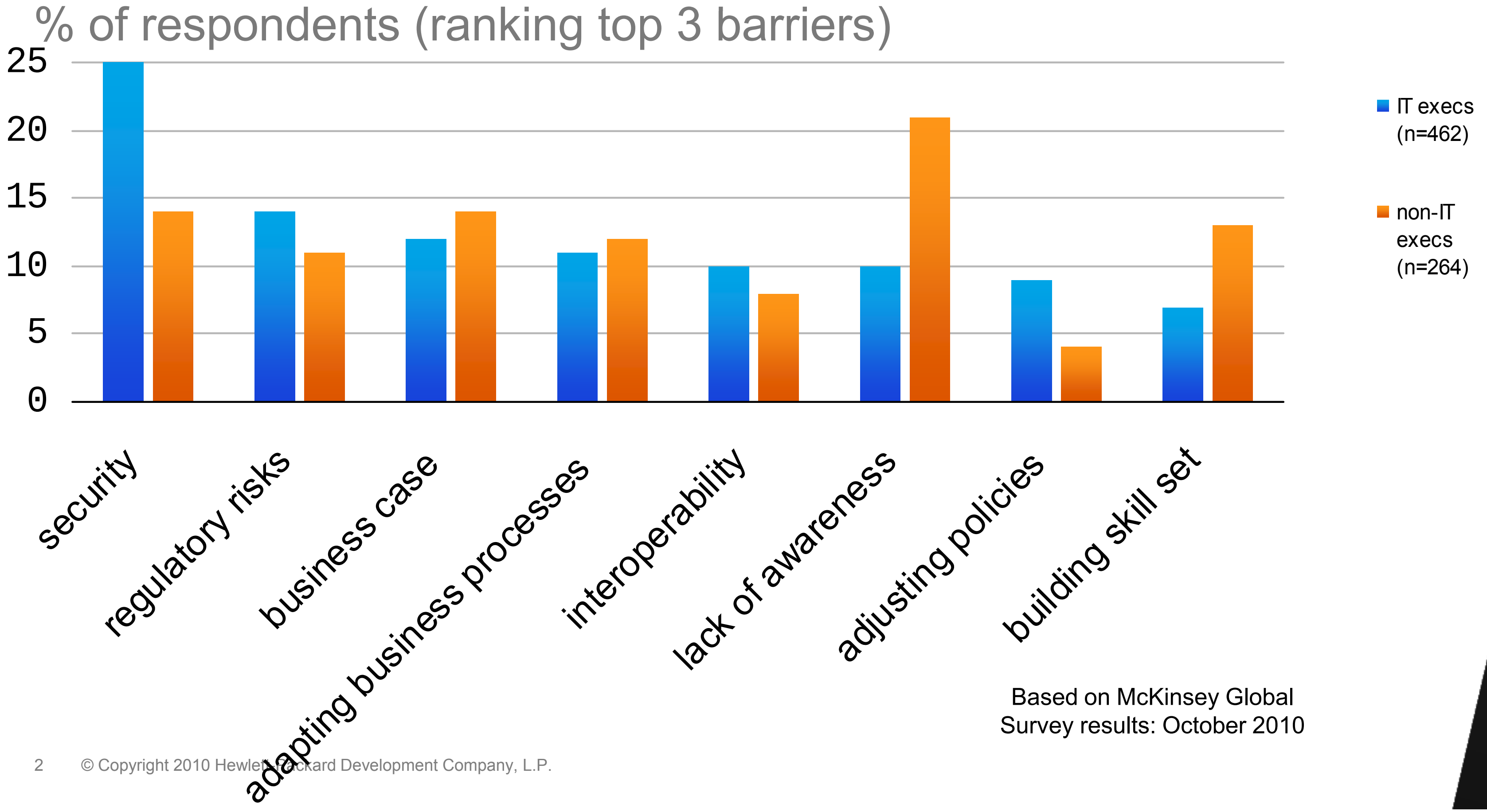
PRIVACY, SECURITY AND TRUST ISSUES ARISING FROM CLOUD COMPUTING

Siani Pearson* and Azzedine Benameur

HP Labs Bristol, UK

December 2010

BARRIERS TO CLOUD TECHNOLOGY



Based on McKinsey Global Survey results: October 2010

CONTENT

– Privacy issues for cloud

– Security issues

– Legal aspects

– Trust

– Addressing these issues

PRIVACY ISSUES

WHAT IS PRIVACY?

