The APAC Juggling Act:
Tips for Global Financial Institutions on Managing Conflicting Regimes

Helen Woollett – Group Privacy Director, Barclays
Brad Bryant – EMEA Privacy Director, Aon UK Limited
Tom De Cordier – Counsel, Allen & Overy
Agenda

• Introduction
• Privacy laws in AsiaPac – recent developments
• Barclays Privacy Programme - Th!nk Privacy
• Tips for managing conflicting regimes
• Questions
Privacy laws in AsiaPac – recent developments

• Many AsiaPac countries recently adopted DP laws (eg. Singapore, PRC, Hong Kong, India, Malaysia, Indonesia, Taiwan, Philippines)

• Some DP laws (eg. Korea, Taiwan, Malaysia, Hong Kong) are based on standards similar to the EU privacy standards

• There are similarities but also many differences between these DP laws, for example:
  □ Scope
  □ Transfer restrictions

• APEC Cross Border Privacy Rules

• Ongoing discussions between WP29 and APEC to develop set of tools to facilitate cross-border transfers of personal data for multi-national companies operating both in the EU and in AsiaPac
Barclays Privacy Programme - Th!nk Privacy
Risk and control in a highly regulated environment

- Banking and financial services businesses are oriented towards their local financial services regulator
- Importance of the ‘branch concept’
- Cross border offerings vs. cross border transfers
- The role of compliance in relation to risk and control
- Privacy as a ‘principal risk’
- Control Issues of Group and Business Unit Significance
- What does all this mean for privacy risk and control?
The Barclays Privacy Programme

• Developed and implemented over a 4 - 5 year period.

• Key components included:
  - Gap analysis
  - Jurisdictional assessment
  - Structure and governance through an operating model
  - Third parties: controls and contracting
  - Incident handling and reporting
  - Awareness raising and education
  - Skilled team
  - Multi-party Model Clauses.
Starting point for communications

Barclays is committed to ensuring that customer and employee information is protected. Customers and colleagues need to know that we will look after their personal information.

• Provide a framework for various communications based on core messages

• Development of a tool kit

• Training documentation

• Measurement of training and awareness

• Encourage the sharing of best practice to improve
Combining generic and campaign communications will increase the effectiveness of your programme. Generic communication activity provides the foundation. Materials are used to deliver basic core messages about behaviours, and are used through channels where these messages will remain in place for the duration of the programme.

Campaign materials are used tactically to address specific issues. First they are used to boost general awareness then they can be used to trigger participation.
Applying this approach to APAC

- Jurisdictional analysis

- Gap analysis:
  - Legal gap
  - Practical gap

- What needs to be done on the ground and how is it affected by the regulatory environment?
  - Local DP regulator?
  - Local DPO required?
  - SAR’s?
  - Manual vs electronic records
  - Transfers
  - Controller/processor
Tips for Managing Conflicting Regimes
Asia Pacific – developments overview

**Vietnam:** Consumer protection law

**India:** Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

**Thailand:** Parliament considering draft privacy law

**Malaysia:** Data Protection Act passed 2010, pending gazettal

**Singapore:** Personal Data Protection Act, 2013; sunrise period to Jan 2014 (Do Not Call) and July 2014 (data protection)

**Australia:** Privacy Amendment (Enhancing Privacy Protection) Act 2012 – in force from March 2014

**Korea:** Personal Information Protection Act; in force from September 2011

**China:** Information Security Guidelines for Protection of Personal Information Within Information Systems for Public and Commercial Services from February 2013, and other laws

**Taiwan:** Personal Information Protection Act; in force from October 2012

**Hong Kong:** Personal Data (Privacy) Amendment Ordinance; in force from April 2013

**Philippines:** Cybercrime Prevention Act and Data Privacy Act, pending rules
APEC data protection working party – update

- W29 and APEC met in Jakarta on 31 January 2013

- Reviewing existing practices to facilitate transfer of personal data for MNCs between EU and APAC

- EU Binding Corporate Rules (BCR) to govern international transfers by corporate groups – ensuring adequate safeguards

