CASSELS BROCK
LAWYERS

Bernice Karn and Cynthia Hill

Privacy Law

Tips for Keeping Your Company Out of the Headlines

March 6, 2008

Privacy Law

- Today's Agenda:
  - The Legislative Landscape
  - Managing Employee Personal Information
  - Dealing with Customer Information
  - Breach Response Strategy
  - Tips for Designing and Managing Effective Privacy Policies

Privacy Law

The Legislative Landscape

Privacy Law - The Legislative Landscape

- **Canada**
  - *Personal Information Protection and Electronic Documents Act* (Federal)
  - *Personal Information Protection Act* (Alberta, B.C.)
  - *An Act respecting the protection of personal information in the private sector* (Québec)

Privacy Law - The Legislative Landscape

- **The Ten Privacy Principles:**
  - Accountability
  - Identifying Purposes
  - Consent
  - Limiting Collection
  - Limiting Use, Disclosure & Retention
  - Accuracy
  - Safeguards
  - Openness
  - Individual Access
  - Challenging Compliance

Privacy Law - The Legislative Landscape

- **United States**
  - No single federal law governs general commercial collection, use and disclosure of personal information
  - Financial Sector Examples:
    - *Financial Modernization Act (Gramm-Leach-Bliley Act*)
    - *Right to Financial Privacy Act*
    - *Fair Credit Reporting Act*
    - *Fair and Accurate Credit Transaction Act*

Privacy Law - The Legislative Landscape

- United States, *continued*
  - *Examples in other sectors:*
    - *Health Care Portability and Accountability Act*
    - *Children's Online Privacy Protection Act*
  - FTC regulation of online practices
  - Regulation of Computers – Examples:
    - *Federal Information Security Management Act of 2002*
    - *Computer Fraud and Abuse Act*

Privacy Law - The Legislative Landscape

- Numerous state laws regulate various aspects of privacy, for example:
  - Arrest Records, Bank Records, Cable TV, Computer Crime, Credit, Criminal Justice, Gov't Data Banks, Employment, Insurance, Mailing Lists, Medical, Polygraphing, Privileges, School Records, Soc. Security Numbers, Tax Records, Telecom Services/Soliciting, Testing, Wiretaps

(Source - Compilation of State and Federal Privacy Laws (1997 ed.), by Robert Ellis Smith)

Privacy Law - The Legislative Landscape

- California has led the way with a comprehensive set of laws regulating the collection use and disclosure of personal information
- Examples:
  - *Online Privacy Protection Act* of 2003
  - *Financial Information Privacy Act*
  - "Shine the Light" – Civil Code sections 1798.83 – 1798.84
  - Data breach disclosure – Now Civil Code Sections 1798.29, 1798.82 and 1798.84

Privacy Law - The Legislative Landscape

- **European Union – Historical Development Milestones**

  *"**Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data**"* - issued by the Organisation for Economic Co-operation and Development in 1980.

Privacy Law - The Legislative Landscape

- **OECD Principles**:
  - Notice
  - Purpose
  - Consent
  - Security
  - Disclosure
  - Access
  - Accountability

Privacy Law - The Legislative Landscape

- ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*** – issued by the Council of Europe of 1981 *(Convention 108)* - January 28, 1981
- ***Directive 95/46/EC - The protection of personal data with regard to the processing of personal data and on the free movement of such data.*** - European Parliament and Council of the European Union - October 24, 1995

Privacy Law - The Legislative Landscape

- ***Directive 95/46/EC – Principles***
  - Protection of fundamental right to privacy of individuals and their right to privacy of processing of personal data
  - Goal of ensuring the free flow of data between member states

Privacy Law - The Legislative Landscape

- ***Directive 95/46/EC – Principles (cont'd)***
  - Personal data to be processed fairly and lawfully
  - Identification of specified, explicit and legitimate purposes
  - Data subject to provide consent to processing unless an exception applies

Privacy Law - The Legislative Landscape

- ***Directive 95/46/EC – Principles (cont'd)***
  - Personal data to be adequate, relevant and not excessive in relation to purposes for which they are collected/processed
  - Personal data to be accurate and up-to-date

