Realities of Outsourcing:
12th in a Series of Webinar Presentations

Outsourcing and Data Protection & Privacy Implications

August 9, 2007

Cynthia O’Donoghue
Tower 42, Level 23, 25 Old Broad Street
London EC2N 1HQ UK.
tel: +44.(0)20.7847.9579
cynthia.odonoghue@pillsbrylaw.com

John Nicholson
2300 N Street, N.W.
Washington, DC 20037
tel: +1.202.663.8269
john.nicholson@pillsbrylaw.com
Global: Where are the privacy laws?

1. 27 EU member states

2. Other EEA countries e.g. Norway, Iceland

3. Non-EEA “adequate” countries e.g. Isle of Man, Guernsey, Switzerland, Canada, Argentina

4. Other countries for a future possible “adequacy” declaration e.g., Australia, Dubai, Hong Kong, Israel, New Zealand

5. Other countries with different types of laws e.g. USA, Taiwan and Russia
EU Data Protection Directive

- Prohibits transfer of personal data outside of EU unless there is "adequate protection" through one or more of the following:

1. “Model contract provisions”;

2. EU-US Safe Harbor Privacy Principles;

3. Binding corporate rules (“BCR’s”) that provide adequate protection;

4. Adequate jurisdictions: 27 EU member States, EEA countries (Norway, Iceland, Liechtenstein) and Switzerland, Canada and Argentina
EU Treaty

First Pillar: Community Domain

Second Pillar: Common Foreign & Security Policy

Third Pillar: Co-operation in the fields of Justice & Home Affairs

The PNR Case
“Any information…”
– content, nature, format

“…relating to….”
– content, purpose, result

“…an identified or identifiable…”
– singling out, reasonable means

“…natural person”
– living individual, business data
The most efficient way to prove “adequate protection” for hosting EU data by the US entity may be by certifying to the Safe Harbor Principles:

- Self-regulatory privacy framework requiring public declaration of adherence to 7 privacy principles:

1. notice (client knows use and purpose of data collection);
2. fair processing (client decides whether and how data will be used and disclosed);
3. access (client can access data to correct it);
4. security (take reasonable steps to protect data);
5. enforcement (service contract assures compliance FTC & DOT have enforcement powers);
6. onward transfer (once in US, data are disclosed to 3rd parties based on client’s notice and choice referenced above and/or confidentiality); and
7. data integrity (reasonable steps taken to maintain data for their intended use).
The BCR provide:

- criteria for processing of data by all group companies worldwide (including intra-group transfers)
- processing criteria based on EU Data Protection Directive
- “safe haven” within company group
- specific safeguards for transfer of data to third parties outside EEA
- complimentary character: NOT: minimum level
  - local law and rights & remedies apply
  - stricter BCR requirements prevail
WP 74 requirements ("inspired" by EU model contracts)

- "binding"
  - internally (compliance)
  - externally (unilateral declaration or contract)
  - data subjects: third party beneficiaries
- "without prejudice" to local rights & remedies
- duty to co-operate with DPAs of all group companies
- jurisdiction/joint & several liability
  - EU exporting group company or
  - EU headquarters
- EU co-ordinated procedure: one lead DPA
Model Clauses inadequate for inter-company data transfers

- Standard contractual clauses that may not be varied
- numerous contracts, numerous permits
- require description data transfers:
  - categories data subjects
  - data transferred
  - recipients of data
  - purpose of transfer
- significant changes require:
  - entering into new Model Contracts
  - new permits
- new notifications
- false sense of compliance
  - compliance on paper
  - no material compliance
Personal data transferred:
- employee data:
  - service history
  - performance appraisals
  - sensitive personal data, e.g. sickness absence records
- customer data

Data security is major concern in outsourcing
The Outsourcing Agreement: Defining Data Rights and Obligations

Why?

