- Member States must protect fundamental rights and freedoms

Theory
- Harmonising national laws removes obstacles to free flow of information

Special rules
- Electronic communications (telecoms, internet, broadcasting)
- Restrictions on data being exported to other countries (if laws not adequate)

Enforcement
- Much of enforcement is behind the scenes
  - Fines e.g.:
    - €60,000 against Microsoft in Spain
    - Fines can reach €500,000
  - Injunctive relief
  - Government procurement sanctions
  - Enforcement likeliest in four areas:
    - HR data
    - Sensitive data
    - International data transfers
    - Marketing
Problems

- Lack of pan-European processes
- Need to deal with 25+ legal systems
- Application of data protection to international data transfers
- Lack of cooperation between regulators in different sectors
  - Over-reliance on bureaucratic procedures that do little to further privacy (e.g., notification)
  - Legal framework dating from pre-Internet age

Moving Data

- 8th Data Protection Principle
- Data transfers are acts of processing
- Transfers must take account of the rights of the Data Subject
- Transfers between European countries permitted
- Transfers outside Europe are qualified
- Some transfers to countries that do not provide adequate protection for interests of data subjects subject to derogations
  - Derogations in Schedule 4 include
    - Consent
    - Contractual necessity
    - Substantial public interest
    - Legal proceedings
    - Protect vital interests

Options for Transfers From EEA

- Adequate level of protection
- Established derogations
- EU Commission findings of adequacy
- Under EU Commission approved standard terms
- National Information Commissioner authorisation
- Under Information Commissioner approved terms
Options to Get Data from EU

- Legislative Adequacy Declaration
  - Certify Compliance with Safe Harbor if US company
- Data Transfer Agreement
  - Mandate US data importer to provide adequate protections (Article 26)
- Include approved contract terms
- Unambiguous Informed Consent
  - EU company may transfer data if it obtains unambiguous informed consent from every data subject before each transfer is made
- Binding Corporate Rules
  - Use of internal policy rules, procedures and mechanisms to ensure the rights of data subjects

Transborder Data Flows

- Exceptions from the requirement to provide an adequate level of data protection:
  - Unambiguous consent of the data subject
  - Transfer needed to perform contract between data subject and business
  - Data subject has made request and transfer needed for pre-contractual measures
  - Transfer needed to conclude or perform third party contract concluded in interest of data subject

Adequate Level of Protection Factors

- Nature of the data
- Country of origin
- Country of final destination
- Processing purposes
- Law in place in transferee country
- International obligations of transferee
- Relevant codes of conduct in transferee
- Security measures in force in transferee
EU Commission Findings of Adequacy

- Switzerland 2000/516/EC
- Hungary 2000/519/EC
- US Safe Harbor 2000/520/EC
- Canada 200/22/EC
- Argentina 30.06.03
- Guernsey

Options for global companies

- Obtain the consent to transfer to substandard countries from data subject
- Build into contracts and business specifications adequate safeguards to protect privacy
- Incorporate contractual clauses/model clauses
- Implement Codes of Conduct
- Treat privacy globally

Privacy in Canada

Follow European Trends?
U.S. Privacy Law Overview

OBJECTIVES

- U.S. Privacy Law Overview
- Volkswagen of America’s Cross-Border Issues
  - Compliance with PIPEDA
  - EU Directive – Safe Harbor

The Self-Regulatory Environment of the U.S.

- No comprehensive law protecting consumer privacy
  - 108th Congress - has introduced approximately 150 bills with privacy implications
- Privacy rights are derived from several sources:
  - Constitutional law
  - Common law
  - Federal statutes and regulations
  - State statutes and regulations
  - International law
**U.S. Privacy Law Overview**

### The FTC

- Federal Trade Commission
  - Created by the Federal Trade Commission Act of 1914
  - Monitors, investigates and prosecutes unfair trade practices
  - Authority to educate and work with businesses to bring them into compliance
  - Broader definition of Unfair Trade Practices

### The FTC

- Federal Trade Commission (cont’d)
  - Has become the “de facto” regulator of consumer privacy
  - First Bush administration gave authority to regulate commercial business practices on the internet
  - Investigative and prosecutorial powers continue to evolve
  - Monitors Internet website companies’ privacy policies and statements

### The FTC’s – 5 Fair Information Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Current Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice-Awareness</td>
<td>Companies collect personally identifiable information without notice</td>
</tr>
<tr>
<td>Choice-Consent</td>
<td>Consumers not given choice as to how personal information collected may be used</td>
</tr>
<tr>
<td>Access-Participation</td>
<td>Consumers have no specific right to access their files</td>
</tr>
<tr>
<td>Integrity-Security</td>
<td>No law requiring that reasonable steps be taken to assure accuracy, integrity or security of collected data</td>
</tr>
<tr>
<td>Enforcement-Redress</td>
<td>Protection through FTC Actions</td>
</tr>
</tbody>
</table>
### U.S. Privacy Law Overview

