First Technical Assistance Seminar on the International Implementation of the APEC Privacy Framework, 2007

-

23rd January 2007, Canberra Australia

Practical Issues in Achieving Regional Privacy Compliance

Chris Connolly
http://www.galexia.com/

galexia

Overview

- Case studies
  - Common factors
  - Operations
- Compliance methodology
- Compliance issues
  - Overview
  - Sample summary table
  - Regional Policy development
- Cross border data transfers
  - Compliance issues
  - Cross border transfers in practice
  - APEC Cross border data policies

Case studies – common factors

- Multinational clients operating in 5 - 10 regional jurisdictions
- Require privacy management for both client data and employee data
- Considerable cross border data transfers to both related entities and third parties
- Regional and global data and communications systems in use, including remote cross border access
- Competing priorities and projects (security, anti-money laundering, IT upgrades, mergers and acquisitions) – privacy competes for attention and resources
- Internal and external audits in place – privacy emerging as an audit component

galexia

Case studies

Client A

- Financial services company
- Wholesale and retail clients
- Operations in:
  - Australia
  - Hong Kong
  - Japan
  - Korea
  - Singapore
  - Chinese Taipei
- Additional data transfer to:
  - China
  - India
  - UK
  - USA

Client B

- Telecommunications company
- Wholesale and retail clients
- Operations in:
  - China
  - Hong Kong
  - Japan
  - Korea
  - Chinese Taipei
  - USA
- Additional data transfer to:
  - Australia
  - EU
  - India

galexia

Typical Compliance Project Methodology

- **Phase 1**: Analysis of client compliance with local privacy requirements. This task involves a review of domestic legislation and codes of conduct, complemented by site visits to each Office to review documentation and procedures and to interview key management staff:
- **Phase 2:** Detailed description of implementation tasks for each Office, including proposed compliance steps.
- **Phase 3:** Development of compliance checklists and a draft Regional Privacy Policy that can assist the client deliver consistent privacy protection in the region.

Compliance Issues - Overview

- Priority of privacy issues is inconsistent. Dependent on:
  - Strength of legislation
  - Profile of regulator
  - Audit requirements
  - Profile of breaches
  - Severity of sanctions
- Common compliance issues are:
  - Management of duplicate databases containing personal information
  - Outsourcing arrangements
  - Offshore transfer of personal data
  - Data retention
  - Privacy training
- Site visits reveal levels of privacy awareness and privacy management issues that are not always apparent from documentation
- Care needs to be taken to ensure compliance regarding both client data and employee data (different rules apply)

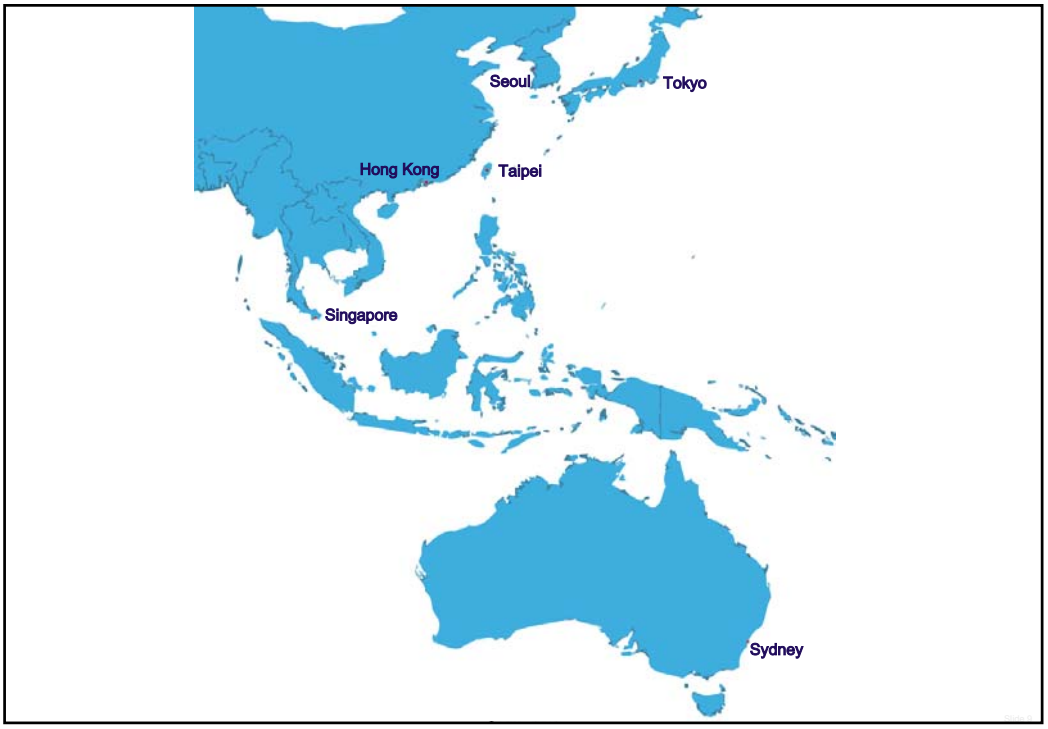
Example Summary Table (Fictional Data)

