



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)
- 



CBA National Privacy Law Section

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

CBA National Business Law Section



**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)



Small World

- ❖ Cash machines everywhere
- ❖ Airline networks
- ❖ E-mail ubiquitous
- ❖ High density storage
- ❖ Multinational businesses









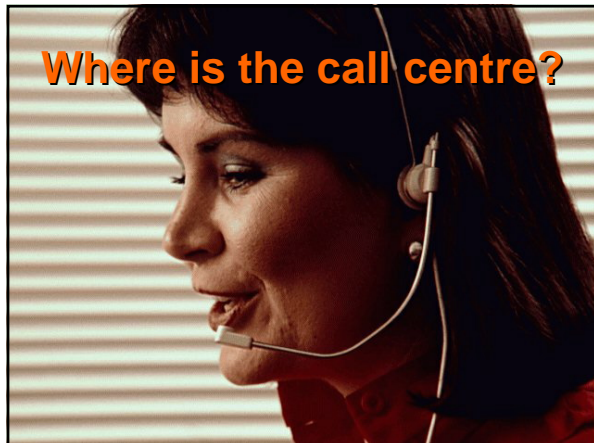




Europe Driving Privacy

- ❖ **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?



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

More trust in government	More trust in private sector / market solutions
Government will root out and control abuse	Mass media will expose/shame abuse
Comprehensive laws preferable – dedicated regulator	Sector – specific laws where necessary – use existing regulators
Self regulation is equivalent to no regulation	Regulation must pass cost benefit test
Broad rules with narrow exemptions	Technology can solve problems caused by technology
Overprotect consumers rather than under-protect	Empower consumers with information – let them choose



Europe Moves

- ❖ 1995 European Union issued privacy directive; in effect 25 October 1998
- ❖ "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 (telcoms, 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
 - €68,000 for spamming in Denmark
- ❖ 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
 - Notification of data processing
 - 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
 - ❖ Bans transfers to countries that do not provide adequate protections 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**
 - Bind the 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 force 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 2000/518/EC
- ✦ Hungary 2000/519/EC
- ✦ US Safe Harbor 2000/520/EC
- ✦ Canada 2002/2/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

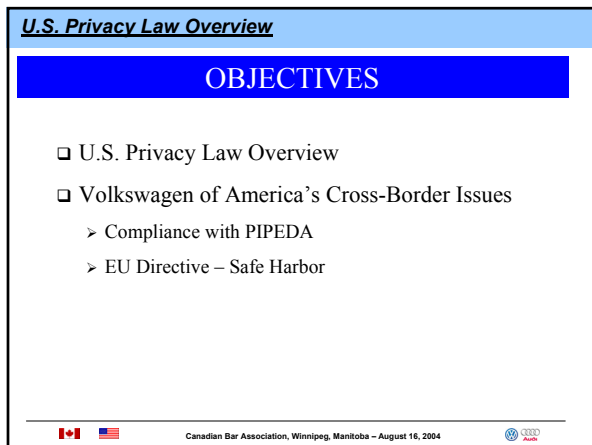
Follow European Trends?



U.S. Privacy Law Update

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

Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004

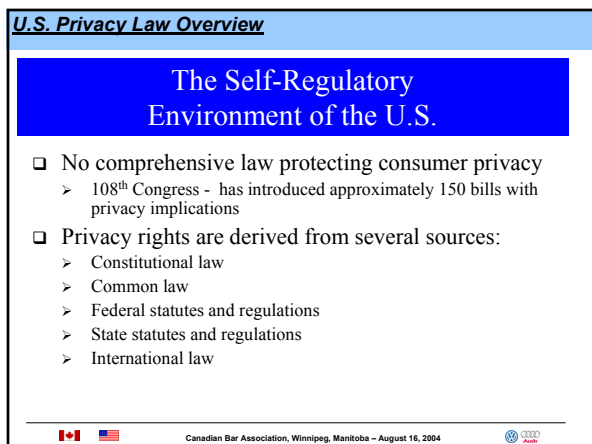


U.S. Privacy Law Overview

OBJECTIVES

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

Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004



U.S. Privacy Law Overview

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

Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004

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

Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004

U.S. Privacy Law Overview

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

Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004

The FTC’s – 5 Fair Information Principles

Principle	Current Practice
Notice-Awareness	Companies collect personally identifiable information without notice
Choice-Consent	Consumers not given choice as to how personal information collected may be used
Access-Participation	Consumers have no specific right to access their files
Integrity-Security	No law requiring that reasonable steps be taken to assure accuracy, integrity or security of collected data
Enforcement-Redress	Protection through FTC Actions

Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004

Evelyn Sullen, Volkswagen of America



Page 12 of 24

2

U.S. Privacy Law Overview

Anatomy of an FTC Action

- ☐ Company has a policy or procedure protecting consumer privacy
- ☐ Company fails to follow it's 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

 Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004 

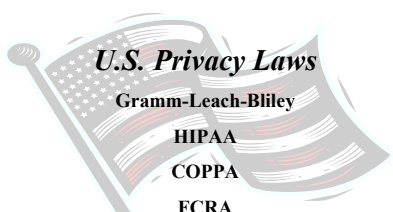
U.S. Privacy Laws



Gramm-Leach-Bliley

HIPAA

COPPA

FCRA





 Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004 

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

 Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004 

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


 Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004
 

Children's Privacy

Children's Online Privacy Protection Act (COPPA)

- ❑ Enacted October 21, 1998
- ❑ 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



 Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004
 



Children's Privacy

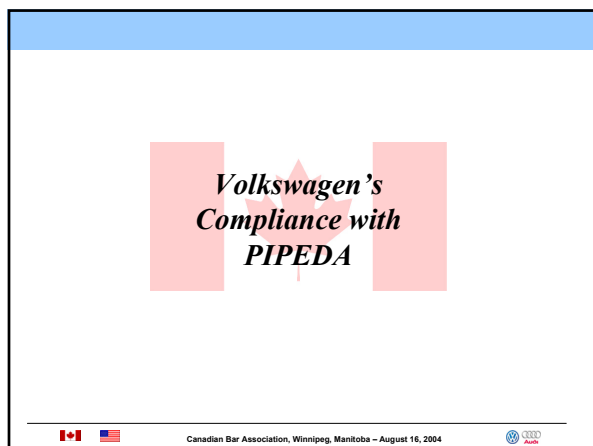
Children's Online Privacy Protection Act (COPPA)

Civil penalties for COPPA violations:

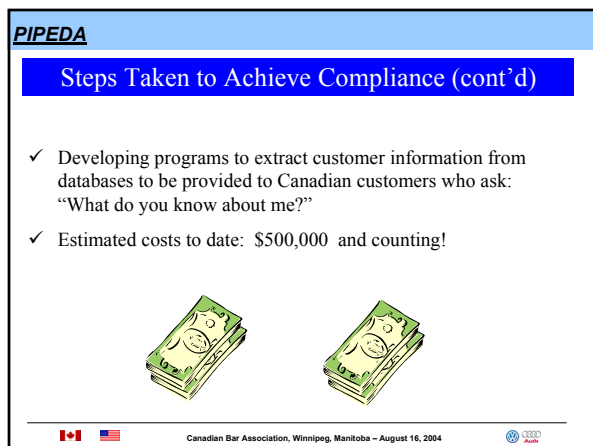
- ❑ Hershey Foods - \$85,000
- ❑ Mrs. Fields Cookies - \$100,000
- ❑ UMG Recordings - \$400,000





 Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004
 












***European Union Data
Protection Directive –
Safe Harbor***






Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004




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



Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004




Safe Harbor

Is it working?

- ❑ Participation in Safe Harbor is voluntary
- ❑ Currently, there are approximately 550 companies on the Safe Harbor list www.export.gov/safeharbor/
- ❑ 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







Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004



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.




Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004




Questions?

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

Thank You!


Canadian Bar Association, Winnipeg, Manitoba – August 16, 2004


Crossborder Privacy Law: The View from Canada

David T.S. Fraser
david.fraser@mcinnescooper.com
(902) 424-1347

Account #
Password

McINNES COOPER
BARRISTERS SOLICITORS & TRADE MARK AGENTS

NPSi

1

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

David T.S. Fraser
david.fraser@mcinnescooper.com

2

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

David T.S. Fraser
david.fraser@mcinnescooper.com

3

CSA Model Code

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

Account #

Password

David T.S. Fraser
david.fraser@mcinnescooper.com

4

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

Account #

Password

David T.S. Fraser
david.fraser@mcinnescooper.com

5

OECD Guidelines

- 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

Account #

Password

David T.S. Fraser
david.fraser@mcinnescooper.com

6

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.

David T.S. Fraser
david.fraser@mcinnescooper.com

7

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.

David T.S. Fraser
david.fraser@mcinnescooper.com

8

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:
 - ¶177 ... 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.

David T.S. Fraser
david.fraser@mcinnescooper.com

9

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

David T.S. Fraser
david.fraser@mcinnescooper.com

10

When can PIPEDA apply?

	Canadian Co.	US Co.	EU Co.
Canadian Resident	Territorial Jurisdiction	Territorial / Passive Personality	Territorial / Passive Personality
US Resident	Territorial / Nationality Jurisdiction		
EU Resident	Territorial / Nationality Jurisdiction		

David T.S. Fraser
david.fraser@mcinnescooper.com

11

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?

David T.S. Fraser
david.fraser@mcinnescooper.com

12

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.”

Account #

Payments

David T.S. Fraser
david.fraser@mcinnescooper.com

13

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?

Account #

Payments

David T.S. Fraser
david.fraser@mcinnescooper.com

14

Crossborder Privacy Law: The View from Canada

David T.S. Fraser
david.fraser@mcinnescooper.com

Account #

Payments

McINNES COOPER

BARRISTERS SOLICITORS & TRADE MARK AGENTS

NPSi

16

Canadian Bar Association Annual Legal Conference - 2004

National Privacy Section/National
Business Law 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.**

2

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?