- APEC use Cross-Border Privacy Rules (CBPR) with company privacy policies validated by APEC recognised Accountability Agents
  - Federal Trade Commission is only AA
  - US and Mexico only formal participants

- Similar approach – binding internal rules subject to prior approval but both are not widely used in practice and may take a long time to implement in your company at present
What similarities can we find? Spotlight on marketing in Hong Kong

- Direct marketing rules
- Implementation process
- Direct marketing enforcement action
- Lessons
Hong Kong – Direct marketing rules from 1 April

- Personal Information Collection Statement (PICS) detailing:
  - Intention to use personal data for direct marketing
  - Kinds of personal data collected for direct marketing
  - Classes of marketing subjects in relation to which the data is to be used
  - Classes of persons to whom the data may be transferred
  - Express consent to the intended use for direct marketing purposes (general or selective)
  - Response channel to communicate consent to the intended use
    (Fair Processing Notices, Transparency)

- Individuals must have clear unambiguous opportunity to opt-out
  (Lawful Processing Requirement)

- Grandfathering if, before 1 April 2013:
  - Personal data used for direct marketing
  - Individual informed of direct marketing use
  - Individual has not opted out
  - Used consistently with requirements of PDPO
Hong Kong – Direct marketing implementation

• Incorporating direct marketing PICS into:
  ▶ Aon branded individual insurance application forms
  ▶ Stand-alone document for non-Aon branded products

• Establishing centralised process for recording opt-out requests
  ▶ Developing implementation and tracking procedures

• Developing business awareness to contact DPO to review direct marketing before issuing
  ▶ Staff notifications
  ▶ Ongoing training / reminders
Hong Kong – Tips

• Clearly define:
  - purpose of collection
  - recipient of transferred data; and obtain consent

  vague terms such as “subsidiaries, partners, affiliates, third parties and other people under duty of confidentiality” is not sufficient without indicating the nature of those businesses to enable individuals to assess recipients with reasonable degree of certainty

• Commissioner’s powers strengthened from 1 April 2013

• Contravention is an offence

• Max penalty for unauthorised transfer for direct marketing is HK$500,000 and 3 years imprisonment (or HK$1,000,000 and 5 years if transferred gain)
Other Similarities? Spam and privacy laws

- Spam laws
- Interaction with privacy laws
- Compliance review before distributing marketing
Spam laws across APAC

<table>
<thead>
<tr>
<th>Country</th>
<th>Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hong Kong</td>
<td>Unsolicited Electronic Messages Ordinance</td>
</tr>
<tr>
<td>Singapore</td>
<td>Spam Control Act</td>
</tr>
<tr>
<td>Australia</td>
<td>Spam Act</td>
</tr>
<tr>
<td>China</td>
<td>Measures for the Administration of Internet E-Mails</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Unsolicited Electronic Messages Act</td>
</tr>
<tr>
<td>Philippines</td>
<td>Cybercrime Prevention Act</td>
</tr>
<tr>
<td>Korea</td>
<td>Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection</td>
</tr>
<tr>
<td>Vietnam</td>
<td>Anti-spam Decree</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Undang-undang Informasi dan Transaksi Elektronic (ITE) (Internet Law)</td>
</tr>
<tr>
<td>Japan</td>
<td>The Law on Regulation of Transmission of Specified Electronic Mail</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Communications and Multimedia Act</td>
</tr>
</tbody>
</table>
Spam and data privacy laws

• Spam - generally understood to refer to unsolicited electronic marketing messages - email, sms, posts on electronic billboards, etc.

• Remind business to contact you to review against Spam law / your internal company policies:
  ❑ advertising identifier in the subject line
  ❑ unsubscribe facility
  ❑ processing opt-out requests within time, etc. – subject to local laws

• Privacy laws may require consent for marketing purposes (not unsolicited)

• Review existing marketing lists to determine if captured by privacy laws and what consents are required – e.g. individuals in their personal and not business capacity (subject to local law)
A Familiar Issue? International Data Transfers from Singapore, Korea and Philippines

- Jurisdiction – off-shoring data processing
- International data transfers
- Breach notification
Extra Territorial Application - Off-shoring Data Processing

• **Singapore**
  - May potentially have extraterritorial application, guidelines pending

• **Korea**
  - Not limited to Korean data processors
  - Extraterritorial application possible for matters affecting Koreans

• **Philippines**
  - Extraterritorial application if:
    - PI about Philippine citizen or resident
    - Entity with link with Philippines whether processing PI in/outside the Philippines about Philippine citizens or resident
    - Entity with other links in the Philippines (business, PI originally collected or held by entity in the Philippines)
International data transfers?

