RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

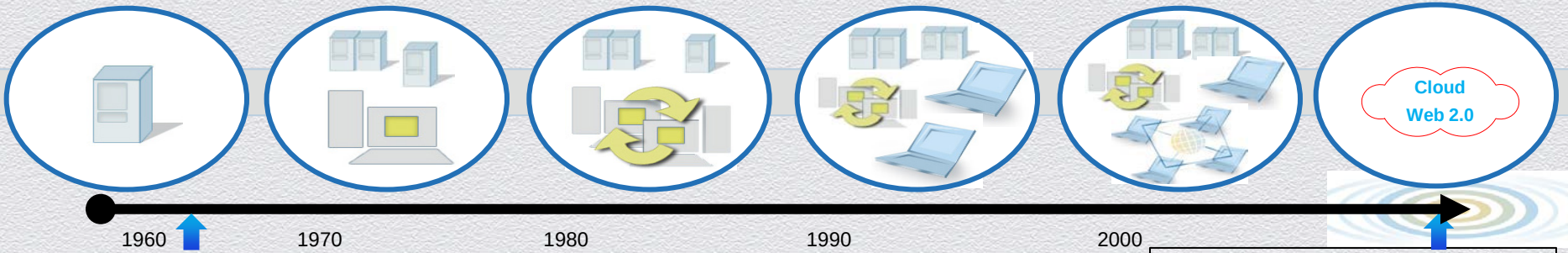
Implementing Privacy Compliant Hybrid Cloud Solutions

SESSION ID: DSP-T07A

Peter J Reid

Privacy Officer, Enterprise Business
Hewlett-Packard Company

Historical IT Outsourcing Perspective



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

2014 – Outsourcing/Cloud are global operations with resources deployed globally; multiple laws and regulations apply

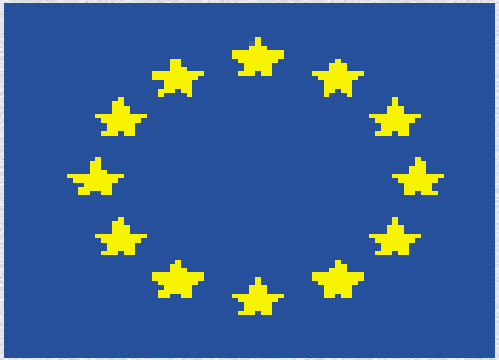
1962 – Compliance requirements – very simple

2014 – Compliance requirements – very complex; global scope

Significant Privacy Legislation Exists Outside US

- **In Europe, the European Data Protection Directive & its supporting country legislation considers privacy (data protection) a human right**
- **Legislation, similar to European Data Protection Directive, has been & continues to be enacted in many other countries**
  - **Argentina ***
  - **Australia**
  - **Canada ***
  - **Hong Kong**
  - **Israel ***
  - **Japan**
  - **New Zealand ***

* Deemed 'adequate' by EC



Most International Privacy Laws Place Restrictions on Trans-Border Data Flow

U.S. Approach To Privacy Legislation, Historically Sector-Based, Has Been Growing

No current U.S. Privacy Laws place any restrictions on Trans-Border Data Flow

- Fair Credit Reporting Act
- Privacy Act
- Family Educational Rights and Privacy Act
- Right to Financial Privacy Act
- Cable Communications Privacy Act
- Electronic Communications Privacy Act
- Video Privacy Protection Act
- FCC TCPA & CPNI Rules
- Driver's Privacy Protection Act
- Telecommunications Act
- Children's Online Privacy Protection Act
- Wireless Communications and Public Safety Act
- Gramm Leach Bliley Act
- Health Insurance Portability & Accountability Act (HIPAA)
- FTC Do Not Call Registry & Telemarketing Rules
- CAN-SPAM Act
- Fair & Accurate Credit Transactions Act (FACTA)
- HITECH Act

