Security in knowledge

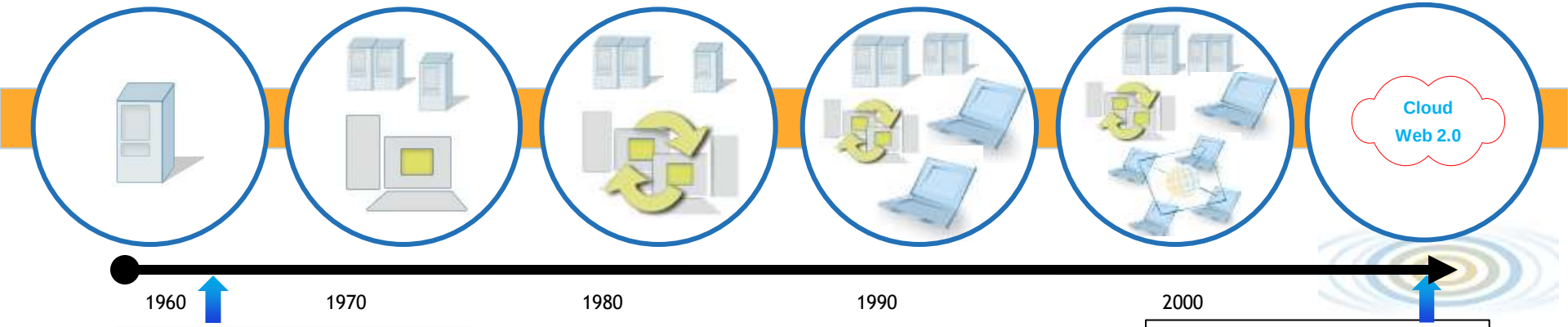
Is a Privacy Compliant Public Cloud Solution an Oxymoron?

Peter J Reid
Privacy Officer
HP Enterprise Business

RSA CONFERENCE 2013

Session ID: DSP-R35B
Session Classification: Intermediate

Historical IT Services Perspective



1962 - Ross Perot Founds EDS; Creates the Outsourcing Industry; Mainframe batch with limited online processing; all local

2013 – IT Services and Public Cloud are global operations with resources deployed globally; multiple laws and regulations apply

1962 – Compliance requirements – very simple

2013 – Compliance requirements – very complex; ITO, BPO, APPS; global scope

Cloud Delivery Models

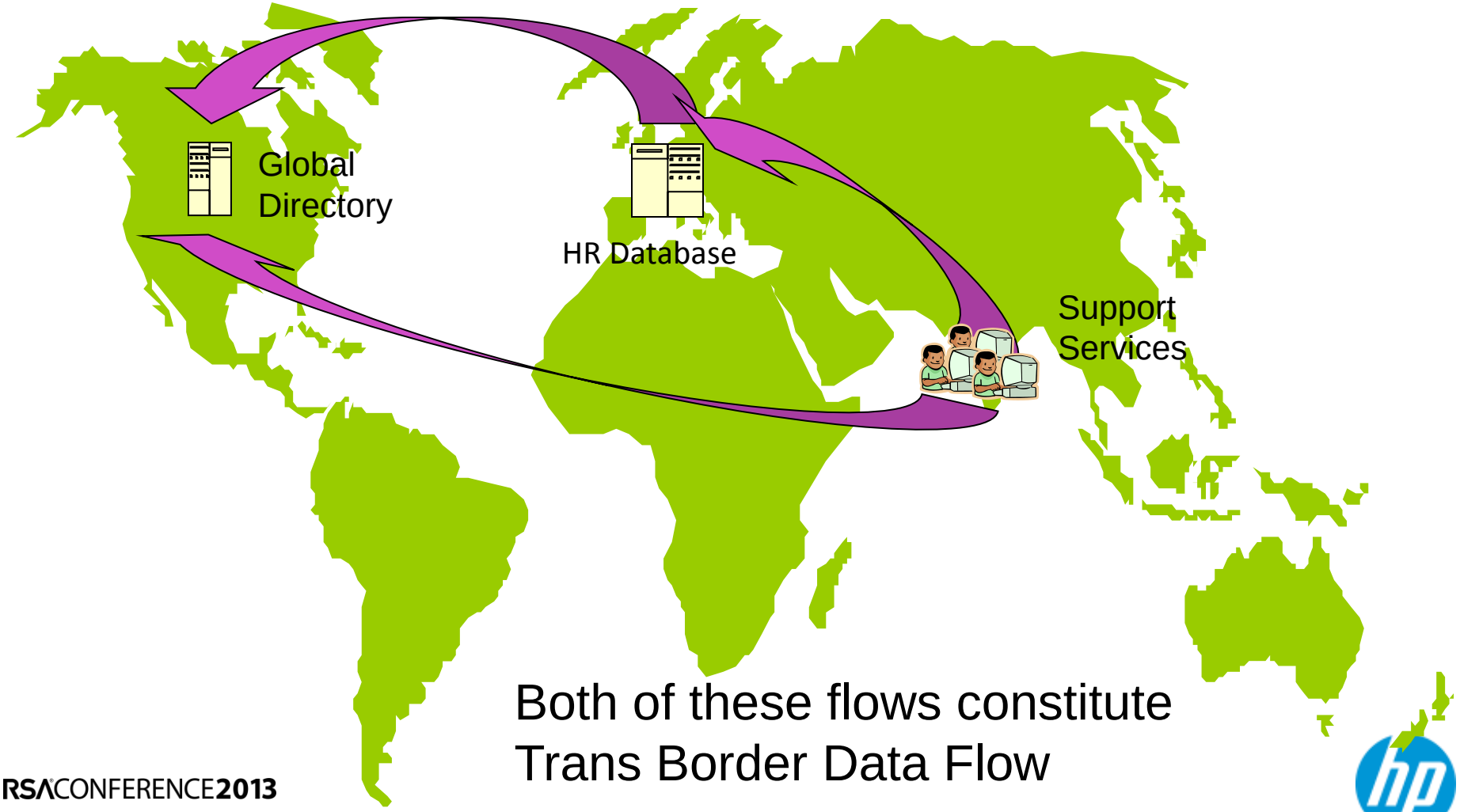
- Various Delivery Models
  - Private, Public, Hybrid
  - Global
  - Regional
  - Local (in country)
- Relative Costs of Delivery Models
  - Global – Lowest
  - Regional - Medium
  - Local – Highest
- Factors that impact selection of Delivery Model
  - Laws & Regulations
  - Internal Policies
  - Business Needs
  - Risk Acceptance