• Is your business involved in transferring personal information across borders?

• Examples
  - Co-operating with your Company affiliates in other countries
  - Call recording and storage
  - Outlook email
  - Salesforce.com
  - Proofpoint
  - PeopleSoft (Oracle)
International data transfers - overview

• Singapore

- Guidelines pending

- Transfer if comparable standard of protection ensured by (i) imposing same restrictions on use/disclosure to purposes; (ii) use/disclosure limited to manner and extent specified in following agreements:
  - Inter-corporate transfers – binding contracts
  - Intra-corporate transfers – binding corporate rules

- Consent not required and consent does not avoid these requirements
International data transfers - overview

• Philippines
  □ Off-shore storage or transfer not prohibited
  □ Controller retains ongoing liability for PI transferred offshore/third parties
  □ Controllers must impose same security obligations as under Act
  □ BPO exception: PI collected from foreign residents under laws of those jurisdictions are not covered even if the PI is processed in the Philippines

• Korea
  □ Consent requirements apply to transfer outside Korea:
    − (i) purpose PI transferred; (ii) PI items; (iii) retention period; (iv) name of transferee; and (v) right of rejection disadvantage
  □ Transfer cannot involve contract that contravenes Act.
Data breach notification - overview

- **Singapore**
  - Silent

- **Philippines**
  - Sensitive PI or PI that may be used for identity fraud (if the Controller/NPC believes real risk of harm to Data Subjects), Controllers are required to notify NPC and Data Subjects
  - Notification:
    - nature of breach, the sensitive PI categories, measures taken to address breach
    - delayed only to determine breach scope, to prevent further disclosures, or to restore reasonable integrity to systems
  - Non-compliance may result in prosecution; imprisonment 18 months to 5 years; fines PHP 500,000 to PHP1 mill (approx USD $12-24,000)
Data breach notification - overview

• Korea

  - If aware unauthorised disclosure, must notify data subject of the following:
    - items of personal information leaked;
    - when and how personal information has leaked;
    - means available to the data subject to minimise damage that could be inflicted
due to the leakage;
    - the data processor’s actions and damage remedy procedures; and
    - the department in charge if damage is inflicted on the data subject.

  - If personal data of 10,000 or more data subjects is disclosed or accessed
    without authorisation, report to Ministry of Public Administration and Safety
    and other organisations

  - Penalties up to five years imprison or fine up to 50 million won (US$45k)
Incident reporting – Aon Approach

• All businesses must report local data incidences through local data protection officers to Aon’s Global Emergency Operations Center (GEOC) in a timely manner.

• Once reported, data incidences are investigated locally with periodic updates provided to GEOC. If a local data protection officer needs assistance during this process they can contact Asia Legal and the Global Privacy Office for guidance and support.

• For data incidences in their region, the DPO must:
  - Notify the GEOC within 24 hours of the incident
    - By email
    - By phone
  - Manage the incident locally and contact Asia Legal, GPO or the GEOC if any assistance is needed
  - Notify GEOC when the incident is closed
Preparing –
tips on building your project plan

- Hong Kong
- Singapore
- Philippines
- Taiwan
- Malaysia
Tips on building your project plan

• Develop your project plan – set a deadline

• Identify business lines, leaders and business contact

• Identify project team - IT, HR, SRM, Marketing, Compliance, Regional Legal

• identify tasks, timelines and directly responsible individuals
  - Map out each business line’s PI inventory
  - Identify collection, use, disclosure
  - Access and correction
  - Care for personal data

• Establish weekly meetings
Data flows to consider in your plan - example

- Transfers at each stage; disclosures, consents, obligations
- Cross-border
- Aon group recipients
- Security matters (involve SRM)
Questions