#### Anatomy of an FTC Action
- Company has a policy or procedure protecting consumer privacy
- Company fails to follow its own privacy policy
- A complaint is filed with the FTC
- FTC conducts investigation
- Redress
  - Consent orders
  - Settlement agreements
  - Fines
  - Bad press
- FTC issues administrative complaint or seeks injunction in federal court
- No private right of action or recovery for consumer

### U.S. Privacy Laws

- **Gramm-Leach-Bliley**
- **HIPAA**
- **COPPA**
- **FCRA**

### Financial Privacy

#### Gramm-Leach-Bliley Act (GLB)
- Enacted November 12, 1999
- Applicable to financial institutions
- Protects security and confidentiality of customers’ nonpublic personal information
- Financial Institutions must provide administrative, technical and physical safeguards
- Must provide initial privacy notice and annual thereafter
- Must offer customers opportunity to opt-out of certain nonaffiliated third party information sharing
- Allows affiliate information sharing
- States may enact laws offering greater protection than GLB
**Medical Information Privacy**

Health Insurance Portability & Accountability Act of 1996 (HIPAA)

- Regulates the use of personal information in the health care industry.
- Protects individually identifiable health information which is created or received by a health care provider, health plan or health care clearinghouse.
- Relates to:
  - Past, present or future mental or physical health or condition of an individual.
  - Health care provided to individual.
  - Payment for health care.

**Children's Privacy**

Children’s Online Privacy Protection Act (COPPA)

- The Act applies to operators of online services that are directed at or knowingly servicing children under 13 years of age.
- Makes it unlawful to collect personal information from a child under 13 without parental consent.
- COPPA only applies to entities that collect personal information online.
- FTC enforces COPPA.

Civil penalties for COPPA violations:

- Hershey Foods - $85,000
- Mrs. Fields Cookies - $100,000
- UMG Recordings - $400,000
### Volkswagen’s Compliance with PIPEDA

#### PIPEDA

**Steps Taken to Achieve Compliance**

- Appointed Chief Privacy Officer to monitor compliance
- Formed a Project Team to Implement Policies & Guidelines
- Notified All Canadian Customers Regarding Rights & Consent
- Created & Distributed Privacy Policy Brochures
- Contractually Obligated Third Parties
- Trained Front-Line Employees
- Implemented Measurements to Audit Compliance

#### PIPEDA

**Steps Taken to Achieve Compliance (cont’d)**

- Developing programs to extract customer information from databases to be provided to Canadian customers who ask: “What do you know about me?”
- Estimated costs to date: $500,000 and counting!
Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004

European Union Data Protection Directive – Safe Harbor

- Approved by the EU in July 2000, after negotiations between U.S. Department of Commerce and the European Commission
- An important way for U.S. Companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws
- Certifying to the Safe Harbor assures that EU organizations know that U.S. companies provide “adequate” privacy protection, as defined by the Directive

Safe Harbor

- Participation in Safe Harbor is voluntary
- Currently, there are approximately 550 companies on the Safe Harbor list
  - Of the companies certified, not all are current with their certification status
- Compliance Alternative – standard contractual clauses
- Currently, Volkswagen of America, Inc. is not on the Safe Harbor list

Is it working?
Safe Harbor

- The Safe Harbor provides a number of important benefits to U.S. and E.U. firms.
  - All 15 Member States of the EU will be bound by the European Commission’s finding of adequacy
  - Companies participating in the Safe Harbor are deemed adequate and data flows continue
  - Member State requirements for prior approval of data transfers either will be waived or approval automatically granted
  - Claims brought by European citizens against U.S. companies will be heard in the U.S. subject to limited exceptions (in theory)
- The Safe Harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive.

Questions?

Evelyn L. Sullen, Staff Attorney
Volkswagen of America, Inc.
Evelyn.Sullen@vw.com
(248) 754-5853

Thank You!
Private Sector Privacy Legislation – briefly!

- Federal
  - Personal Information Protection and Electronic Documents Act
- Quebec
  - Act respecting the protection of personal information in the private sector
- British Columbia
  - Personal Information Protection Act
- Alberta
  - Personal Information Protection Act
  - Health Information Act
- Ontario
  - Personal Health Information Protection Act (in force 1 Nov 04)
- Saskatchewan
  - Health Information Protection Act
- Manitoba
  - Personal Health Information Act

Privacy Principles

- Other than Quebec, all are based on the principles of the Canadian Standards Association Model Code for the Protection of Personal Information:
- Quebec’s is “substantially similar” to the principles.

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance
 CSA Model Code

• Rooted in the OECD Guidelines
• Requires (in short)
  – A privacy officer, internal/external accountability
  – Clear communication of purposes
  – Informed consent
  – Limited collection
  – Limited use, disclosure and retention
  – Right of access and requirement of accuracy
  – Safeguards for data

OECD Guidelines

• All Canadian private sector laws are based on the eight principles of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Information (1980)
  – Also federal public sector law – Privacy Act

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

OECD Guidelines were the basis for the European Data Protection Directive (1995), which requires “adequate” protection for European data in other jurisdictions
  – Not policed in the other jurisdiction ... export control
PIPEDA

• Silent regarding jurisdictional aspects, other than substantially similar provinces
  – Unclear in the text whether PIPEDA applies to PI moved from Alberta to BC.
  4. (1) This Part applies to every organization in respect of personal information that
     (a) the organization collects, uses or discloses in the course of commercial activities; or
     (b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

• No findings and no FCT authority.