At the broadest level, privacy is:

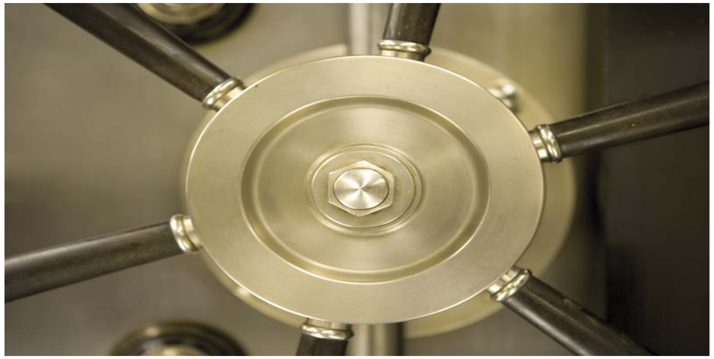
- The right to be left alone
- The right to associate with whom you choose

In the commercial/consumer context:

- Privacy is about the protection and careful use of the personal information of customers
- Meeting the expectations of customers about the use of their personal information

For corporations, privacy is about:

- The application of laws, policies, standards and processes by which Personally Identifiable Information (PII) of individuals is managed



IVACY BASICS

ition – Personally identifiable information

sonally Identifiable Information commonly referred to as personal data or personal rmation in Europe and Asia, can be defined as *information that can be traced to a ticular individual,* and include such things as the items listed below:

-ull name: Mike Smith
-lome address: 123 Main St.
-lome phone: 408-555-1212
-Social security number or national identity number
-Credit card #: 4755-5555-5555
-Email address: jdoe@jdoe.com
-Password: 851pass392
-Date of birth: 4 April 1975

IVACY BASICS

ition – Sensitive information

nsitive Information can be considered as a sub-set of personal information, and ause of its sensitive nature greater care must be taken in its handling. Use is cially regulated in EU. Sensitive information includes information revealing:

Racial or ethnic origin
Political opinions
Religious or philosophical beliefs
Trade-union membership and
Data concerning health or sex life.
Financial or medical information.

IVACY CHALLENGES

ndividuals

- solicited marketing
- ntity theft
- vealing personal information friends, family members
  - : Behavioral advertising
- ntended use or inferences from information
  - g. from Social Networking data
- vernment surveillance
- bpoena of information stored “in the cloud”

IVACY CHALLENGES

Businesses

- ta breaches
  - an be costly (on average $204 per record, according to 2010 Ponemon stitute study)
- untry-specific laws expose companies to a risk of litigation
- hen customers are concerned for the welfare of their privacy it n affect a company's ability to do business.
- gative public attention and loss of brand value
- mplexity of managing privacy

IVACY ISSUES FOR CLOUD COMPUTING

- mplex information environment
  - Data flows tend to be global and dynamic
  - Data proliferation
  - Dynamic provisioning
- ck of user control
- authorised secondary usage
- tention of data
- s data been properly destroyed?
- ve privacy breaches occurred?
- ho is at fault in such cases?

PRIVATE PROPERTY
AUTHORIZED
PERSONNEL ONLY
AUTHORIZED USERS
KEEP GATE CLOSED AT ALL TIME!
IF YOUR LOCK IS NOT ON THIS GATE,
IT IS BECAUSE YOU HAVE NOT MADE
ARRANGEMENTS FOR LEGAL ACCESS.
PLEASE CALL (213) 316-73-73

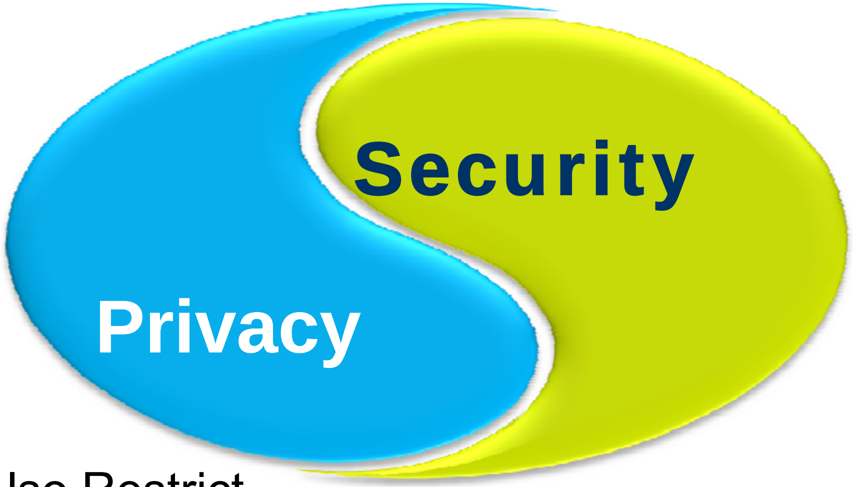
ECURITY ISSUES

W ARE SECURITY AND PRIVACY DIFFERENT?

