CERN 13 May 2014

Negotiating Cloud Contracts
+
UK G-Cloud i Case Study

Kuan Hon

Research Consultant, Cloud Legal Project
Centre for Commercial Law Studies
Queen Mary, University of London

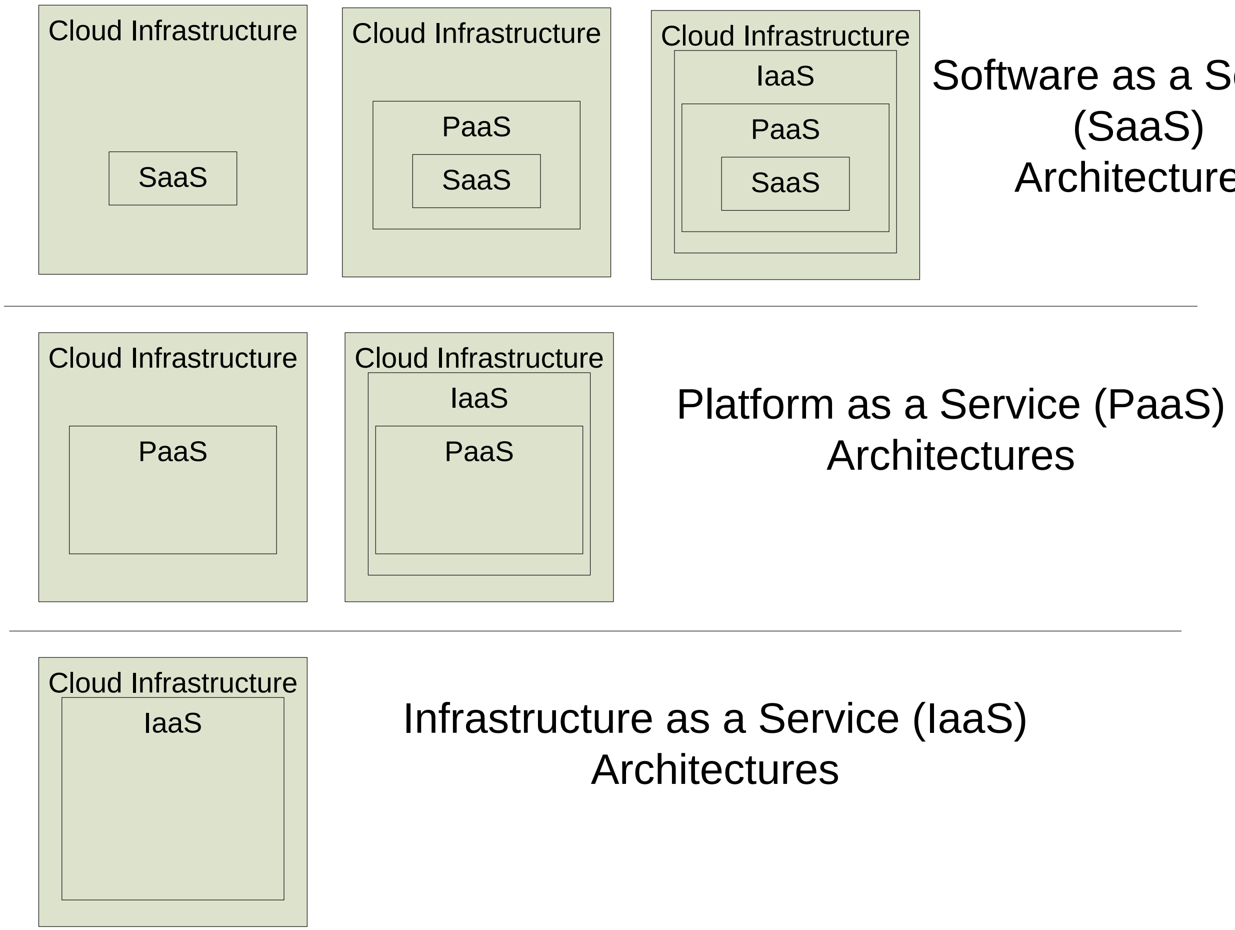
w.k.hon@qmul.ac.uk

Queen Mary
University of London
Centre for Commercial Law Studies

Overview

- Self
- Cloud Legal Project
  - Millard (ed), Cloud Computing Law (OUP 2013), chapters 3 – 5 (incl UK G-Cloud)
    - including cheap Kindle edition
- A4Cloud paper ; MCCRC
- This session – intro, negotiations, G-Cloud

Cloud layers / “stack”– different architectures, possible hidden layers –> **Who** holds user's data? **Where?**



Cloud Infrastructure
SaaS

Cloud Infrastructure
PaaS
SaaS

Cloud Infrastructure
IaaS
PaaS
SaaS

Software as a Service (SaaS) Architectures

Cloud Infrastructure
PaaS

Cloud Infrastructure
IaaS
PaaS

Platform as a Service (PaaS) Architectures

Cloud Infrastructure
IaaS

Infrastructure as a Service (IaaS) Architectures

+ SaaS on IaaS

+ cloud “platform” software infrastructure + physical infrastructure for each

From
http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt

Queen Mary
University of London
Centre for Commercial Law Studies

Models - 4 key points

- Varying user expertise needed – SaaS to IaaS
- Spectrum, not distinct – esp. IaaS / PaaS
- Classification may depend on viewpoint

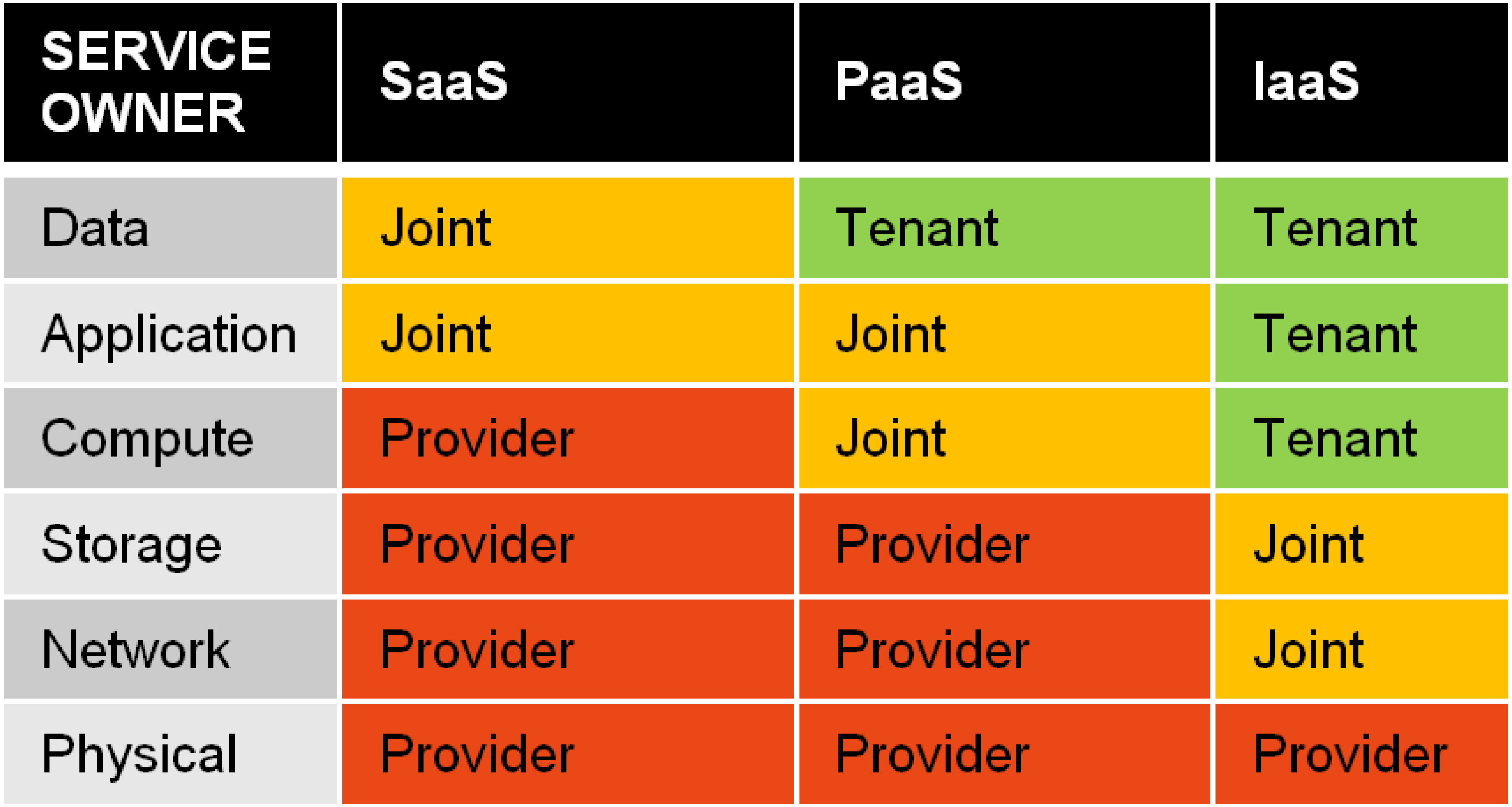
User ---- DropBox ---- Amazon

SaaS IaaS

- Ecosystem of players – which component / service?

Control *not* always completely lost

- Differing degrees of control – not one size fits all
- Self-help – firewalls, encryption / tokenisation (keys),



SERVICE OWNER	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Table © Cloud Security Alliance reproduced with permission

Key characteristics

- Combo term – analogy: cooking
- Componentised – hardware, software etc
- Cake (layer) – layers of services possible
- Commoditised, Common Infrastructure (public)
  - Shared resources – same hardware, app instance, DB / table
- Cook-it-yourself – self-service
- Cost (not necessarily cheap, you get what you pay for)
- Control – degrees differ
- Country of location – & compliance
- Customers, especially consumers – importance, education
- Competition & competitiveness, lock-in
- Comparisons – certifications ?
- Contracts – standard terms, negotiation ?

http://www.scl.org/site.aspx?i=ed26082

Key differences from traditional outsourcing

- Disassociation or abstraction – physical vs logical
- Diverse supply chain – hardware, software, *services*
- Don’t always know or have influence over all suppliers
- ‘Direction of travel’ reversed
- DIY – self-service
- Design - affects access / control by users, sub-providers
- Data
  - distributed
  - divided into fragments
  - duplicated – to different locations, changing ?
  - ‘deletion’
- Dependence – on shared third party resources incl connectivity
- Degrees of control

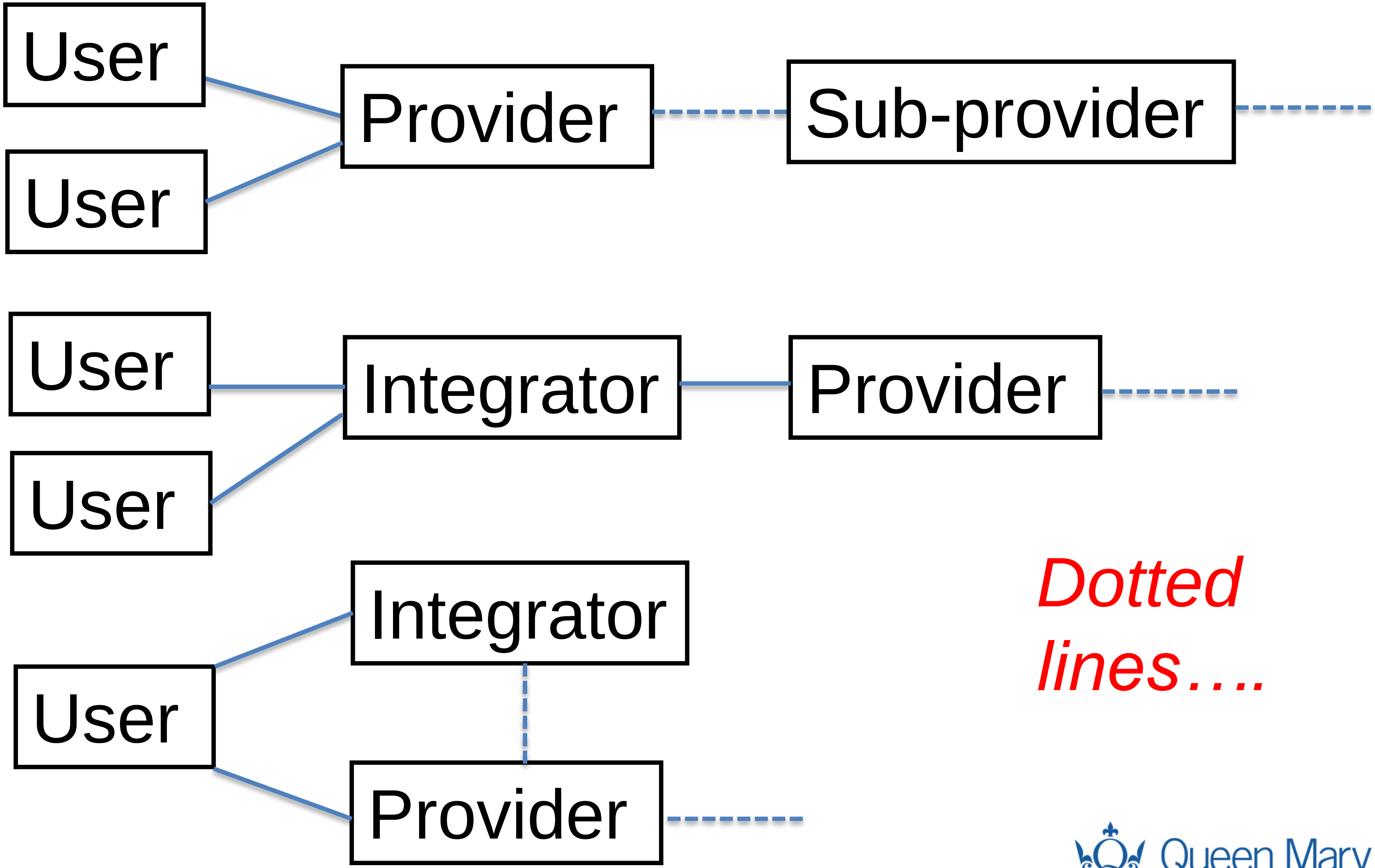
http://blog.kuan0.com/2014/02/9-ds-of-cloud-computing-what-different.html

Key aspects relevant to legal analysis

- Shared third party resources
- Multiple players / layers
- Data storage
- Data location
- Design – provider access ?
- User control
- In practice – functionality, security, legal / regulatory compliance
- Extent of cloud personal data processing at CERN?

Cloud contract terms

Common contractual structures/usage models: 2 kinds of users



Dotted lines….

Queen Mary
University of London
Centre for Commercial Law Studies

Cloud contract terms - introduction

- Consumer web services legacy: ‘off the shelf’ cloud computing
  - Providers' standard terms
  - Click-through - easy, quick, free / credit card
  - Users' internal procurement procedures…
- Cloud Legal Project research
  - 2010 - standard cloud providers' terms
  - 2012 - negotiated cloud contracts

Standard terms – summary of findings

- "Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services" - Bradshaw, Millard & Walden (2010) - updated in 2013 (book)
- 31 sets of standard T&C (defined broadly)
  - ➢ Each mapped against 20 main categories
- Key findings included:
  - ➢ Pay more, get more !
  - ➢ Arrangements' complexities rarely addressed properly
  - ➢ Inappropriate / unenforceable / illegal terms

Queen Mary
University of London

Centre for Commercial Law Studies

Standard terms – key specific risks

- Liability exclusions / disclaimers
- Provider's sub-contracting
- Change / discontinuation of services
- Data recovery after termination

- Enforceable ?
    - consumers; unfair standard terms

Why do users seek changes?

- Provider-favourable terms
  - Though not always
- Commercial - eg SLAs, risk allocation
- Legal / regulatory compliance - esp.
  - ***personal data - data protection laws***
  - ***financial services***

Can users negotiate successfully?

- **User's position**
  - Esp. financial institutions, government
    - insist on own terms !
  - Mostly confidential, but eg Cambridge U
- **Provider's position**
- NB **integrators** – risk of mismatch

Negotiated contracts research

- “Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now” – Hon, Millard & Walden (2012) or http://bit.ly/negotiatedcloudcontracts - slightly updated in book – & later in 2014
- Methodology - Dec 2010 to early 2012
  - ➢Detailed “no names” interviews - anonymised
    - o Cloud providers / users /others (including integrators and law firms)
  - ➢FOI requests

Top 6 issues in negotiated cloud deals

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

Liability

- Standard: exclude / limit provider's liability
- Difficult even for very large users
- Deal breaker, but some liability negotiated…
- Only for defined types of losses, with caps
- Liability for breach of confidentiality / privacy / data protection – esp. integrators
- Data integrity / backups (& solutions)
- User’s own liability – integrators etc

Service level agreements

- Commercial, pricing-related
  - varied; may be high anyway
- Lack of standards to measure / compare
- Mission-critical / real-time applications
  - higher availability, more notice, etc
- Monitoring service levels – provider site, tools
- Remedies for breach of SLAs
  - restricted - service credits, types of failure, time limits
  - some monetary rebates
  - more negotiable than service levels

Data protection laws – contract issues

- Most negotiated data protection terms:
  1. data location
  2. data confidentiality (then)
  3. data processor agreement
  4. role of sub-providers
- ‘Personal data’ only (cf anonymous data), but some issues of broader relevance
- Article 29 Working Party WP196

Confidentiality

- User data disclosed in negotiations
  - NDA / confidentiality obligation
- Confidential data processed in the cloud (possibly including third party's data)
  - confidentiality obligation
- Survival of obligation after termination – 5-7 years, forever…

Disclosure of user's data

- Does provider have access to user’s data?
- Explicit contractual rights to access, eg support
- Users may seek to restrict
  - usage monitoring – but billing…
  - ***use*** of resulting information
- Law enforcement request / subpoena, court order
  - right to disclose on order, even request – standard
    - PATRIOT Act fears; recent US warrant for emails stored in Ireland
  - obligation to notify request, so user can challenge?
  - partners with datacenters in different countries?

Security - general

- Users’ biggest concern, esp financial institutions
- What security measures, who should take them?
  - NB self-help – backups, encryption / tokenisation
- Pre-contractual pen testing (ongoing is rare):
  - impact on provider’s service
  - possible solutions
    - provider's own test
    - user testing allowed, under specific agreement
    - certifications eg SSAE16, ISO 27001 – now draft 27017, 27018 (code)
- Security undertakings
  - to comply with whose security policy?
  - industry standard certifications?

Security – audit rights

- Rights to logs – eg Brevo
  - ➢ provider tools – sufficient for some; trust and transparency
- Audit rights – though shared multi-tenant…
  - ➢ esp. financial institutions / integrators with regulated clients
  - ➢ personal data - sub-providers, even data centres (WP196)
- Otherwise, must rely on undertakings:
  - ➢ “The only way to find out if they have actually complied is if they have a major breach or loss of confidential information!”
- Practical compromise – provider’s third party audit?
- Should laws recognise third party audits to industry standards for compliance purposes ? - incentives

Security breaches

- Standard – no obligation; won’t agree unless eg telcos
  - Possibly for operational reasons – systems
- Users may seek:
  - undertaking to monitor / detect breaches
  - undertaking to notify user
  - right to give notice to remedy + right to terminate
- Possibilities - promptly notify affected users only?
- Post-breach actions
  - covered by standards if agreed
  - joint action unlikely

Lock-in and exit – different aspects

1. Initial term - eg 3 years
2. Exit strategy - termination, insolvency etc
3. Dependence on proprietary service, data / metadata formats
4. Practical dependence - developers

Term and termination

- Initial minimum term (1-3 yrs) cf “pay as you go”
  - automatic renewal / rollover unless terminated by notice
- Provider’s rights to terminate / suspend
  - eg insolvency, material breach – terminate / suspend
  - restrict to non-payment? esp. user with end users (“rogue user”)
  - NB Acceptable Use Policies & provider’s right to change
  - compromise ?
- User’s rights to terminate
  - termination for convenience – not always; notice periods
  - material breach, breach of confidentiality, security policy, IPRs…
  - change in control of provider, if required by regulator etc

Data retention

- During term
  - regulatory, litigation, law enforcement, e-discovery / disclosure, preservation of evidence
- After termination
  - Grace period
  - Ease of process
  - Return if requested (cf self-service retrieval)
  - Assisted migration obligation? (eg different format)

Data deletion after termination

- No provision, or only if requested
  - ➢ degrees of “deletion” – from where, to what standard ?
- Obligation to delete permanently everywhere ?
  - ➢ esp. if personal data, sub-providers
  - ➢ reasonable endeavours to erase from media etc ?
  - ➢ personal data - Microsoft Article 29 Working Party letter – changes: commitment to delete within certain period
- Evidence of deletion
- Deletion *during* term
  - ➢ or quarantine; also user awareness / education

Unilateral service changes / termination

- Enterprise-oriented providers more likely to agree to restrict (or already restrict this)
- SaaS commodity services
  - no choice?
  - but qualification re. not adversely affecting service; termination right?
- IaaS / PaaS
  - user may have to update application code
  - core services – consent / notice
  - materially detrimental changes

Intellectual property rights

- Common splits – but issues:
  - user-developed IaaS / PaaS applications ? - user application vs provider's platform / tools
  - customisations, user-contributed improvements ?
  - assignment to provider / exclusive use period; user consent for provision to other users / “competitors”
- Third party applications – licences?
  - included with service, or port user’s own licences ?
    - logging VM numbers / locations problematic
  - licensing basis matching ?