Conflicts of laws

• Traditional bases of jurisdiction
  – Territorial Principle – A state has the jurisdiction to regulate individuals and subjects within its territory, including internal waters and airspace. This is the primary and most universal base for jurisdiction.
  – Nationality Principle – Civil law countries have traditionally asserted jurisdiction over their nationals, regardless of where they may be located.
  – Passive Personality Principle – States have assumed jurisdiction over crimes committed abroad against its nationals.
  – By Agreement – A country may, by agreement, grant another country jurisdiction over certain persons or subjects within its borders.

Conflict of Laws

• Canadian criminal law has been upheld when applied for cross border crime: Libman v R (telemarketing scam targeting US residents)
• LaForest J. applied the “real and substantial” connection test to uphold charges in Canada
• Notably commented:
  ¶77 … I also agree with the sentiments expressed by Lord Salmon in Director of Public Prosecutions v. Doot, supra, that we should not be indifferent to the protection of the public in other countries. In a shrinking world, we are all our brother’s keepers. In the criminal arena this is underlined by the international cooperative schemes that have been developed among national law enforcement bodies.
Conflict of Laws

- If territorial jurisdiction, PIPEDA may apply
  - **Collection** in Canada
  - **Use** in Canada
  - **Disclosure** in Canada
  - **Processing** in Canada
- If Canadian resident, PIPEDA may apply
- If Canadian company, PIPEDA may apply

When can PIPEDA apply?

<table>
<thead>
<tr>
<th></th>
<th>Canadian Resident</th>
<th>US Resident</th>
<th>EU Resident</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Canadian</strong></td>
<td>Territorial Jurisdiction</td>
<td>Territorial / Nationality Jurisdiction</td>
<td>Territorial / Nationality Jurisdiction</td>
</tr>
<tr>
<td><strong>US</strong></td>
<td>Territorial / Nationality Jurisdiction</td>
<td>Territorial / Passive Personality</td>
<td>Territorial / Passive Personality</td>
</tr>
<tr>
<td><strong>EU</strong></td>
<td>Territorial / Nationality Jurisdiction</td>
<td>Territorial / Passive Personality</td>
<td>Territorial / Passive Personality</td>
</tr>
</tbody>
</table>

Scenario

- CallCo, a US company, operates a call centre in Ontario through its Canadian subsidiary.
- US Bank ("Bank"), hires CallCo to sell its identity theft insurance to Bank’s account holders.
- All account holders are US residents.
- Does CallCo have to comply with PIPEDA?
- Does Bank have to comply with PIPEDA?
- Bonus questions:
  - Does CallCo have to comply with GLB?
Scenario (con’t)

• Does PIPEDA apply?
• Contacts with Canada?
  – Presence of call centre only
  – CallCo is US company
  – Bank is US company
  – Called customers are in the US
• Office of the privacy commissioner says ...
  – They have jurisdiction!
  – “PIPEDA is part of an international scheme for the (hopefully) seamless protection of personal information.”

Practical matters

• Who will complain?
• Who will know where to complain?
• Can the Privacy Commissioner reach you/your client?
• Can the Federal Court reach you/your client? (or assets?)
• Is the company merely an agent?
• Are appropriate agreements in place to ensure cooperation/compliance?
Cross-Border Issues for Privacy Law Compliance – Canada, the U.S. and the E.U.

**Canadian Bar Association Annual Legal Conference - 2004**

National Privacy Section

Cross-Border Issues for Privacy Law Compliance – Canada, the U.S. and the E.U.

Monday August 16, 2004

Speakers: Simon Chester, McMillan Binch LLP, Toronto

David Fraser, McInnes Cooper, Halifax

Evelyn Sullen, Volkswagen of America, Inc., Auburn Hills, Michigan

Moderator: David Young, Lang Michener LLP, Toronto

---

**Cross-Border Issues for Privacy Law Compliance**

Over-Arching Themes

1. What are the issues – transfer of data or simply cross-national compliance, or both?

2. Do privacy laws based on OECD models rest on outdated assumptions?

3. Options for aligning compliance.
Cross-Border Issues for Privacy Law Compliance

Discussion Topics
What are the issues facing multi-nationals as they try to align their privacy compliance procedures?
Do privacy laws based on OECD models rest on outdated assumptions?
What is the vision of the EU Privacy Directive? How is this playing in North America?
How is the U.S. responding to privacy issues internationally? How are U.S.-based companies responding?
What is the impact of the post–September 11 world (e.g. U.S. Patriot Act)?
What extra-territoriality issues arise and how do Canadian laws respond?

Outsourcing issues.
Approaches to meeting multiple norms.
How should Canadian companies respond to U.S., E.U. privacy regimes?
New developments in the E.U. and the U.S. What impact will they have (a) internationally; (b) on cross-border issues and (c) for Canadian privacy law?