Implications of Laws & Regs on Cloud

- Privacy & Data Protection Laws
  - EU Data Protection Directive
    - Trans Border Data Flow
    - Security
  - APEC
- Export Control Laws
  - ITAR, Global Trade Laws
    - Trans Border Data Flow
    - Security
- Corporate Governance Laws
  - SOX
    - Security
- Data Breach Laws
  - 46 U.S. States, Germany, UK
    - Security
- Industry Specific
  - GLBA, HIPAA/HITECH, TCPA
    - Security

What is Trans Border Data Flow?

1. Personal Information from one country moved to another
2. Personal Information in one country can be accessed from another



Both of these flows constitute
Trans Border Data Flow

Biggest Compliance Challenges

- Data mapping and data flow analysis
  - Knowing where your personal and other confidential information is and where is it going is a key factor in compliance.
  - In the “Cloud” space, this becomes a critical issue
- Organizational
  - Business
  - IT
  - Legal (internal & outside counsel)
  - Compliance

Public Cloud - Do you have the answers?

First ask yourselves:

- What types of information, subject to regulations, is stored in your company's systems? (e.g. personal information, financial information, sensitive corporate information, export controlled information)
- Do you know exactly where that information is stored?
- Have you documented all the data flows, including all sources and destinations?
- Which regulations are you subject to?
- Does your IT organization understand the implications of all the regulations you are subject to?
- What is your compliance organization structure? Where does it reside?

Public Cloud – Service Providers' Positions

Then ask your providers:

- Where will my data be stored and from where will it be accessed?
- What are their privacy and data protection programs and policies?
- What are their security programs and policies?
- Are all of their service providers and sub-contractors obligated to meet your internal and contractual Privacy and Security requirements?
- How will they help us meet our regulatory and corporate compliance obligations?

Summary

When engaging a Cloud Service Provider

- The contract
  - Clarify roles and obligations of parties
  - Compliance responsibility cannot be transferred
- Technical and organizational measures
  - Processing risk and nature of data are key to what is ‘appropriate’
  - Ask for evidence of
    - Privacy and security policies
    - Implementation of security controls
    - Training of personnel
  - Be prepared to conduct site visits
- If transfers of PI out of the EU/EEA will occur
  - Establish the requirements under which transfers may take place
  - If EU Model Contracts are required, start work on them as soon as possible to avoid delays in delivery of service

Security in knowledge