- Contract must cover DP compliance obligations/principles
- 7th principle states if Data processor is processing on behalf of a Data Controller:
  - Must use a “written” contract
  - Data Processor is to act only on Data Controller’s instructions
  - Data Processor is required to comply with 7th principle -- “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"
- Ensure “flow-down” to Data Processor
- Protections and remedies
Controllers and processors

- Will the service provider be a data controller or only a processor?
- Data controllers determine:
  - the purposes for which and
  - the manner in which
    personal data are, or are to be, processed
- If data remain under the control of an EEA person, regulatory issues will be less severe
Security obligations

- “X is the controller, Y is the processor” – are you sure?
  
  *The Swift Case*

- Compliance with instructions [consistent with agreement?]
- Appropriate security obligations [identified where?]
- Other restrictions? No further use, assistance with subject access requests, regulatory complaints etc
- Other evidential/accessibility requirements?
“Relying on consent may….prove to be a false good solution”

“The importance of consent constituting a positive act excludes….any system whereby the data subject would have the right to oppose the transfer only after it has taken place”

“Specific difficulties might occur to qualify a data subject’s consent as freely given in an employment context, due to the relationship of subordination between employer and employee. Valid consent in such a context means that the employee must have a real opportunity to withhold his consent without suffering any harm, or to withdraw it subsequently if he changes his mind”

Is the insistence on no detriment correct?
In March the ICO found 11 banks in breach of the DPA after investigating complaints about the disposal of personal information discarded in waste bins outside their premises.

- ICO has obtained formal undertakings to comply with DPA requirements.

Penalties getting stronger:
- Spain
- France
- Czech Republic
- United Kingdom – pending legislation
North American Privacy Framework

“It is not easy to describe the present position of legal opinion on [privacy law in North America]. Only a poet can capture the essence of chaos.”

– R.H. Coase

- Canada
- US Federal Laws/Regulations
- US State Laws
- Questions
Canadian Privacy Law

- Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Enacted in 2000
  - Defines personal information very broadly (although not as broadly as EU)
  - Embodies 10 “privacy principles”:
    - Accountability
    - Identified Purpose
    - Consent
    - Limited Collection
    - Limited Use, Disclosure
    - Accurate, Complete and Up-to-Date
    - Safeguard
    - Transparency
    - Access
    - Challengeable Compliance

- Accountability principle means that businesses remain accountable for whatever information they transfer to a service provider and for the actions of the service provider.

- Implications for Outsourcing
  - Companies obtaining personal information about Canadian residents should include provisions protecting against vicarious violation of applicable data privacy laws.
**Canadian Privacy Law – The Wrinkle**

- PIPEDA applies in a Canadian province **unless** that province has passed a data protection law that is substantially similar to PIPEDA.

- 3 provinces have passed laws that have been deemed substantially similar to PIPEDA, so in those provinces, those laws apply instead of PIPEDA: Alberta, British Colombia and Quebec.

<table>
<thead>
<tr>
<th>Public vs. Non-Public Information</th>
<th>PIPEDA</th>
<th>Province Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice and Consent</td>
<td>Notice of purpose for collecting information, generally, must be provided. Consent must be obtained (but can be implied, opt-out or opt-in).</td>
<td>Quebec/Brit. Col. – Consent from employees not required, but must receive notice re: purposes of disclosure/use of personal info. Quebec: Establishing file on individual requires notice of (1) object of each piece of info in the file; (2) use of info; (3) categories of persons with access to info; (4) location where kept; and (5) individuals’ rights of access and rectification.</td>
</tr>
<tr>
<td></td>
<td>No distinction. Publicly available info must be used for the purpose the info was made public.</td>
<td>Quebec only protects info that relates to a natural person and allows that person to be identified.</td>
</tr>
</tbody>
</table>
U.S. Federal Laws

- U.S. position is philosophically different from EU.
- Only those things that can actually be demonstrated to cause harm to the individual are regulated.
- U.S. takes a sector-based approach to privacy protection. Only specific, sensitive information is regulated:
  - Financial (Gramm-Leach-Bliley Act, Fair Credit Reporting Act)
  - Medical (Health Insurance Portability and Accountability Act)
  - Children (Children’s Online Privacy Protection Act, Federal Educational Records Privacy Act)
  - Other sector specific regulation (Telecom Act, Video Privacy Protection Act, Drivers License Protection Act, Do-Not-Call Implementation Act, etc.)
- Sarbanes-Oxley requires information security/assurance.
- U.S. Federal Trade Commission enforces companies’ compliance with their own privacy policies and requires companies to provide a minimum level of security.
Gramm-Leach-Bliley (GLBA)

