Cloud computing—the use of contracts as a means of governing networked computer services.

Kevin McGillivray
PhD Research Fellow, UiO
kevin.mcgillivray@jus.uio.no
Agenda

• Introduction to cloud computing
• Legal issues
• Project focus and RQs
• COCO Clouds EU Project
Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Resource Pooling

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Public
Private
Hybrid
Community

Essential Characteristics
Delivery Models
Deployment Models
Control over delivery models

http://www.nist.gov/itl/cloud/
http://www.nist.gov/itl/cloud/
Central issues in Cloud Computing

- **Lack of control**: availability, security, vendor lock-in (data-hostage clauses etc), confidentiality, access by law enforcement

- **Transparency**: What is happening at the different layers of the service?
  - Differences from outsourcing

- **Shared Infrastructure**: trust

- **Compliance**: data and consumer protection laws, government data, financial or health data, interception/communications regulations

- **Legal**: Contract law, IPR, tort, conflicts of laws etc.
Why is cloud interesting from a legal research perspective?

- **Location of Data** ➔ Relevance for the service vs. Relevance for national laws (DPL etc.)
  - Application of national law?
  - Access by national authorities
  - What liabilities are taken up along the way?

- **Contractual asymmetry** ➔ Cloud consumer vs. CSP

- **Complexity of services** ➔ Allocation of responsibilities (layers and technology)

- **Global data transfers** ➔ Impact on national legal regimes
Jurisdiction

- Jurisdiction may be impacted by the type of legal issue (DPL, tort law, contract law, criminal law).
- At least 4 Possible legal systems applicable
  - (1) Legal system where CSP is located
  - (2) Legal system where cloud client is located
  - (3) Legal system where data is stored
  - (4) If personal data is collected and processed, location of the individual to whom the data concerns.
Legal issues (contracts)

- One-size-fits-all contracting
  - Negotiation is possible, but difficult
  - Most services offered on a take-it-or-leave-it basis

- Attempts to solve all compliance challenges with one contract--not enough attention paid to national laws

- EU concerns: Difficult for users to exercise rights
  - Limited liability
  - Unilateral changes to terms
  - Choice of law and choice of forum
“As is” service is the norm

• Disclaimer of all warranties and limitation of liability common
• Disclaimers often extend to all partners/subcontractors
• What is the warranty worth?
Direction of Contracts

• **Outsourcing**
  – “One-direction”
  – Traditional IT outsourcing purchaser had more bargaining power
  – Long negotiation periods common in IT outsourcing
  – Audits common in IT outsourcing

• **Cloud**
  – More complex contracting structure
  – Synchronizing terms in existing structure
Cloud Consumer

CSP

Secondary Data Center

Servers (Amazon/Google etc.)

Third Party Apps./soft

No-K

K

K

K

K
Sub-contracting/ Partner concerns

- Services are often layered / complex
- How widely are data being shared (servers, software etc.)? How is the data being used by 3rd parties or “partners” at each layer?
- Is personal data accessible?
- Difficult to perform audits (multiple copies, partners change, located globally)
- Deletion challenges
- “In the view of the WP29, the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service.” 3.3.2 Subcontractors.
Responsibilities in the Cloud
Google and the City of LA

CSC

K

City of LA

K

Google (sub-K)

NDA
Common terms—some considerations

- Limits on use of the data (behavioral advertising etc.)
- Level of security
  - “reasonable” vs. a specific standard
  - Does the contract require notice of a breach?
  - Audits, third-party verification
  - Who is responsible for security?
- Data location
- Confidentiality/Access
  - Access by CSP employees
  - Helpdesk employees?
- AUP
- Account suspension/termination events/deletion
- Ownership of data
- Indemnification (Cloud Consumer/CSP)
- Variation of Contract terms
- Choice of law or forum
EU Data Protection in Cloud Computing

- Limits on processing of personal data

- Cloud consumer → Controller
- Cloud Service Provider → Processor (generally)
- Well suited for Cloud?

http://blog.questionmark.com/
Article 17 of Directive 95/46/EC

Security of processing

3. The carrying out of processing by way of a processor must be governed by a **contract or legal act binding the processor to the controller** and stipulating in particular that:

- the processor **shall act only on instructions from the controller,**

- the obligations set out in paragraph 1 [appropriate technical and organizational measures] as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
Data storage

Once a file is added to your Dropbox, the file is then synced to Dropbox’s secure online servers. All files stored online by Dropbox are encrypted and kept securely on Amazon’s Simple Storage Service (S3) in multiple data centers located across the United States. You can find more information about Amazon S3 or learn about Amazon S3’s security measures on the Amazon website. (Dropbox.com)

If you use the Service, you acknowledge that you may be sending electronic communications (including your personal account information and Content), through computer networks owned by Evernote and third parties located in California and other locations in the United States and other countries.” (Evernote.com)
Consider the risks when placing personal data on the cloud

<table>
<thead>
<tr>
<th>Arrangement of the CSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Determine the structure of the cloud service</td>
</tr>
<tr>
<td>• Identify the parties and the role they will play (Controller, processor, sub-processor etc.)</td>
</tr>
<tr>
<td>• Location, roles, access of sub-contractors and partners</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Type of Data (personal, sensitive etc.) and responsibilities</td>
</tr>
<tr>
<td>• Determine obligations that cannot be outsourced to the cloud</td>
</tr>
<tr>
<td>• Differences between delivery and deployment models (IaaS, PaaS, SaaS) (private, public, hybrid)</td>
</tr>
<tr>
<td>• Responsibility for security? Access?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Where will the data be located?</td>
</tr>
<tr>
<td>• If outside the EU, are safeguards in place (SCC, BCR)?</td>
</tr>
<tr>
<td>• Is it possible to audit the activities of the CSP?</td>
</tr>
<tr>
<td>• What does the contract say?</td>
</tr>
</tbody>
</table>
Research Questions

• What role do contracts play as a means of governing, organizing, and enforcing the legal relationships created in cloud computing?
  – Enforcement mechanism + Memorialization of cooperation and relationships

• Is the central role of contracts and self-regulation adequate or should states play a greater role?
  – Private ordering vs. state regulation

• What changes by using cloud? Is cloud a good idea?
How ought the cloud be governed?

Contracts– more “lawful” role
• Modernize agreements
• Compliance with national laws

National laws– more active role
• Update rules→ Clearer compliance standards
• EU→ Change controller processor balance
• “Balkanization” of the cloud

International treaty?
Increased self and voluntary regulation?
• Future of private ordering
• Architecture/Standards (Self-regulation)
• Role of industry and third-parties
• **ISO/IEC 27017** — Information Security management for cloud systems (in Development)
• **ISO/IEC 27018** — Data protection for cloud systems (in Development)
CONFIDENTIAL AND COMPLIANT CLOUDS

To facilitate the writing, understanding, analysis, management, enforcement and dissolution of data sharing agreements.

- "My data cannot be accessed outside of the EU"

To consider the most appropriate enforcing mechanisms.

To address key challenges for legally compliant data sharing in the cloud.

http://www.coco-cloud.eu/
Compliance by Design

- Fair and Lawful Processing
- Proportionality
- Minimality
- Purpose Limitation
- Data Subject Influence
- Data Quality
- Data Security
- Sensitivity
Compliance Requirements may depend on the type of data

eHealth Pilot- sharing highly sensitive medical data such as medical images and their corresponding reports;

eGovernement Pilot- sharing of civil data of citizens between and across different Italian Public Administrations;

SAP Mobile Sharing Pilot- confidential business information shared over a mobile network.
Sources of compliance

- Data privacy laws
- Contracts
- IP laws
- Confidentiality rules
- Rules specifically applicable to government-held data
DSA: making the distinction

Data shared → Data type

- IP protected → Licensing
- Personal data → Controller-to-controller, Controller-to-processor
- Confidential information → Non-disclosure agreements
Selected References

EU


Articles

- W. Kuan Hon, Christopher Millard & Ian Walden (2012), 'Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now', STANFORD TECHNOLOGY LAW REVIEW, 16 (1), 50.