ersonal Information-andling Mechanisms

dual Rights"

- airness of Use
- lotice
- hoice
- ccess
- ccountability
- ecurity



Privacy Laws Also Restrict -Border Data Flow of nal Information

Protection Mechanisms

- Authentication
- Access controls
- Availability
- Confidentiality
- Integrity
- Retention
- Storage
- Backup
- Incident response
- Recovery

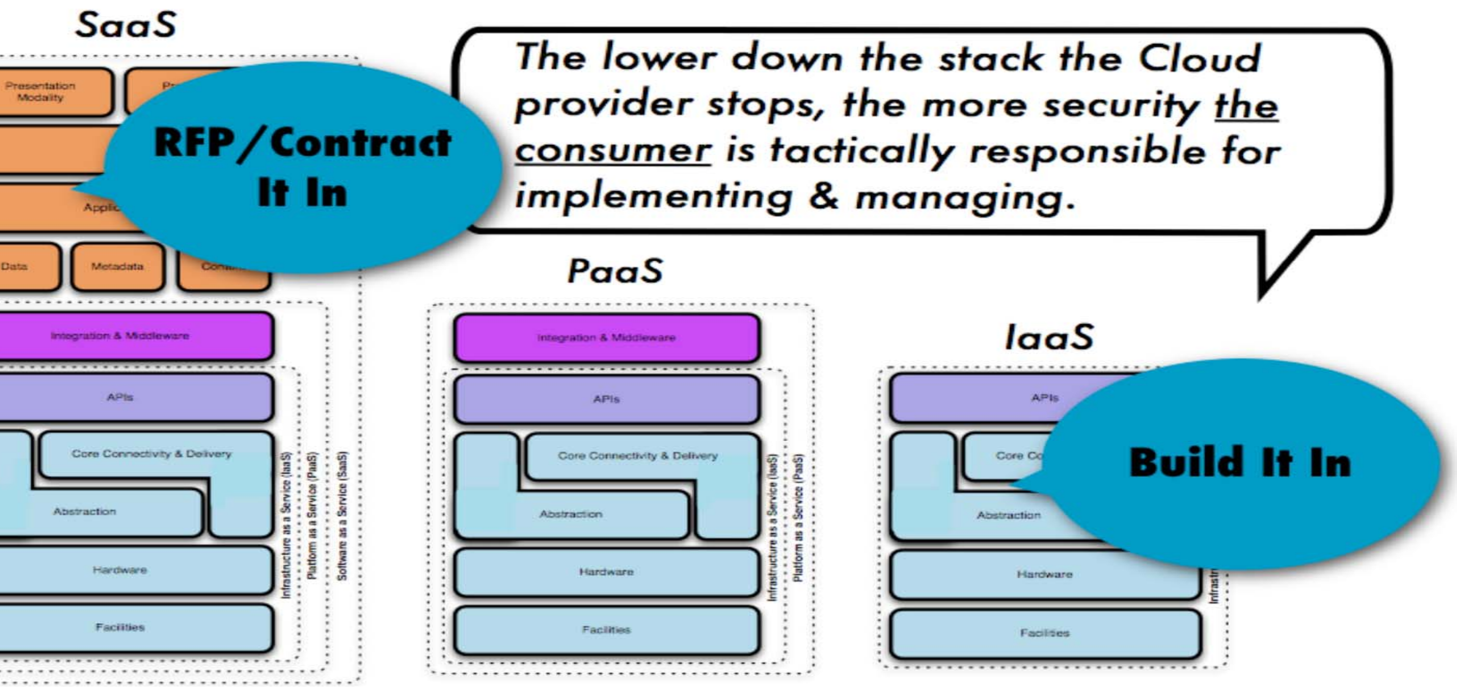
ERVIEW

rivacy relates to ersonal information

Security and confidentiality can relate to all information

Context is important: different information can have different privacy, security and confidentiality requirements

IE CLOUD SECURITY ALLIANCE ECURITY HIERARCHY


The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.