Other Privacy Regulatory Considerations

- FTC Act - 1914 (section 5 “unfair & deceptive practices”)
- 46 U.S. states now have Identity Theft Notification laws (aka Data Breach laws); HITECH Act has similar requirements as do several EU countries. Similar laws now being considered in other geographies
- Payment Card Industry Data Security Standards (PCI DSS)
- Online Behavioral Advertising (OBA) laws in place and proliferating
- USA Patriot Act

Privacy Restrictions On Trans-Border Data Flow

Privacy & Data Protection regulations restrict transfer of "personal information" across national borders

a. Transfers from all countries with comprehensive national legislation are restricted
   i. EU/EEA, Switzerland, Argentina, Australia, Canada, Japan, Korea, Mexico, etc.
b. From EU/EEA countries, personal information can be transferred to countries that have "adequate protection"
   i. All other EU/EEA member states are deemed to be adequate ✓
   ii. Switzerland, Canada, Argentina, Israel, New Zealand, Uruguay all have regulations deemed adequate by the EU ✓
   iii. No other countries (e.g. US, Brazil, China, India, Malaysia, Philippines, Costa Rica) are deemed adequate by the EU, so transfers are restricted ✘

Overcoming Privacy Restrictions

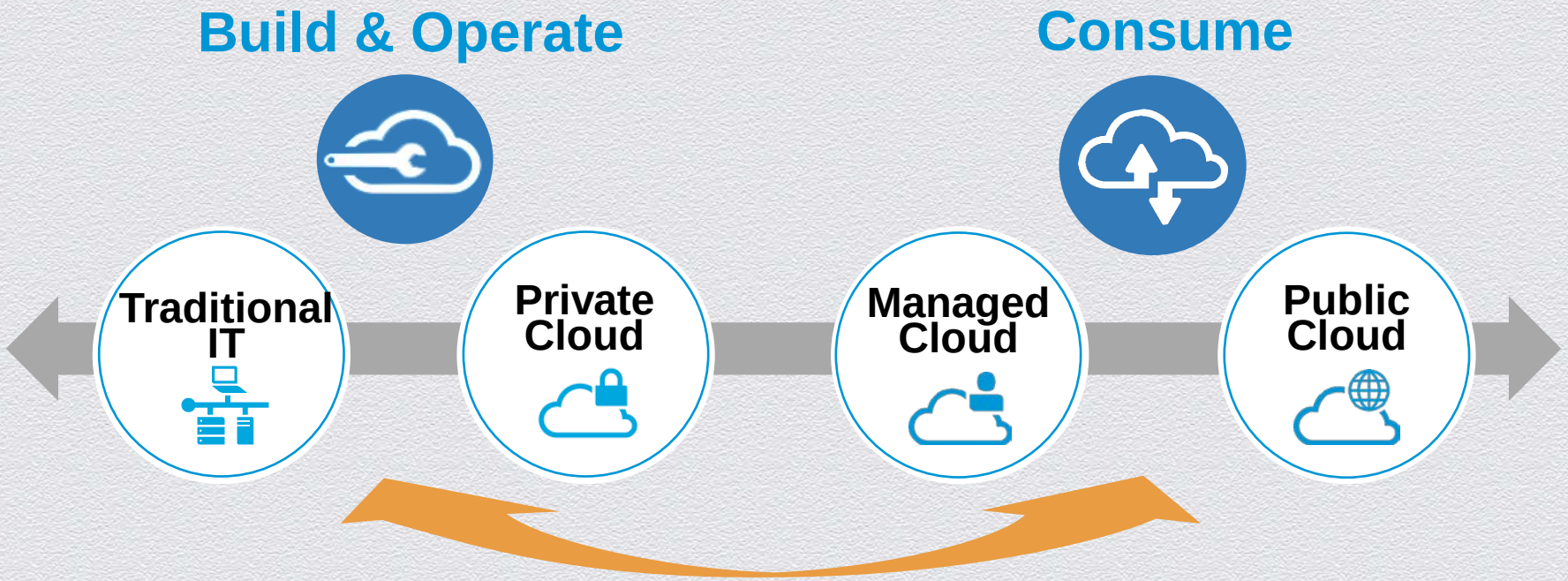
Mechanisms to overcome transfer restrictions