- Requires “financial institutions” to protect security and confidentiality of customers’ non-public financial information.
- Authorizes various agencies to coordinate development of regulations: Comptroller of the Currency, SEC, FDIC, FTC, etc.
- Requires annual notice of privacy policy and practices.
- Financial institutions subject to additional “guidance” from FDIC and other regulatory bodies

Implications for outsourcing:

- Financial institutions must include relevant protections in the outsourcing agreement, including compliance with relevant privacy and security policies.
- Tier 1 outsourcing suppliers frequently have security practices that are superior and more consistently applied than individual companies; however, an outsourcing customer must do appropriate due diligence to confirm this.
- May require expanded audit provisions to enable financial regulators to inspect supplier facilities.
Health Insurance Portability and Accountability Act (HIPAA)

- Requires health care entities to:
  - implement new privacy policies
  - comply with technical security requirements
  - provide notice/secure authorizations for a range of uses and disclosures of health information, and
  - enter into written agreements with business partners regarding the ability to share such information.

Covered Entities must regularly review and update documentation.

- HIPAA security regulations:
  - Fall into three categories: Administrative, Physical, Technical
  - Each category includes:
    - “standards”: WHAT the organization must do; and
    - “implementation specifications”: HOW it must be done.

Implications for Outsourcing

- Certain types of outsourcing (HRO, claims processing) may require compliance with HIPAA obligations and execution of Business Associate Agreement.
Children’s Online Privacy Protection Act (COPPA)

- Who is covered:
  - The "operator" of a commercial web site or online service "directed to children under 13" that collects "personal information" from children; and
  - The "operator" of a general audience web site who has "actual knowledge" that it is collecting "personal information" from children under 13.

- Requirements:
  - Site “directed to children” - must be a link to privacy policy on the home page and at each area where the site collects personal information from children.
  - “General audience” site with a separate area directed to children - must be a link to privacy policy on the home page of the children's area.
  - Must obtain parental consent for collection/use of children’s information.
  - Must notify parents of any change to usage/disclosure practices.
  - Verified parents must be able to review data collected about their children upon request and can revoke consent/request deletion of information at any time.

- Failure to comply can result in fines of $10,000 per violation.

Implications for Outsourcing

- Contractual provisions must require compliance with relevant privacy policy and enable compliance with COPPA.
- Contractual provisions should provide indemnification for failure.
In the absence of comprehensive federal privacy legislation, various U.S. states are passing privacy laws.

California has led the way

- AB 1950 - Requires a business that:
  - Stores personal information about a California resident to implement reasonable security procedures and practices appropriate to the nature of the information to protect it from unauthorized access, destruction, modification, use or disclosure.
  - Discloses personal information about a California resident to a 3rd party as part of a contract to require the 3rd party to implement and maintain the same reasonable security procedures and practices appropriate to the nature of the information to protect it from unauthorized access, destruction, modification, use or disclosure.
- SB 27 “Shine the Light” law – governs disclosure of information to a 3rd party where discloser knows that 3rd party will use information for marketing.
- CA Online Privacy Protection Act - operator of a commercial web site or an online service is required to conspicuously post a privacy policy containing specific information on its web site, and comply with the terms of that policy

Implications for outsourcing agreements

- Companies who outsource must understand implications of state laws and include relevant contractual provisions.
U.S. State Laws – Data Breach Notification

- Require certain organizations suffering a data breach of certain types of personal information to notify the individuals whose information was accessed under certain circumstances.