RFP/Contract It In

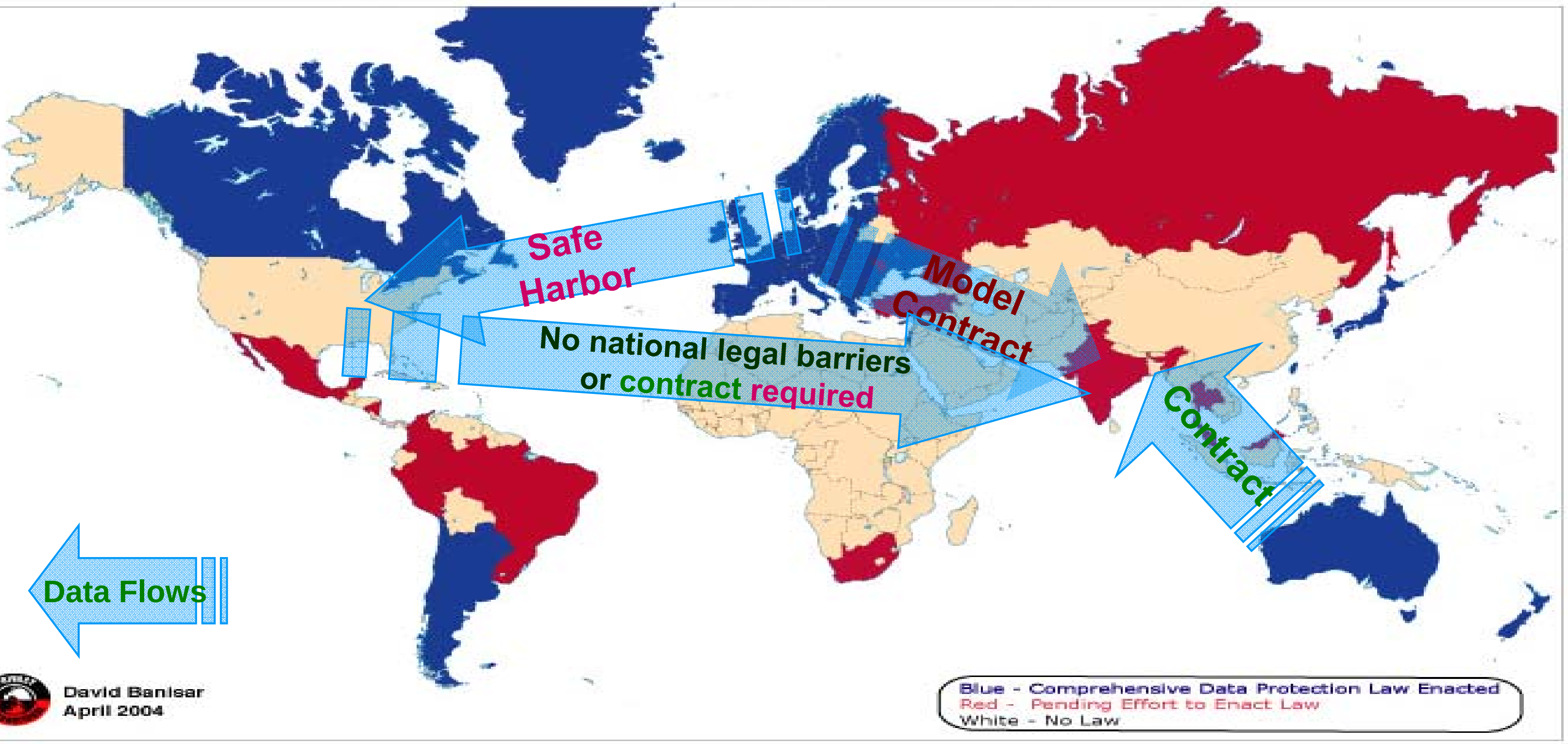
Build It In

CURITY ISSUES FOR CLOUD MPUTING

- cess control
- ntrol over data lifecycle
- ailability and backup
- ck of standardisation
- dit
- lnerabilities, e.g.
  - tnets and trojan horses exist in cloud services
  - ata theft in cloud
  - oss-VM side channel attacks