a. Information can be transferred from a company in an EU/EEA country or Switzerland to it's U.S. entity if that entity has joined U.S. DoC Safe Harbor
   i. Safe Harbor applies only to transfers of PI from the EU to the U.S.
   ii. Safe Harbor also allows "onward transfers" to other jurisdictions
b. Personal information can also be transferred from any EU/EEA country to any non-EU/EEA country, other than "approved adequate countries", if:
   i. A model contract has been signed & in many instances approved by the country regulator, or
   ii. Binding Corporate Rules (BCR) /Binding Corporate Rules for Processors (BCR-P) have been approved, or
   iii. The individual has "freely given" consent
c. Transfers from other countries with national privacy legislation also require contractual agreement. APEC has introduced Cross Border Processing Rules (CBPR, CBPR-P)

Summary of Laws & Regulations Impacting Cloud

	Implications
Privacy & Data Protection Laws	
• EU Data Protection Directive	• Trans Border Data Flow
• Canada's PIPEDA, Provincial laws	• Security
• US Sectoral Laws (e.g. GLBA, HIPAA/HITECH)	• Security
Export Control Laws	
• ITAR, Global Trade Laws	• Trans Border Data Flow
Corporate Governance Laws	
• SOX	• Security
Data Breach Laws	
• 46 U.S. States	• Security
• HITECH	• Security
• EU Data Protection Regulation	• Security

Enterprises shifting to a hybrid cloud model

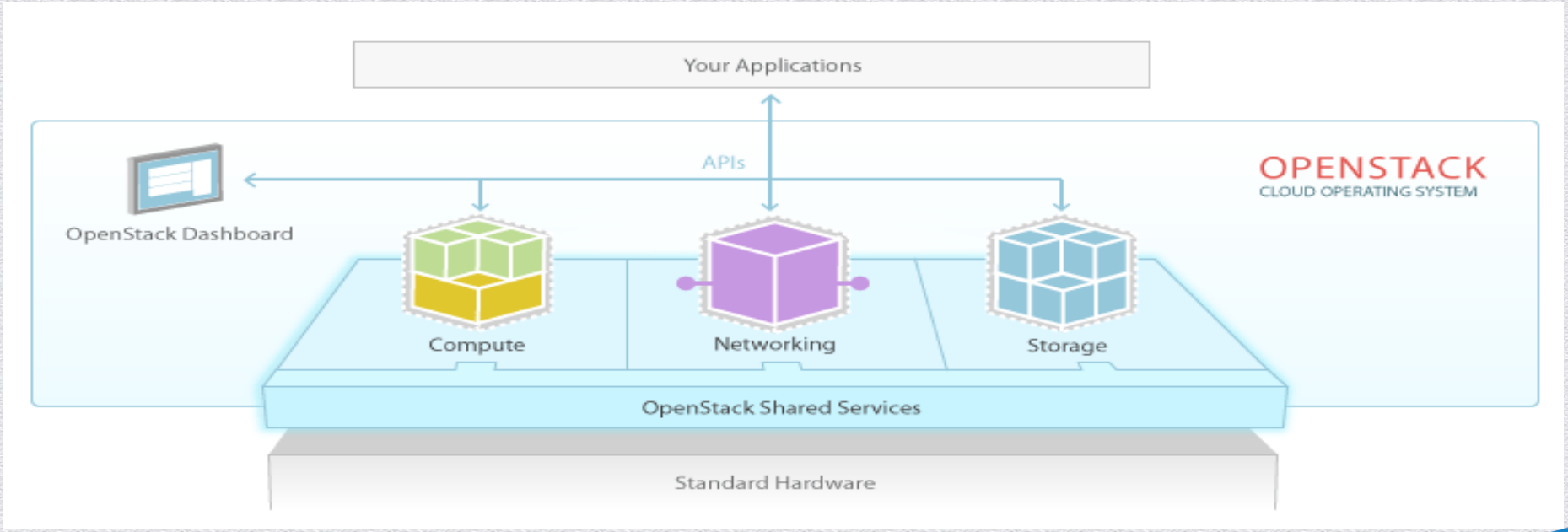


Service Level Agreements (SLAs)