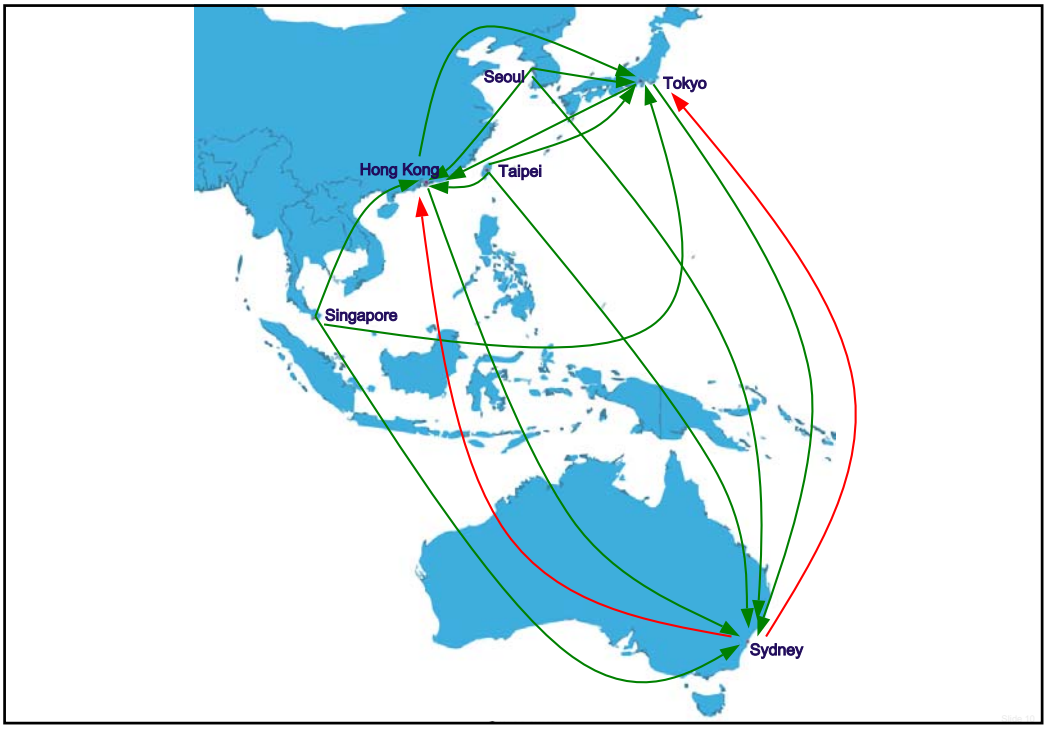
Component	Australia	Hong Kong	India	Japan	Korea	UK
PCO	Compliant	Partial compliance	Partial compliance	Non compliant	Compliant	Non compliant
Privacy policy	Partial compliance	Partial compliance	Compliant	Compliant	Non compliant	Non compliant
Data collection	Compliant	Compliant	Partial compliance	Compliant	Non compliant	Compliant
Records	Compliant	Non compliant	Non compliant	Non compliant	Compliant	Compliant
Comms	Partial compliance	Partial compliance	Compliant	Compliant	Compliant	Compliant
Complaints	Compliant	Compliant	Partial compliance	Compliant	Compliant	Partial compliance
Access	Compliant	Compliant	Compliant	Compliant	Compliant	Compliant
Security	Compliant	Partial compliance	Partial compliance	Compliant	Compliant	Compliant
Outsourcing	Partial compliance	Partial compliance	Non compliant	Non compliant	Non compliant	Partial compliance
Offshore tfr	Partial compliance	Compliant	Non compliant	Non compliant	Partial compliance	Partial compliance
Surveillance	Partial compliance	Partial compliance	Non compliant	Compliant	Compliant	Compliant
Data retention	Compliant	Partial compliance	Compliant	Non compliant	Non compliant	Non compliant
Training	Non compliant	Compliant	Partial compliance	Non compliant	Compliant	Compliant