GAL ASPECTS

TA PROTECTION LAWS AROUND THE ORLD

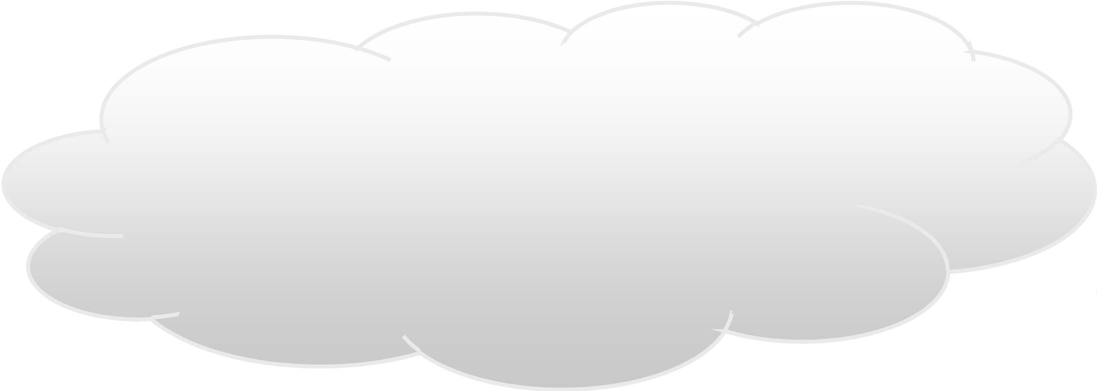

Safe Harbor
Model Contract
No national legal barriers or contract required
Contract
Data Flows
David Banisar
April 2004
Blue - Comprehensive Data Protection Law Enacted
Red - Pending Effort to Enact Law
White - No Law

GAL ISSUES FOR CLOUD COMPUTING

- cation matters
- ficult to comply with legislation
  - specially transborder data flow requirements
- ta processors must use ‘reasonable security’
- SP may be forced to hand over data stored in cloud
- uation subject to change

RUST ISSUES

OUD PERSPECTIVES



Cloud Service Provider

Cloud Service Consumer

- u own and manage all of the IT assets
- u assume the specific costs and risks e service components

Two very different roles

Two very different perspectives

- You don't need software, hardware, technical knowledge.
- You don't own the assets.
- You don't assume the specific costs and risks of the service components