Availability, Security, Performance, Compliance, Cost

openstack™
CLOUD SOFTWARE

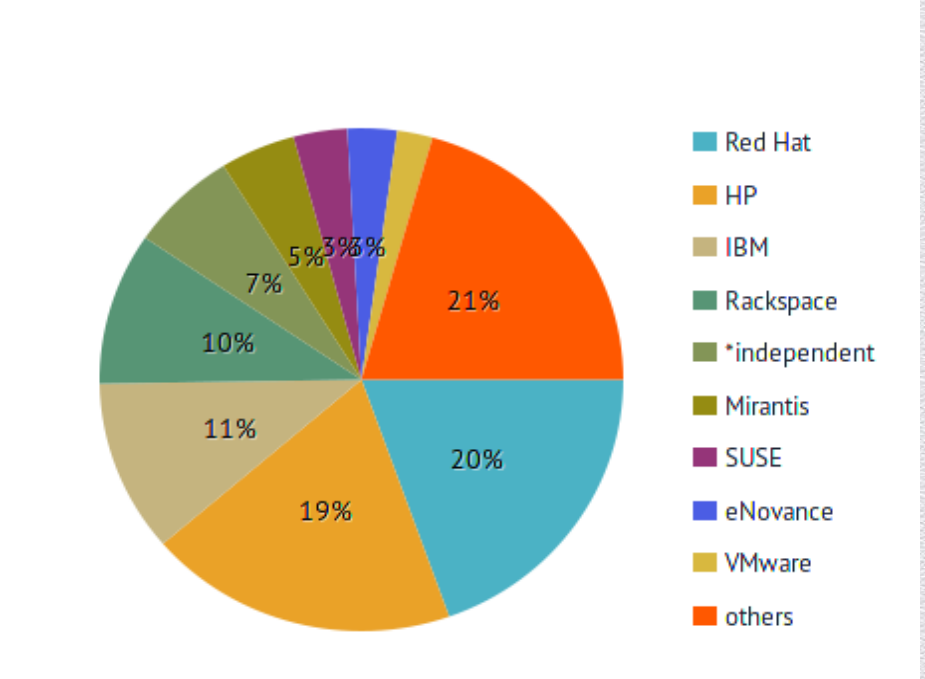
Open source software for building private and public clouds



http://www.openstack.org/

Openstack Contributors

- Unaffiliated individuals
- Commercial entities
- Nonprofit organizations
- National and local governments
- Number, quality, and area of contributions can change daily



Biggest Cloud Compliance Challenges

Data mapping and data flow analysis

- Knowing where your personal and other confidential information is and where it is stored and from where it can be accessed is a key factor in compliance.
- In the “Public/Hybrid Cloud” space, this becomes a critical issue as it determines compliance requirements when your data is being stored and processed by a third party

Privacy & Outsourcing – 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?

Privacy Considerations – Do you have the answers?

Then ask your providers:

- Where will my data be stored and from where can it be accessed?
- What are your privacy and data protection programs and policies? Do you have approved BCR or BCR-P in the EU? Do you have approved CBPR or CBPR-P in APEC member countries?
- What are your security programs and policies? Do they meet the security requirements of HIPAA, PCI DSS, etc?
- Are all of your sub-contractors obligated to meet your internal and contractual Privacy and Security requirements?
- How will you help us meet our regulatory and corporate compliance obligations?

Summary

When engaging a cloud service provider

- The contract
  - Clarify roles and obligations of parties
- 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 (e.g. Model Contracts, BCR, BCR-P, etc)
  - If EU Model Contracts are required, start work on them as soon as possible to avoid delays in delivery of service
- Always remember, you cannot “outsource” your compliance obligations

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO