Cloud Computing –
The Legal Background

Kuan Hon
Consultant, Cloud Legal Project
Centre for Commercial Law Studies
Queen Mary, University of London
http://cloudlegalproject.org / w.k.hon@qmul.ac.uk

Personal: @kuan0 | http://kuan0.com
Outline

- Introduction
- Cloud computing features
- Legal issues
- Questions/comments – end only
Introduction

- **Cloud Legal Project**
  - CCLS autumn 2009
  - [http://cloudlegalproject.org/Research](http://cloudlegalproject.org/Research)

- **Personal**

- **Attendees**
  - users, developers, providers, lawyers?
Legal background

- Rights
- Responsibilities – legal obligations, liability
- Sources – law, regulation, contract
- Application to cloud, & differences
- Perspectives differ – user, provider, developer/provider, data subject etc
But first...
Mindsets: Technologists vs Lawyers
Technologists
Technologists

1100
1010
0101
Lawyers
Interpreting the interpreters

Legislation X

Case A:
‘X means…’

Case B:
‘Case A means…’
Length of the Chancellor’s foot
The Denning Dimension

“The little old lady wins!”
Certainty? Hah!

‘It depends…’

Interpretation
Context
Probabilities
pity

...let’s kill all the lawyers!
Ask an English lawyer about other countries’ laws…
Ask a divorce lawyer about *IP* law…
Ask a GP, or bowel surgeon, to operate on your brain?!
Laws & the internet...
UK, EU
CLOUD COMPUTING FEATURES
So, what *is* cloud computing?

- Use of **IT resources** over a network (e.g., internet), scalable on demand.
- US NIST definition, and service models:
  - **Software as a Service (SaaS)** - apps
    - *Incl.* Storage as a Service (also SaaS!)
  - **Infrastructure as a Service (IaaS)** – compute, storage
  - **Platform as a Service (PaaS)** – app development/hosting platform
Deployment models: private, public and hybrid clouds... **community clouds**
Models - 4 key points

- User expertise required – SaaS to IaaS
- Spectrum, not distinct – esp. IaaS / PaaS
- Classification may depend on viewpoint

User ---- DropBox ---- Amazon

SaaS       IaaS

- Ecosystem of players – which component / service?
Cloud layers/‘stack’ – different possible architectures, possible hidden layers

---> **Who** holds user’s data? **Where?**

- **Infrastructure as a Service (IaaS)**
  - Physical infrastructure for each!

- **Platform as a Service (PaaS)**

- **Software as a Service (SaaS)**

Key cloud computing features relevant to legal analysis

- Multiple providers? (layers)
- Data replication, deletion
- Sharding/chunking/fragmentation
- Location – multiple; changing?
- Design - provider access; encryption
- Use of/dependence on shared, third party resources, incl connectivity
LEGAL ISSUES
Who owns data in the cloud?

- Information 'Ownership' in the Cloud, Reed
- ‘Ownership’ of digital data
- Data created outside the cloud
  - 3 C’s and a D
- Data created in the cloud
  - By cloud user
  - By cloud provider
- Contract terms
Running applications in the cloud

- Running patented software on US servers?
- Open source software
  - run vs distribute/release
  - Afferro GPL licence
Other IP law issues - infringement?

- Database right – ‘re-utilisation’ - which country?
  - Of uploader, server, and/or recipient?
  - Football Dataco v Sportradar - ECJ
    - mere accessibility…
    - ‘at least’ recipient’s country, iff targeted
    - uploader/server?
  - Broader application?

- Takedown of infringing content – as per ‘normal’ sites? Copies?
Data protection law – foundational issues

- **What?** - “personal data”
- **Who?** - responsibility
- **When?** – applicability of laws
- **Where?** – location (& **how** – transfer)

- **Issues may differ** – user, provider, data subject
Data protection - law vs IT

“Data protection” (law)

“Technical & organisational measures”

IT security & IT “data protection”
What information is regulated – “personal data” in the clouds

- Significance of “personal data” definition
- Anonymised data, encrypted data
  - What is “good enough”?
- Fragmented data
- Anonymisation/encryption procedure
- Suggestions:
  - Status of encrypted data; encryption etc procedures
  - Realistic risk of identification/harm
Who is responsible for personal data in the cloud?

- Controller vs processor - significance
- Cloud user
- Cloud provider(s) – metadata; access?
- What *should* provider’s status be?
  - E Commerce Directive-style defences for infrastructure providers (unless access + control)
  - End to end accountability (instead of binary controller/processor distinction)

When do EU data protection laws apply to a non-EEA cloud user/controller?