a Protection

Tru st

Privacy

PECTS OF TRUST

l science

bjective

mporal

k

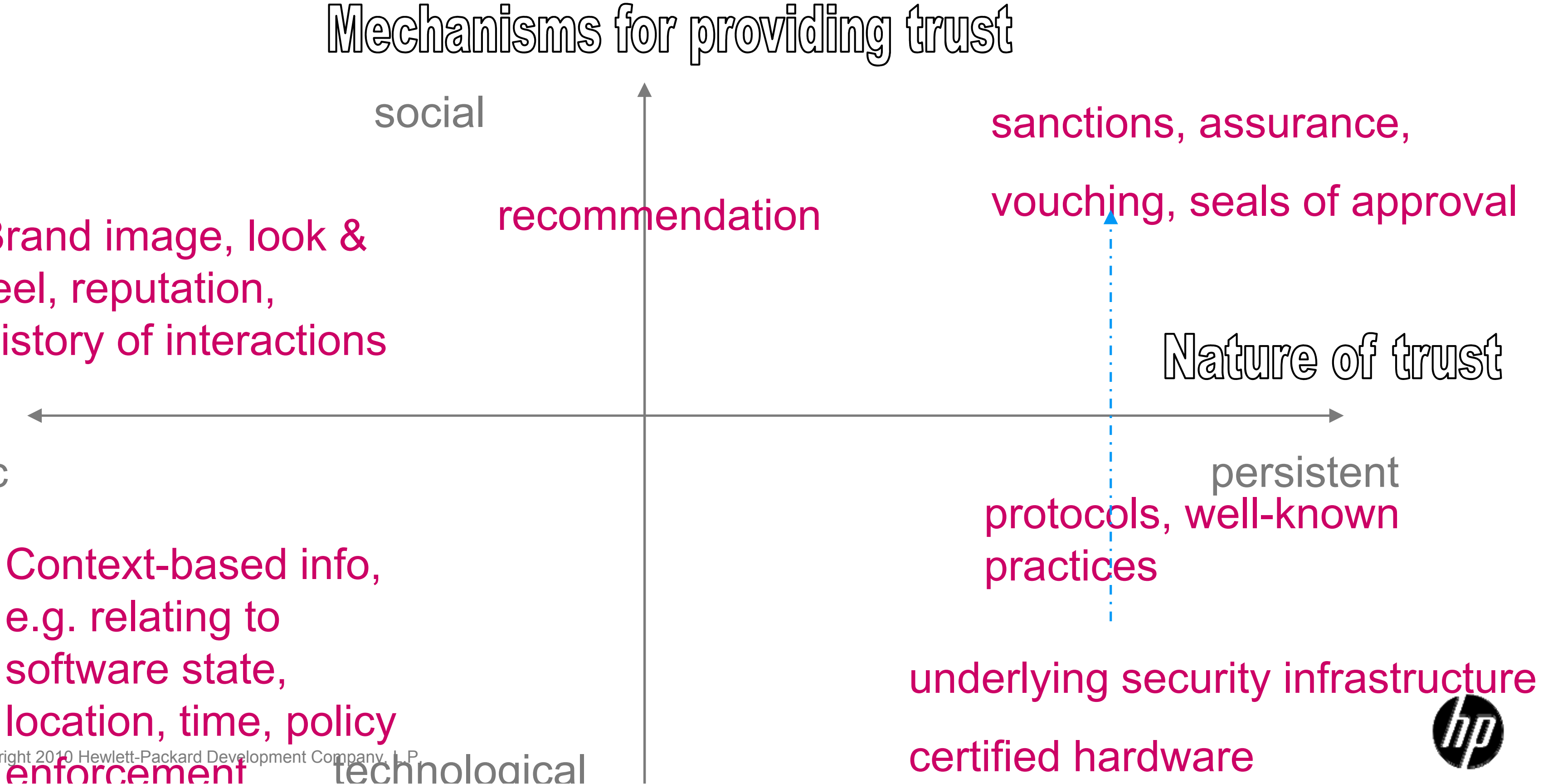
egation

namic

Studies of on-line trust

- Brand image
- Provision of assurance info
- Security & privacy

RSISTENT VS. DYNAMIC TRUST



Mechanisms for providing trust

social

recommendation

sanctions, assurance,

vouching, seals of approval

Brand image, look &
eel, reputation,
istory of interactions

Nature of trust

c

persistent

protocols, well-known
practices

Context-based info,
e.g. relating to
software state,
location, time, policy
enforcement

technological

underlying security infrastructure

certified hardware

UST ISSUES FOR CLOUD COMPUTING

- eak trust relationships
  - on-transitivity of trust, esp. ‘on demand’ models
  - ust mechanisms need to be propagated right along chain of service provision
- ck of consumer trust
  - ue to lack of transparency and control
  - sp. for sensitive info
  - ust key to adoption of SaaS

DRESSING IVACY, SECURITY D TRUST ISSUES

e different approaches

PORTANCE OF CONTEXT

- vacy need be taken into account only if the cloud service handles rsonal information, in the sense of collecting, transferring, processing, aring or storing it
- vacy threats differ according to the type of cloud scenario, e.g.
  - low privacy threat if the cloud service is to process information that is (or is very shortly to be) public, cf. NY Times
  - high privacy threat for cloud services that are dynamically personalized – based on people's location, preferences, calendar and social networks, etc.
- ntext is central to requirements
  - The same information collected in a different context by a different entity might have completely different data protection requirements.
  - Multiple requirements may need to be met by the same provider.
    - e.g. cloud-based services marketplace customer engaged in international health study would have to comply with EU and US privacy laws, and as the data controller, would need a way to obtain assurances that any potential service suppliers are employing proper data privacy protection practice
- ctors: location, sensitivity of data, culture, trust relationships,…

TANDARDISATION

ernationally recognized
ud Computing standards

evant Industry
anizations with substantive
ud
mputing initiatives and
grams

vernment and international
ndards and practices
anizations

Cloud Security Standards

OASIS

CSA cloud security alliance

THE Open GROUP Making standards work®

Trusted Cloud

Industry Programs

JERICHO

DMTF

tmforum

Open Cloud Consortium

ISACA® Serving IT Governance Professionals

OpenGridForum OPEN FORUM | OPEN STANDARDS

SNIA

IEEE

Best Practices Organizations & Programs

ISO

NIST National Institute of Standards and Technology

enisa

ANSI American National Standards Institute

ETSI

SIGN FOR PRIVACY

Is	Is Not
Driven by global and local regulations	A replacement for other Secure Design Principles and requirements
Initial set of best practice design principles and standards	Bolted on at end of design process

DRESSING ISSUES IN CLOUD MPUTING

ocedural measures

- etermining capabilities of CSP before selection
- egotiating contracts
- estricting transfer of confidential data to CSP

ta security mitigation

- ncryption

echanisms for increasing trust

- ivacy infomediaries, sticky policies, agents

lutions need to address a combination of issues above => new echanisms

RRENT RESEARCH

fuscation

sign patterns

countability in the cloud

tural language policies in contract associated with lower-level chine-readable policies that

