RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

The Impact of National Laws on International Cloud Deployments.

SESSION ID: CDS-T10

Robert Gregory

Partner
Maddocks Lawyers, Australia
Robert.Gregory@maddocks.com.au
@robgreg225

Introduction and Overview

- International Data Protection and Privacy Law
- Reference Case
- Application of relevant laws to Reference Case
- Questions and Discussion
- Conclusion and Summary

International and National Data Protection and Privacy Law

- Overview of framework of international and national legal systems
- Data Protection and Privacy Laws
- Trans border data flows
- Comparison of high level features of each national law

Reference Case

- Cloud based system
- Supplier is US Corporation
- Infrastructure located in US, UK (EU), Singapore and Japan
- Customer is Australian Corporation
  - Customer's customers (users) includes individuals residing in US, France (EU), China and Australia
- User information includes information in relation to their health status

Application of Laws to Reference Case

- Start from the ‘bottom up’:
  - the personal information about users is the way in:
    - national / regional laws of:
      - USA, EU, China and Australia,

      all apply to the collection of personal information about and from those users
- Then, the Customer (being and Australian Company) is bound by Australian *Privacy Act* 1988
  - Must disclose purpose for collection, that it will be offshored and must look for functionally equivalent protection

Application of Laws to Reference Case

- Customer should / will require from its Supplier:
  - Practical protections built into infrastructure – including security / encryption of storage and end to end comms links
  - Acceptance of responsibility to deal with Customer's Users' information in a way which is consistent with the Customer's obligations to users

Application of Laws to Reference Case

- US based Supplier will need to consider:
  - Can it meet it's contractual obligations to Customer (so that Customer can meet its regulatory and contractual obligations to its Users)
  - What about national environment?
    - Does US Federal or State law provide for sufficient protection?
    - What about other jurisdictions in which Infrastructure is located (US, EU, Singapore, Japan)?
    - Can the national legal treatment / protection of information in one jurisdiction influence a decision about where to locate and how to manage the service?

Share.
Learn.
Secure.

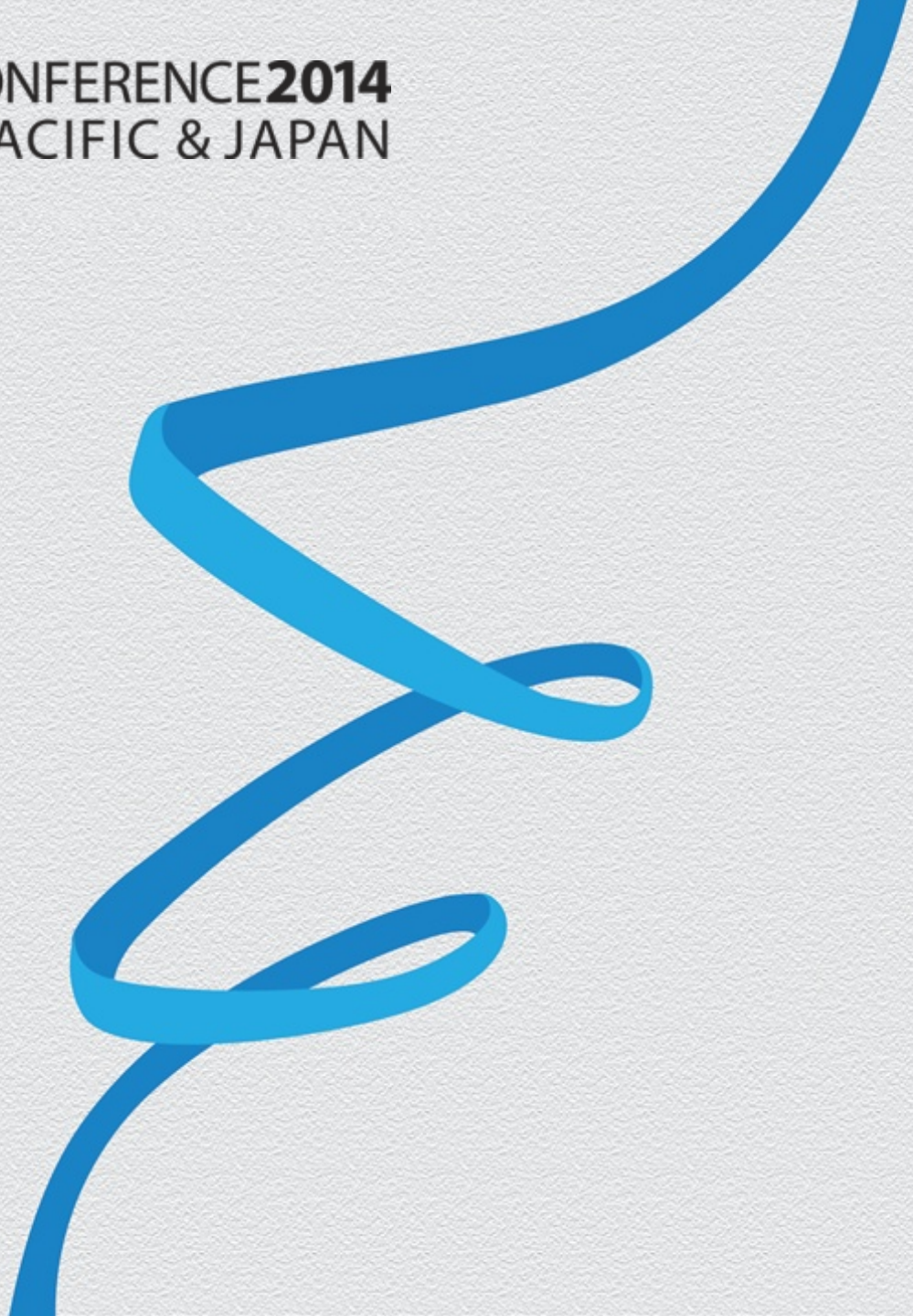
Capitalizing on
Collective Intelligence

Questions and Discussion

Conclusions and Summary

- As well as technical aspects of infrastructure architecture, capacity and detailed design – it is also necessary to consider the legal and regulatory framework which will apply
- While an understanding of the international legal aspects of national security, data protection and privacy law is helpful for context, detailed analysis of relevant national regulatory systems and laws will be required
- In most cases it is quicker and more efficient to build in privacy (as well as security) from the initial architecture and design, rather than to retro fit
- However regulation, like security, is constantly evolving so architecture needs to be flexible enough to deal with future changes and challenges

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN



#RSAC