- “EEA establishment” + ”context” - incl. through third party
- Public international law
- “Use” of EEA “equipment”
  - Cookies (“equipment”) – SaaS
  - EEA data centre/provider?
- Even within EEA…
Where can “personal data” be located?

- UK Government’s ICT Offshoring (International Sourcing) Guidance, 2011 - data location restrictions
  - national security
  - data protection laws

- Data protection:
  - data protection laws - all sectors, sizes
  - transfer restriction - EEA only unless “adequate protection” or specific exception
  - “transfer” - remote access
EEA, EU, Europe…

(for large version & table listing countries)

©Kuan Hon (2012), licence: http://creativecommons.org/licenses/by-nc-sa/2.0/uk/
“Adequate protection”

- How? Who decides?
- Approved methods to achieve
- ICO – controller decides (cf others)
- Now vs future…
“If we include entities outside the European Union, the data transfer that is inevitable with cloud computing — and which has no legitimacy under data privacy law — makes clouds inherently impermissible.”

German regulator Thilo Weichert
“The DPA does not prohibit the overseas transfer of personal data, but it does require that it is protected adequately wherever it is located and whoever is processing it. Clearly, this raises compliance issues that organisations using internet-based computing need to address.”

UK Information Commissioner (“Personal Information Online”)
How can personal data be transferred outside the EEA? - 1

- Whitelisted countries
  - a short list

- US Safe Harbor –
  - applicability - “processors”; layers/sub-providers & onward transfers
  - restricted - non-US/EEA data centres (Danish DPA)
  - adequacy - concerns
How can personal data be transferred outside the EEA? - 2

➢ BCRs
   ○ within group only, time/costs

➢ Model clauses – as is, no changes; if layered?
   ○ For EEA customer using a cloud provider –

<table>
<thead>
<tr>
<th>Provider</th>
<th>Sub-provider</th>
<th>Covered by model clauses?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-EEA</td>
<td>Non-EEA</td>
<td>Yes</td>
</tr>
<tr>
<td>EEA</td>
<td>Non-EEA</td>
<td>No</td>
</tr>
</tbody>
</table>

Queen Mary University of London
Centre for Commercial Law Studies
So, in practice… regional clouds

- Can users choose their data’s location?
  - No choice
  - In practice…

- Regions? - increasingly
  - EEA ≠ EU ≠ Europe – Danish DPA (Google)
  - *Contractual* commitment? Amazon...
  - Verification of location? Trust
But even *within* the EEA…

- Establishments / data centres in *multiple* EEA Member States?

- **Obstacle**: lack of harmonisation, inconsistencies/conflict - eg security requirements

- Abolish?

- Full paper
  
Law enforcement access to cloud data

- Requests to *providers* for user data
  - system design, user encryption?
- US PATRIOT Act - bogeyman?
  - all countries…
  - providers’ terms: rights; scope; notice
  - data protection law: export, & ICO cloud guidance
- Walden’s Cloud Legal Project paper, ComputerWorldUK summaries
The future...

- Regulators’ guidance in July 2012
- ICO guidance Sep 2012
- Draft Data Protection Regulation
- Not very cloud-appropriate!
  - QMUL press release, papers
Meanwhile, in practice

- Location, location, location
- Encryption, encryption, encryption
  - Limitations – speed; value-add; operations
  - Key management critical
- Contract, contract, contract (next…)
- Contract - procurement
  - Internal controls
  - Due diligence
Cloud contract terms - introduction

- Legacy of consumer web services – ‘off the shelf’ cloud computing
  - Providers' standard terms
  - Click-through - easy, quick, free / credit card
  - Users’ internal procurement

- Cloud Legal Project research
  - 2010 - standard cloud providers' terms
  - 2012 - negotiated cloud contracts
Some possible contractual structures
- 2 types of users

Dotted line means, may (or may not) exist
Cloud contracts

- “Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services”, Bradshaw, Millard & Walden

- 31 sets of standard T&C (defined broadly)

- Key issues include:
  - Complexity & multiple dependencies
  - Predictability
  - Inappropriate / unenforceable / illegal
General findings