Privacy Law - The Legislative Landscape

- ***Directive 95/46/EC – Principles (cont'd)***
  - Retention of personal data that permits identification of data subjects to be no longer than necessary for purposes for which they were collected or processed
  - Data subject's right of access and objection
  - Confidentiality and security of processing
  - Notification to national authority of processing

Privacy Law - The Legislative Landscape

- ***Data Transfer Issues***
  - Permitted Transfers
  - Countries regarded as safe
  - USA – “Safe Harbor” Program

Privacy Law - The Legislative Landscape

- ***Permitted Transfers from EU***
  - Consent
  - Contract performance
  - Substantial public interest/“vital” interests
  - Legal Claims
  - Terms Approved by the Commission (Standard Clauses)
  - Intra Corporate – Binding Corporate Rules
  - Data from public register

Privacy Law - The Legislative Landscape

- ***EU "approved" countries***
  - Argentina
  - Canada
  - Guernsey
  - Isle of Man
  - Switzerland

Privacy Law - The Legislative Landscape

- ***USA "Safe Harbor" Elements***
  - Public notice
  - Opt out
  - Opt in
  - Onward Transfer
  - Security
  - Data integrity
  - Access
  - Enforcement

Privacy Law - The Legislative Landscape

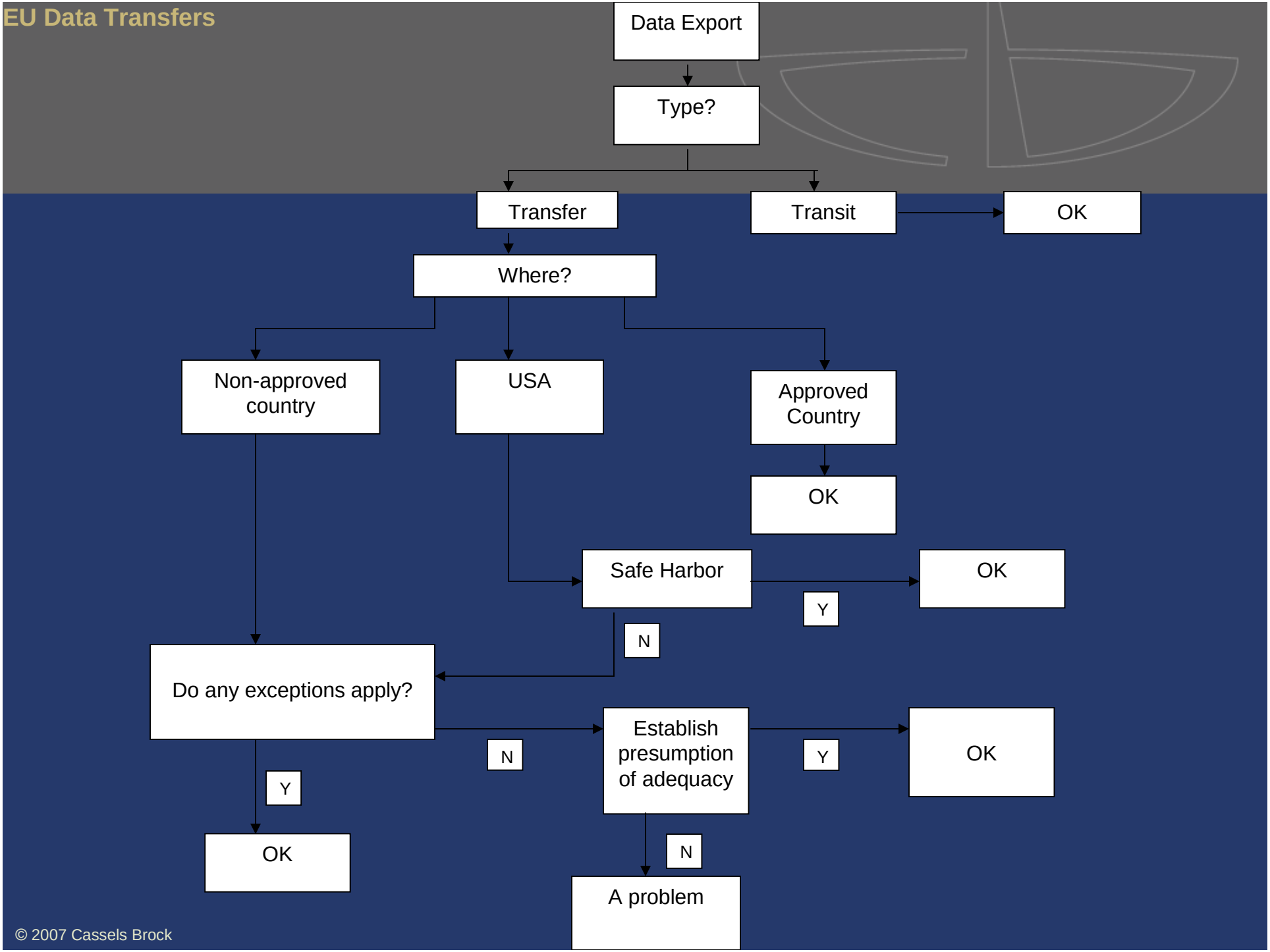
- ***Additional directives:***
  - Directive 2002/58/EC, July 12, 2002, concerning the treatment of personal data and privacy in the sector of electronic telecommunications;
  - Directive 2006/24/EC, March 15, 2006, requiring member states of the EU to pass into law an obligation for telecom providers to retain phone, email and web traffic data for up to two years;
  - Directive 96/9/EC, March 11, 1996, on the legal protection of databases.

