PRIVACY, SECURITY AND TRUST ISSUES ARISING FROM CLOUD COMPUTING

Siani Pearson* and Azzedine Benameur
HP Labs Bristol, UK
December 2010
BARRIERS TO CLOUD TECHNOLOGY

% of respondents (ranking top 3 barriers)

- Security
- Regulatory risks
- Business case
- Interoperability
- Lack of awareness
- Adjusting policies
- Building skill set

Based on McKinsey Global Survey results: October 2010

© Copyright 2010 Hewlett-Packard Development Company, L.P.
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

© Copyright 2010 Hewlett-Packard Development Company, L.P. 5 January, 2011
IVACY BASICS

Definition – Personally identifiable information

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

- Full name: Mike Smith
- Home address: 123 Main St.
- Home 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

Definition – Sensitive information

Sensitive Information can be considered as a sub-set of personal information, and because of its sensitive nature greater care must be taken in its handling. Use is specially 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.
PRIVACY CHALLENGES

Individuals

solicited marketing

Identity theft

Revealing personal information friends, family members

Behavioral advertising

Intended use or inferences from information

g. from Social Networking data

Government surveillance

Subpoena of information stored “in the cloud”
IVACY CHALLENGES

Businesses

Data breaches can be costly (on average $204 per record, according to 2010 Ponemon Institute study)

Country-specific laws expose companies to a risk of litigation when customers are concerned for the welfare of their privacy it can affect a company's ability to do business.

Negative public attention and loss of brand value

Complexity of managing privacy
IVACY ISSUES FOR CLOUD COMPUTING

Complex information environment
Data flows tend to be global and dynamic
Data proliferation
Dynamic provisioning
Lack of user control
Authorised secondary usage
Intention of data
Has data been properly destroyed?
Have privacy breaches occurred?
Who is at fault in such cases?
How are Security and Privacy Different?

**Personal Information-Handling Mechanisms**
- Dual Rights
- Fairness of Use
- Notice
- Choice
- Access
- Accountability
- Security
- Privacy Laws Also Restrict Border Data Flow of Personal Information

**Protection Mechanisms**
- Authentication
- Access controls
- Availability
- Confidentiality
- Integrity
- Retention
- Storage
- Backup
- Incident response
- Recovery
Privacy relates to personal information

Security and confidentiality can relate to all information

Context is important: different information can have different privacy, security and confidentiality requirements
The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.

**SaaS**

**PaaS**

**IaaS**

RFP/Contract
Build It In

It In
CURITY ISSUES FOR CLOUD COMPUTING

cess control
ntrol over data lifecycle
ailability and backup
ck of standardisation
hit
nerabilities, e.g.
ontnets and trojan horses exist in cloud services
ata theft in cloud
ross-VM side channel attacks

right 2010 Hewlett-Packard Development Company, L.P.
DATA PROTECTION LAWS AROUND THE WORLD

[Map showing data flows and legal barriers]
LEGAL ISSUES FOR CLOUD COMPUTING

cation matters
dicult to comply with legislation specially transborder data flow requirements
ta processors must use ‘reasonable security’
P may be forced to hand over data stored in cloud
uation subject to change
RUST ISSUES
Cloud Perspectives

Cloud Service Provider

You own and manage all of the IT assets
You assume the specific costs and risks of the service components

Two very different roles

Cloud Service Consumer

- 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

Two very different perspectives
PECTS OF TRUST

Studies of on-line trust

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

Copyright 2010 Hewlett-Packard Development Company, L.P.
RISSENT VS. DYNAMIC TRUST

Mechanisms for providing trust

Social

- Brand image, look & feel, reputation, history of interactions

Recommendation

- Sanctions, assurance, vouching, seals of approval

Nature of trust

- Persistent
  - Protocols, well-known practices
  - Underlying security infrastructure, certified hardware

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

Technological
Trust issues for cloud computing

1. Weak trust relationships
   - Non-transitivity of trust, esp. ‘on demand’ models

2. Lack of trust mechanisms need to be propagated right along chain of service provision

3. Lack of consumer trust
   - Due to lack of transparency and control
     - Esp. for sensitive info

Trust key to adoption of SaaS
DRESSING PRIVACY, SECURITY, AND TRUST ISSUES

The different approaches
PORTANCE OF CONTEXT

Privacy need be taken into account only if the cloud service handles personal information, in the sense of collecting, transferring, processing, sharing or storing it.

Privacy 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.

Text 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

Factors: location, sensitivity of data, culture, trust relationships,…
STANDARDISATION

Internationally recognized Computing standards relevant Industry organizations with substantive computing initiatives and programs government and international standards and practices organizations
<table>
<thead>
<tr>
<th>Is</th>
<th>Is Not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driven by global and local</td>
<td>A replacement for other Secure Design Principles and</td>
</tr>
<tr>
<td>regulations</td>
<td>requirements</td>
</tr>
<tr>
<td>Initial set of best practice</td>
<td>Bolted on at end of design process</td>
</tr>
<tr>
<td>design principles and standards</td>
<td></td>
</tr>
</tbody>
</table>
DRESSING ISSUES IN CLOUD COMPUTING

Procedural measures
- determining capabilities of CSP before selection
- negotiating contracts
- restricting transfer of confidential data to CSP

Data security mitigation
- encryption
- mechanisms for increasing trust
- privacy infomediaries, sticky policies, agents

Solutions need to address a combination of issues above => new mechanisms

Copyright 2010 Hewlett-Packard Development Company, L.P.
CURRENT RESEARCH

fuscation

sign patterns

accountability in the cloud

cultural language policies in contract associated with lower-level
chine-readable policies that
define usage constraints of the associated PII
transmitted through the cloud associated with PII
itted 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 Controller
- PIA Process
- Stakeholder Concerns
- Risks of technology
- Risks of PII or processing

Data Subject
- 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)

EVLONING CLOUD ACCOUNTABILITY (or TRUST) STANDARDS
CONCLUSIONS

Advantages of cloud computing can bring higher risk to data privacy and security.

- Rapid scaling (through subcontracting), remote data storage, sharing services in a dynamic environment
- User concern, particularly for financial and health data
- Associated lack of trust + difficulties in meeting legal requirements
- Business inhibitor

We are currently researching the development of solutions.

Consent management, sticky policies, risk analysis, data obfuscation
Q&A