- 37 states, District of Columbia, Puerto Rico

- State laws have varying requirements and definitions
  - “Trigger” for action can be knowledge-based or “risk”-based
    - Knowledge-based
    - Risk-based (information materially compromised or likelihood of harm required)
    - May apply to corporations, state agencies, or both
    - May exempt HIPAA, GLBA or entities subject to similar state laws
    - May tie to Interagency Guidelines (issued under GLBA) or other guidance
  - May apply to entities only within the state, or may apply to any entity with data about citizens of that state
  - May exempt entities from notice requirements if entity has its own notification procedures.
    - >25 states have some level of exemption
U.S. State Laws – Data Breach Notification

- Personal information not uniformly defined.
  - Montana: Only SSN is considered personal information.
  - Arkansas: Includes medical information combined with a name.
  - Georgia: Any password or other identifier that permits access to an account without the name as personal information.
- Notification periods after discovery not uniform, nor are the exceptions for delaying notice (e.g., for internal investigation, corrective action or to assist law enforcement). Some require “immediate” notification; others require “prompt” or “timely” notice.
  - Florida includes stiff penalties for a failure to give notice within the prescribed period.

Implications for Outsourcing

- Varying state requirements mean that companies should include requirements that a service provider will notify them of a data breach, regardless of circumstances.
- Companies should try to include indemnification for costs resulting from a data breach
  - Limitation on circumstances may be negotiated – negligence vs. strict liability
- Failure to comply with service provider’s own security policy may be a material breach of agreement.
Data Breach – Minnesota

Dec. 18, 2006: TJX discovers intruders hacked into their computer system illegally accessing customer data of approximately 45.6 million customers.

Stolen data covered half to all transactions U.S., Puerto Rico and Canadian stores. Customer information also stolen from transactions occurring in the U.K. and Ireland.

Aug. 1, 2007: Plastic Card Security Act goes into effect in Minnesota:

- Any entity that receives payment card (credit/debit card) information from a Minnesota customer may not retain card security code data, the PIN verification code number, or the full contents of the magnetic stripe data after a transaction is authorized. Security information for debit card transactions may be retained for 48 hours.

- If an entity or any of that entity’s service providers suffers a data breach and either the entity or the service provider has violated these retention restrictions, that entity is strictly liable to financial institutions for the costs to remediate and recover from the breach including:
  - cancellation or reissuance of access devices,
  - closure of accounts and stop payment transactions,
  - opening/reopening of accounts affected by breach,
  - any refund or credit for unauthorized transactions resulting from the breach,
  - notification of cardholders affected by breach
Like California’s initial approach to security breach notifications, companies doing business with Minnesota customers are subject to the Minnesota law.

Implications for Outsourcing

- Any entity subject to the Minnesota law should include requirements for compliance with the data security restrictions.
- The contract should include an indemnification for costs resulting from a service provider data breach where the service provider failed to comply with the requirements.
<table>
<thead>
<tr>
<th>Relevant Statute(s)</th>
<th>United States</th>
<th>Canada</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>State/Province Legislation</td>
<td>No over-arching legislation; Sector specific.</td>
<td>PIPEDA and “substantially similar” provincial laws.</td>
<td>EU Directive</td>
</tr>
<tr>
<td>State data privacy laws (e.g. CA)</td>
<td></td>
<td>Alberta</td>
<td>Member State Implementing Laws</td>
</tr>
<tr>
<td>Data breach notification laws</td>
<td></td>
<td>British Columbia</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quebec</td>
<td></td>
</tr>
<tr>
<td>Transborder Restrictions</td>
<td>No federal statutory restrictions. Certain guidance/regulations specific to financial inst.</td>
<td>No restriction under PIPEDA. Certain guidance/regulations specific to financial institutions.</td>
<td>“Adequate” Countries OR under Model Clauses or BCRs (or to a Safe Harbor entity in the US)</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Outsourcing must be permitted under published privacy policy.</td>
<td>Outsourcing entity remains accountable for handling of information. Contractual clauses must protect against liability for supplier actions.</td>
<td>Non-EEA/“Adequate”: Model clauses/BCR or commitments US vendor Safe Harbor compliant. EU: Compliance with data controller reqmmts.</td>
</tr>
</tbody>
</table>