Privacy Law - The Legislative Landscape

Examples of Other Countries

- Australia
- Mexico
- India
- China

EU Data Transfers



Privacy Law - Employee Information

Managing Employee Personal Information

Privacy Law - Employee Information

- Functional Areas
  - The hiring process
    - Who is involved
    - What data are collected
    - Uses of the data
    - References and background checks

Privacy Law - Employee Information

- Other Human Resources Functions
  - Employee Referral Programs
  - Organization charts and compensation
  - Payroll/Benefits
  - Performance Management
  - Training
  - Labour Relations

Privacy Law - Employee Information

- Other Human Resources Functions – *continued*
  - Occupational Health and Safety Issues
  - Security and Employee Monitoring
    - Video surveillance
    - Email surveillance

Privacy Law - Employee Information

- Provincial Laws
  - *Personal Information Protection Act* (Alberta, B.C.)
    - Different approach for employee personal information
  - *An Act respecting the protection of personal information in the private sector* (Québec)
    - General treatment
    - Section 20/Nominative lists

Privacy Law - Employee Information

- Trends in the case law
  - Collection of employee personal information - non-medical
  - Collection of employee personal information - medical
  - Withholding personal information from employees
  - Disclosure of employee personal information to others

Privacy Law - Employee Information

- Monitoring employees
- Use of employee personal information
- Denial of request to correct personal information

Privacy Law – Customer Information

Dealing with Customer Information

Privacy Law – Customer Information

- Types of data typically collected
- Channels of collection
- Uses of customer data
- Dealing with franchisees
- Typical disclosures

Privacy Law – Customer Information

- Trends in the cases
  - Proper vs. improper disclosures
  - Collection techniques and retention periods
  - Uses of customer information
  - Safeguarding customer information
  - Cross border transfers of customer information

Privacy Law

Breach Response Strategy

Privacy Law – Managing a Breach

- Preparation in Advance
  - Minimize amounts of PI collected
  - Minimize length of time retained
  - Keep a record of those systems that contain personal information
  - Classify PI in terms of sensitivity
    - Do any categories give rise to mandatory notification in any jurisdictions?

Privacy Law – Managing a Breach

- Preparation in Advance, *continued*
- Restrict access based on sensitivity of PI and need to know
  - Assign privileges to see certain categories of PI
  - Monitor access to highly sensitive PI
  - Terminated employees and contractors – remove privileges immediately

Privacy Law – Managing a Breach

- Preparation in Advance, *continued*
  - Rethink uses of laptops, PDAs, other portable storage devices
    - Restrict users and type of information that can be carried
    - Restrict downloading of certain sensitive data
    - Use of encryption on all sensitive data
  - Training and communications
    - Monitor compliance and make employees aware of monitoring
    - Include all employees, whether permanent, temporary or contract
    - Penalties for violation of policies

Privacy Law – Managing a Breach

- Preparation in Advance, *continued*
  - Service providers and other business partners – establish how they will handle your PI by contract
    - Audit and enforce this third party compliance
  - Use intrusion detection systems/“ethical hacking”
  - Use data encryption, access controls on systems
  - Dispose of records and equipment in a secure manner
  - Update security plan annually and any time when a material change in business practices occurs

Privacy Law – Managing a Breach

- Preparation in Advance, *continued*
  - Written policy for internal notification first
  - Appoint one person to co-ordinate internal notices
  - Train employees on response plan
    - Have 24/7 contact information available
    - Train employees in recognizing a breach and where to report it
  - Assign key roles to individuals

Privacy Law – Managing a Breach

- Preparation in Advance, *continued*
  - Prepare plans to contain, control and correct any security breach
  - Data custodian must be required to notify the data owner upon discovery of any incident that may involve a security breach
  - Prepare list of appropriate law enforcement officials that may have to be notified
    - Law enforcement may have additional suggestions

Privacy Law – Managing a Breach

- Preparation in Advance, *continued*
  - Ensure that your privacy policy has collected consent for use of e-mail to notify of data breach
  - Have a process in place for sending out notices
    - i.e., who writes it, format, means of transmission
  - Update notification plan annually and any time when a material change in business practices occurs

Privacy Law – Managing a Breach

- Quarantine/Containment
  - Activate response team – internal and external
  - What security systems were breached?
  - Was the incident isolated or systemic?
  - If the breach could be ongoing or repeated, what steps can be taken to stop it?
  - Preserve evidence

Privacy Law – Managing a Breach

- Risk Assessment
  - What type of information has been compromised?
  - Form of media compromised?
  - Extent of the problem?
  - Theft or loss?
  - Can or has the information be recovered?
  - What could happen with the compromised information?

Privacy Law – Managing a Breach

- Risk Assessment, *continued*
  - Risk, type and magnitude of harm to data subjects
  - Mitigation strategies for data subjects
  - Reputational risk to organization
  - Risks with credit card associations
  - Any contractual risks?

Privacy Law – Managing a Breach

- Deciding to notify
  - Has there actually been a breach?
    - Lost or stolen computer or other device with sensitive PI?
    - Unauthorized copying of PI?
    - Unauthorized person using information – e.g., fraudulent accounts/reported identity theft
  - Timing of Notice
    - Determine scope of breach first

Privacy Law – Managing a Breach

- Deciding to notify, *continued*
  - Check any statutory timing requirements in affected jurisdictions
  - If illegal activities involved, contact law enforcement
    - Advise law enforcement of your decision to notify and timing
    - If advised to wait by authorities – ask for notice as soon as the authorities give the OK and *be ready to notify*

Privacy Law – Managing a Breach

- Who to Notify?
  - Those individuals whose information was compromised
  - In some jurisdictions such as California, the compromise of only certain information triggers notice obligations
  - If individuals cannot be identified, notify relevant groups, if possible
  - Take care to limit notification only to individuals whose information was compromised – avoid “blanket” notifications
  - Document notification process for future reference, possibly for litigation

Privacy Law – Managing a Breach

- Who to notify - *continued*
  - Privacy Commissioner
  - Law Enforcement
  - Consumer credit reporting agencies
  - Insurers
  - Regulators
  - Third party contractors
  - Affiliates/business units
  - Employees/unions

Privacy Law – Managing a Breach

- Contents of notice
  - Keep it clear and simple
  - Describe breach and types of information compromised
  - List what has been done to protect the information from further compromise
  - Offer a toll free number for assistance
  - Provide information on how individuals can mitigate the problem in terms of their information – e.g., credit bureau notices
  - Provide contact information for relevant regulatory authorities such as the Federal Privacy Commissioner

Privacy Law – Managing a Breach

- How to notify
  - First class mail
  - E-mail, if consent obtained to use email for that purpose, and email is the usual means of communication
  - Some jurisdictions allow website/TV/radio/print media notification if the breach is large scale
  - Consider PR firm for drafting notice

Privacy Law – Managing a Breach

- Mopping Up
  - Conduct a post-mortem – what worked and what didn't
  - Track and resolve complaints from data subjects, other interested third parties
  - Incorporate learnings into updated response plan

Privacy Law - Policies

Tips for Designing and Managing Effective Privacy Policies

Privacy Law - Policies

- Developing a Policy
  - Basic Issues – understanding scope
    - Types of information collected?
    - What is personal information and what is not?
    - Jurisdictional – where do you need to comply?
      - Look at operations, sales, manufacturing, vendors, customers
    - Legislative requirements affecting information practices in various jurisdictions (unrelated to privacy)

Privacy Law - Policies

- Drilling Down
  - Who handles the information?
    - Internal groups
    - External groups
  - For what purposes?
  - To whom is it disclosed?
    - Intra enterprise
    - Extra enterprise
  - Purposes of disclosure?

Privacy Law - Policies

- Developing a data matrix
  - Catalogue who needs to see what and why
  - Classify each data category by sensitivity of the information
  - List the security precautions taken for each category
  - List the retention periods for each category
  - List the responsible business owner and support groups

Privacy Law - Policies

- Implementation
  - Communication of plan
  - Buy in – keep it simple and understandable
  - Amendment/rectification of information handling practices that are deficient
  - Supervision and Enforcement

Privacy Law - Policies

- Application
  - Needs to apply throughout the organization – i.e., to all controlled affiliates and their employees
  - Independent contractors such as service providers, consultants, agents, sales representatives and distributors must be required to agree to the policy as well

Privacy Law - Policies

- Supervision and Enforcement
  - Who has overall responsibility for the policy?
  - Who has day-to-day responsibility for implementation?
  - What is the relationship between these persons or departments and the functional units handling the information?
  - What other relationships need to be supervised?
    - Auditors, I.T. providers, outsourced service providers

Privacy Law - Policies

- Supervision and Enforcement – *continued*
  - Provide for periodic spot checks and audits
  - Prescribe process for reporting perceived violations
  - Outline steps to be taken to respond to a complaint or investigation by a Privacy Commissioner

Privacy Law - Policies

- Supervision and Enforcement – *continued*
  - Every new employee should receive a copy and acknowledge that they are required to comply
  - Refresh acknowledgement on a regular basis
  - Policy should provide that non-compliance can lead to termination of employment

Privacy Law - Policies

- Benefits of an enforceable policy
  - Uniform standard across the organization
  - Qualification as “binding corporate rules” for EU purposes (i.e., jurisdictions outside of Canada)
  - Driven by the company’s culture and processes (vs. a solution imposed by outside forces)
  - Likely easier to communicate to employees and contractors (rather than administering contractual rules or Safe Harbor compliance)
  - Makes compliance in EU easier - simpler approval process
  - Increases consumer confidence in organization

Privacy Law - Policies

- Difficulties in Implementing Privacy Policies
  - Ensuring consistency in application – especially where organization is world-wide
  - Weighing privacy risks vs. needs of the organization
  - Reputational risk of failure
  - Monitoring other applicable legislation worldwide and its effect on privacy policy/practices
  - Requires significant legal, I.T. and training efforts/cost
  - Obtaining EU approval for policy as binding corporate rules

Privacy Law - Policies

- Recommended Tools for Management
  - Business Unit Self-Audit Checklists
  - Lists of Privacy FAQs Using Practical Examples from the Business
  - Legal Requirements by Jurisdiction
  - Security Guidelines – Systems and personnel
  - Key Contacts
  - References to External Sites for Guidance

Privacy Law - Policies

- Key Success Factors
  - Create a strong compliance culture, with support from top management of the organization.
  - Think globally, but act locally for implementation, monitoring and management.
  - Have escalation structure up through the organization to higher management.
  - Follow the higher of policy standards or local laws.
  - Continual training of employees on privacy.

Privacy Law - Policies

- Key Success Factors – *continued*
  - Communicate privacy issues throughout the organization.
  - Periodic audits and inspections to ensure privacy commitments are met.

Privacy Law

THANK YOU FOR YOUR ATTENTION!

CASSELS BROCK
LAWYERS

www.casselsbrock.com

2100 Scotia Plaza, 40 King Street West, Toronto, Canada M5H 3C2 Phone 416 869 5300