- Liability
- Disclaimers
- Choice of law and jurisdiction
- Change/terminate service, terms
- Data recovery following termination of service
- Subcontracting
- IP rights
<table>
<thead>
<tr>
<th>Choice of law specified by cloud provider...</th>
<th>Number *</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>US State</strong>: California (most common), Massachusetts (Akamai), Washington (Amazon), Utah (Decho), Texas (The Planet)</td>
<td>15</td>
</tr>
<tr>
<td><strong>English law</strong>, probably because service provider based there</td>
<td>4</td>
</tr>
<tr>
<td><strong>English law</strong>, for customers in Europe / EMEA</td>
<td>4</td>
</tr>
<tr>
<td><strong>Other EU jurisdictions</strong> (for European customers): eg. Ireland (Apple), Luxembourg (some Microsoft services)</td>
<td>2</td>
</tr>
<tr>
<td><strong>Scottish law</strong> (Flexiant)</td>
<td>1</td>
</tr>
<tr>
<td><strong>The customer's local law</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>No choice of law expressed or implied, or ambiguous choice</strong> (eg. “UK Law” for g.ho.st)</td>
<td>3</td>
</tr>
</tbody>
</table>

* Number in each category is out of 31 contracts analysed by QMUL Cloud Legal Project
http://www.cloudlegal.ccls.qmul.ac.uk/
Negotiated contracts research


- Methodology - Dec 2010 to early 2012
  - Detailed “no names” interviews
  - Cloud providers / users / others (including integrators and law firms)
  - FOI requests
Why do users seek changes?

- Provider-favourable terms
  - Though not always
- Commercial, eg SLAs, risk allocation
- Legal / regulatory compliance, esp.
  - personal data
  - financial services
Can users negotiate successfully?

- User's position - bargaining power
  - Esp financial institutions, government - *their* mandatory standard terms, eg UK G-Cloud
  - Mostly confidential, but eg Google / City of LA; Cambridge U

- Provider's position

- Cloud is only part of larger deal

- NB integrators – risk of mismatch
Top 6 issues in negotiated cloud deals

1. Exclusion / limitation of liability
2. Service levels
3. Security and privacy, incl DP
4. Lock-in and exit
5. Providers' rights to modify service unilaterally
6. IPRs
Summary - signs of market changes

- Customer-appropriate vs cloud-appropriate -> fudge - user risk (eg regulatory) **or** provider agrees meaningless / impossible terms
- High end (user demand) + low end (regulatory / consumer protection action) + increasing provider competition -> standard terms shift?
- Education - lawyers, policymakers, even IT channel (not software licensing, product sales, traditional outsourcing)
- Industry standards and certifications - and legal / regulatory recognition for compliance purposes
UK G-Cloud programme v1

- Framework agreement + call-off contracts
- Overlay approach – provider's terms + overriding terms
  - US gov social media sites
  - risks
- Issues with v1
  - *which* provider terms
  - substantial / material amendments – public procurement law
  - provider can change terms!
- v2 – restricts changes, but clarity…
- Full paper available
Other legal issues…

- Competition law - **lock-in** vs interoperability / portability, standardisation efforts
  - CLP paper

- Etc etc…
  - Running software in the cloud -
    - Export control? *(eg. use of cryptography)*
  - Tax?
  - Derivatives? *(cloud markets)*
Cloud users – practical questions

- Cloud use/migration - what, how, when, why, who (incl. layers), where?
- Shop around; multiple providers?
- Due diligence – for *particular* intended use
  - Incl. system design, certifications, financial, data portability/deletion
  - Legal / security / risk assessments – involve early, inform fully – ENISA papers
  - Contract terms – check, negotiate? Own end users?
- Self-help - own security measures, backup; insurance? Monitoring, audits?
Cloud providers – practical questions

- Regulatory review of contract terms
  - suitability for intended users, users’ compliance needs
  - competitive advantage?
- Pre-contractual disclosures/transparency
  - security, sub-providers, locations
- Tools for users – monitoring location etc
- More broadly:
  - Education / awareness
  - Industry standards and third party certifications
Making life easier?

LAST YEAR WE RECOGNIZED THAT OUR PROCESSES WERE FAR TOO COMPLEX

SO WE PUT THEM INTO THE CLOUD

LET THE CLOUDS MAKE YOUR LIFE EASIER

By Oliver Widder, [Geek and Poke](http://www.geekandpoke.com).

Queen Mary, University of London

Centre for Commercial Law Studies
Forecast: cloudy and changeable… but bright!

- Benefits – but unintended consequences…
- Legal / regulatory obligations continue
- Physical location
- Differences in cloud service providers
- Risks of compelled disclosure and other external disruptions
- Regulators and lawmakers…
- Cloud contracts evolution – customers, competitors, regulation, cases
References and further reading

- CLP research - http://cloudlegalproject.org/Research
- Including links to some resources – http://bit.ly/cloudlinks
- Future CLP papers
  - Consumer protection
  - Cloud governance
Thanks for listening!

Any questions…

Kuan Hon
w.k.hon@qmul.ac.uk

Personal:
@kuan0 | http://kuan0.com