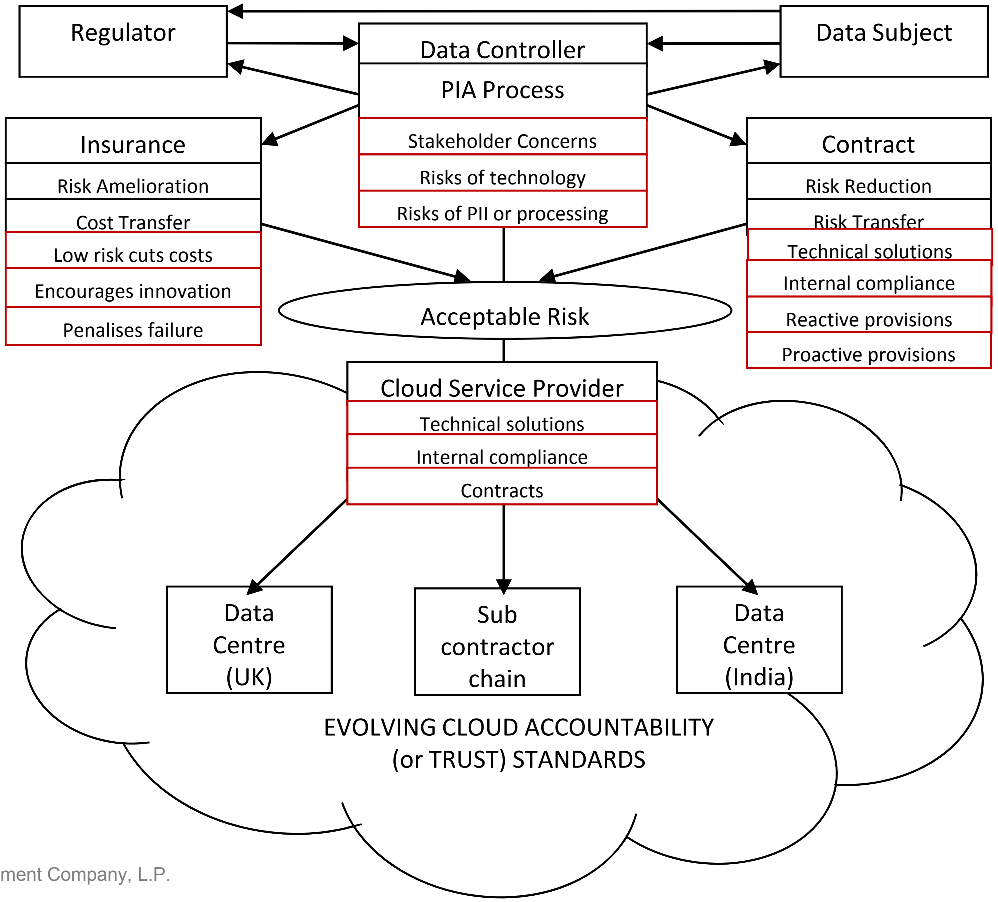
- efine usage constraints of the associated PII
- nsmitted through the cloud associated with PII
- ted upon automatically within the cloud without the need for human ervention