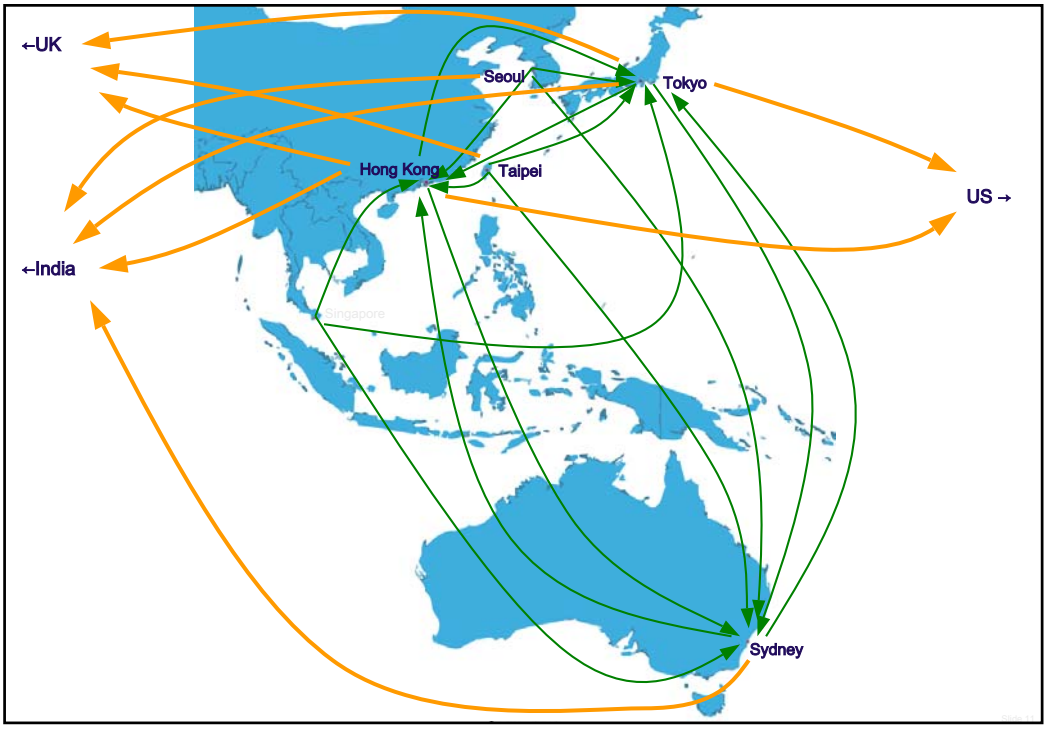
Regional Policy Development

- Some multinational clients wish to develop Regional Privacy Policies (in addition to local privacy policies)
  - » Although each office may have its own corporate identity, some organisations prefer to develop regional policies and protocols.
  - » A regional statement of commitment to privacy can send a positive message to consumers and regulators.
  - » The implementation of common compliance checklists can also help to ensure a higher degree of regional consistency and compliance.
  - » Regional policies deliver best practice even in jurisdictions without privacy legislation.

- However, Regional Policies also raise some implementation issues:
  - » Confusion where an office has two privacy policies
  - » Inconsistencies between regional and local privacy policies
  - » Identifying the first point of contact for queries and complaints


Seoul
Tokyo
Hong Kong
Taipei
Singapore
Sydney


Seoul
Tokyo
Hong Kong
Taipei
Singapore
Sydney



Cross Border Data Transfers in Practice

- **Formal agreements**
  - » In practice, some cross border data transfers are only subject to informal agreements – the absence of formal written agreements is an obstacle to promoting awareness and managing privacy compliance
- **Multiple transfers**
  - » Some data is transferred and re-transferred many times across multiple borders
- **Related entities**
  - » Defining related entities is difficult, and unlikely to always meet consumer expectations – multinationals have complex corporate structures
- **Outsourcing**
  - » Some data is transferred across borders and then outsourced (and vice versa) – determining responsibility for managing privacy compliance is complex
- **Multiple copies**
  - » Complex data processing often results in the same personal information being recorded in multiple locations – presenting a challenge for notice, consent, access, data quality and data retention principles
- **Access control**
  - » A common hidden form of cross border data transfer is the provision of regional or global remote access to data

APEC Cross Border Data Policies

- **Discussion Model 1 – Choice of Approach**
  - Some businesses are seeking greater consistency – they wish to benefit from re-using policies in multiple jurisdictions and may have concerns that these cannot be centrally approved under this model
- **Discussion Model 2 – Council of Regulators**
  - Some APEC jurisdictions do not have a single privacy regulator – businesses deal with a sector specific regulator who takes responsibility for privacy compliance in that specific sector (e.g. financial services, health and telecommunications)
  - Some APEC jurisdictions do not have a privacy regulator at all, but businesses may still transfer data to that jurisdiction and desire consistent management of privacy across the region
- **Discussion Model 3 – APEC Region Trustmark Model**
  - Many businesses are already subject to external audits and will want to avoid duplication
  - Will this Model extend to outsourced service providers?
- **Generic issues (applicable to all 3 Discussion Models)**
  - Businesses are uncomfortable with submitting policies for approval (time, expense) and have become used to risk / complaints based privacy regimes
  - Many data transfers will extend beyond APEC jurisdictions

Galexia

- www.galexia.com/
- Contact Galexia
  - Sydney Office
    - Suite 95, Jones Bay Wharf,
      (Lower deck, East side)
      26-32 Pirrama Rd,
      Pyrmont NSW 2009
      Australia
    - Telephone: +61 (02) 9660 1111
    - Facsimile: +61 (02) 9660 7611
    - Email: manage@galexia.com