vacy protecting controls built into different aspects of the business cess

- going process of review throughout the contractual chain

k assessment & decision support to assess harm

COUNTABILITY



Regulator

Data Subject

Data Controller

PIA Process

Stakeholder Concerns

Risks of technology

Risks of PII or processing

Insurance

Risk Amelioration

Cost Transfer

Low risk cuts costs

Encourages innovation

Penalises failure

Contract

Risk Reduction

Risk Transfer

Technical solutions

Internal compliance

Reactive provisions

Proactive provisions

Acceptable Risk

Cloud Service Provider

Technical solutions

Internal compliance

Contracts

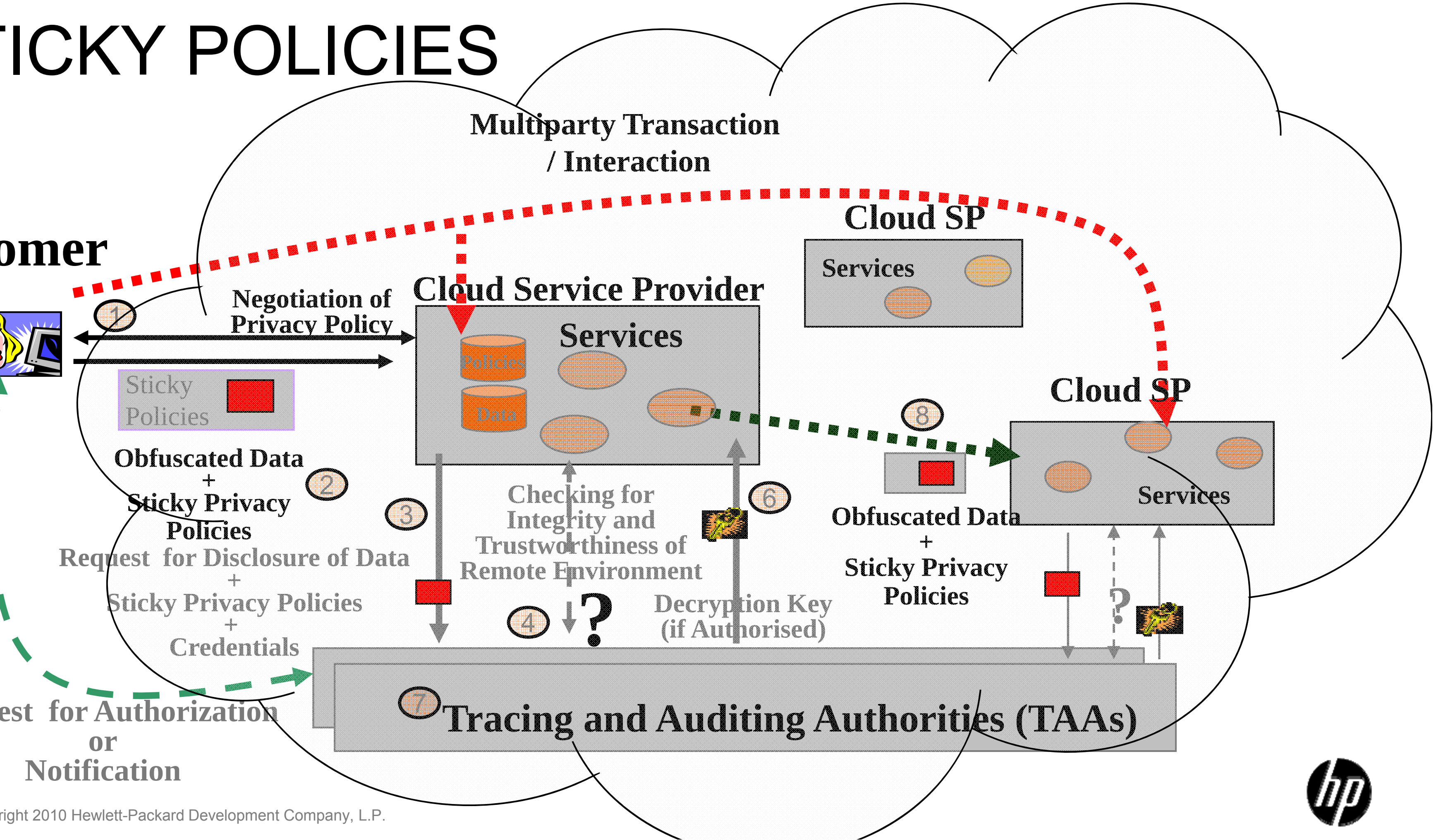
Data Centre (UK)

Sub contractor chain

Data Centre (India)

EVOLVING CLOUD ACCOUNTABILITY
(or TRUST) STANDARDS

TICKY POLICIES


Multiparty Transaction / Interaction
omer
Negotiation of Privacy Policy
1
Sticky Policies
Obfuscated Data + Sticky Privacy Policies
2
Request for Disclosure of Data + Sticky Privacy Policies + Credentials
3
Cloud Service Provider
Services
Policies
Data
Checking for Integrity and Trustworthiness of Remote Environment
4
?
Decryption Key (if Authorised)
6
Cloud SP
Services
8
Cloud SP
Services
Obfuscated Data + Sticky Privacy Policies
?
7
Tracing and Auditing Authorities (TAAs)
est for Authorization or Notification

NCLUSIONS

- vantages of cloud computing can bring higher risk to data vacy and security
  - g. Rapid scaling (through subcontracting), remote data storage, sharing services in a dynamic environment
- y user concern, particularly for financial and health data
- sociated lack of trust + difficulties in meeting legal requirements business inhibitor
- e are currently researching the development of solutions
  - Consent management, sticky policies, risk analysis, data obfuscation

Q&A