Market is changing…

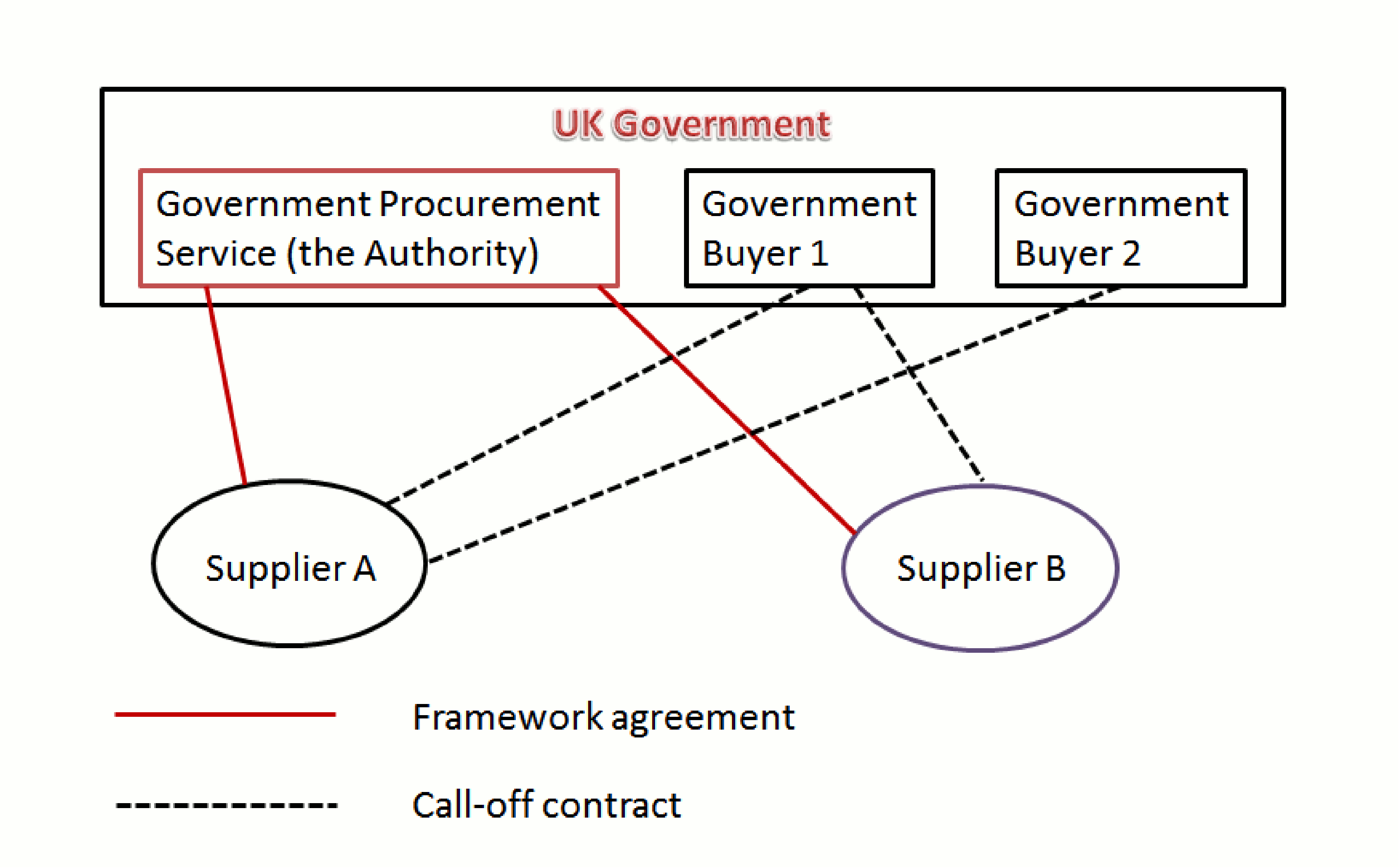
- Providers’ terms not sufficiently customer-appropriate, users’ terms or requests not sufficiently cloud-appropriate…
- Resulting fudge - user takes risk (eg regulatory), or provider agrees meaningless / impossible terms
- User demand at high end – educating providers, should filter down to middle market
- Regulatory / consumer protection action at low end – should filter up to middle
- Increasing provider competition – terms as differentiator – signs of localisation
- Education of lawyers, policymakers, even IT channel needed – not software licensing, product sales, traditional outsourcing
- Industry standards and certifications needed - and legal / regulatory recognition for compliance purposes

UK G-Cloud i

UK G-Cloud programme

- Commercial Workstream 2011
  - didn't draft G-Cloud documentation
- UK G-Cloud v1 and the impact on cloud contracts - Hon, Millard & Walden (2012)
  - updated version, incl Gi to Giii, in book
- First procurement Gi – live Feb 2012
  - Chant: 'the fastest framework procurement in UK government'
- Sales - > £150m total, to end Mar 2014
  - Not sales, but ***savings*** – McDonagh: '…seeing 50-90% savings by adopting cloud. …total cost of ownership.' Chant estimated that Government saved £90 million in the first year of G-Cloud. Dept of Health web hosting £0.8m to £25k - SME

Contractual structure



G-Cloud procedure

- 4 lots – IaaS, PaaS, SaaS, ‘specialist’ (not software)
- Rolling – every 6 months – Gi, Gii etc; Gv 22 May 2014
  - Reason – refresh; iterative, so refinements for lessons learned
  - Differences eg max call-off duration (1 -> 2 yrs), contract terms
- Suppliers - application – docs, incl supplier terms
  - Assurance; [accreditation – later]; award
- Buyers – CloudStore – not click’n’buy; poss complexity
- Contractual documents per provider
  - Framework Agreement
  - Provider’s standard terms
  - Call-off contract(s) / ‘order form’ – NB blanks

UK G-Cloud – issues / risks

- Overlay approach – provider's terms + overriding terms
  - ➢ as per US government approach to social media sites
    - derived from Commercial Workstream, but no full follow-through
  - ➢ Framework Agreement > Call-Off Agreement > completed Order Form [> Collaboration Agreement] > provider’s terms ‘as set out in the Framework Schedule 1 (G-Cloud Services)’ > ‘any other document referred to in the Clauses of this Call-Off Agreement’
- Risks
  - ➢ gaps, arguments
  - ➢ public procurement law – not overlay - next

UK G-Cloud – public procurement law

- Changes in contract terms - *between* OJEU and awards
  - ➢ eg Gi liability provision; Gii 'best endeavours' to 'reasonable'
- Changes in contract terms - afterwards?
  - ➢ Material change requiring fresh procurement for validity ?
    - ○ FW-6.4 Subject to the Authority's Approval (that shall not be unreasonably withheld or delayed) the Supplier **may vary, but not materially change,** the Catalogue entries with any new reduced prices and/or **Service Definitions** in respect of all Orders placed thereafter…. **Once the G-Cloud Services have been ordered by a Contracting Body**, the Supplier hereby **undertakes to maintain the Supplier Terms** as at the time of the Order and for the duration of any Call-Off Agreement.
  - ➢ 'order form' too…

UK G-Cloud – security

- Security accreditations
  - IL0 OK
  - IL1 and above – PGA – CESG
    - ISO27001 – scope ?
    - Updated template
    - Backlog - Cloudstore too
    - Sales & accreditation info
    - Tool to track submissions
- UK gov beta cloud security principles
- UK security classifications system change (summary)
  - Official [was Unclassified, Restricted, Confidential], Secret, Top secret – mapping ?

Queen Mary
University of London
Centre for Commercial Law Studies

UK G-Cloud – other issues

- Transparency…
  - Provider terms on CloudStore – but DPA checklists ?
  - Publication on ContractsFinder ? – some order forms
  - Documents – only registered suppliers - D&B (cf Gi-ii)
- CloudStore to move to Digital Marketplace - in alpha
- Buyer education
  - vs traditional procurements (& risks if new / different terms)
  - multiple suppliers – collaboration agreement? (Gv)
- Providers' open letter Jan 2014
- HMG offer (& CLP on procurement)

Summary

Practical questions for cloud users 1 - general

1. Internal – employees bypassing usual **procurement** procedures?
2. What functions to migrate? – not everything is suitable for cloud
3. Can you stage the migration? – pilots / trials with test (not real) data
4. Minimum / maximum acceptable contract term ? – may affect pricing
5. Can you use different providers, for the same / different functions ?
6. Which specific services / terms incl TOS, T&C, SLAs, Privacy Policy, AUP, etc), from which providers, suit your specific intended use ? – investigate a range; can you even impose your standard terms ?
7. **Legal / security / risk assessments** – involve early, inform fully
8. Worth negotiating (yet) ? – eg (free) pilots/trials; some terms OK
9. Can you get a better deal from others eg integrators ? Community ?
10. Can you insure ? Is coverage scope etc adequate ?
11. NB contracts with **own end users / customers**

Practical questions for cloud users 2 – the service

1. **How well does the service suit your intended use / data ?**
2. Is the infrastructure multi-layered and, if so, in what way? ***Who*** controls the critical infrastructure (and from ***where***)?
3. What info can you get on security: pen testing, certifications etc ?
4. How easily can the provider / third parties access your data, monitor your processing?
5. Where will your data be processed (incl. storage / replication / support; location of any sub-providers, their data centres)?
6. How confident are you that you could regain control of your data without leaving behind copies and / or key metadata ?
7. How easily could you move your data to another cloud service (or back to your own systems), and how long would it take ?
8. What if your cloud provider / their provider goes bust ?

Practical questions for cloud users 3 - other

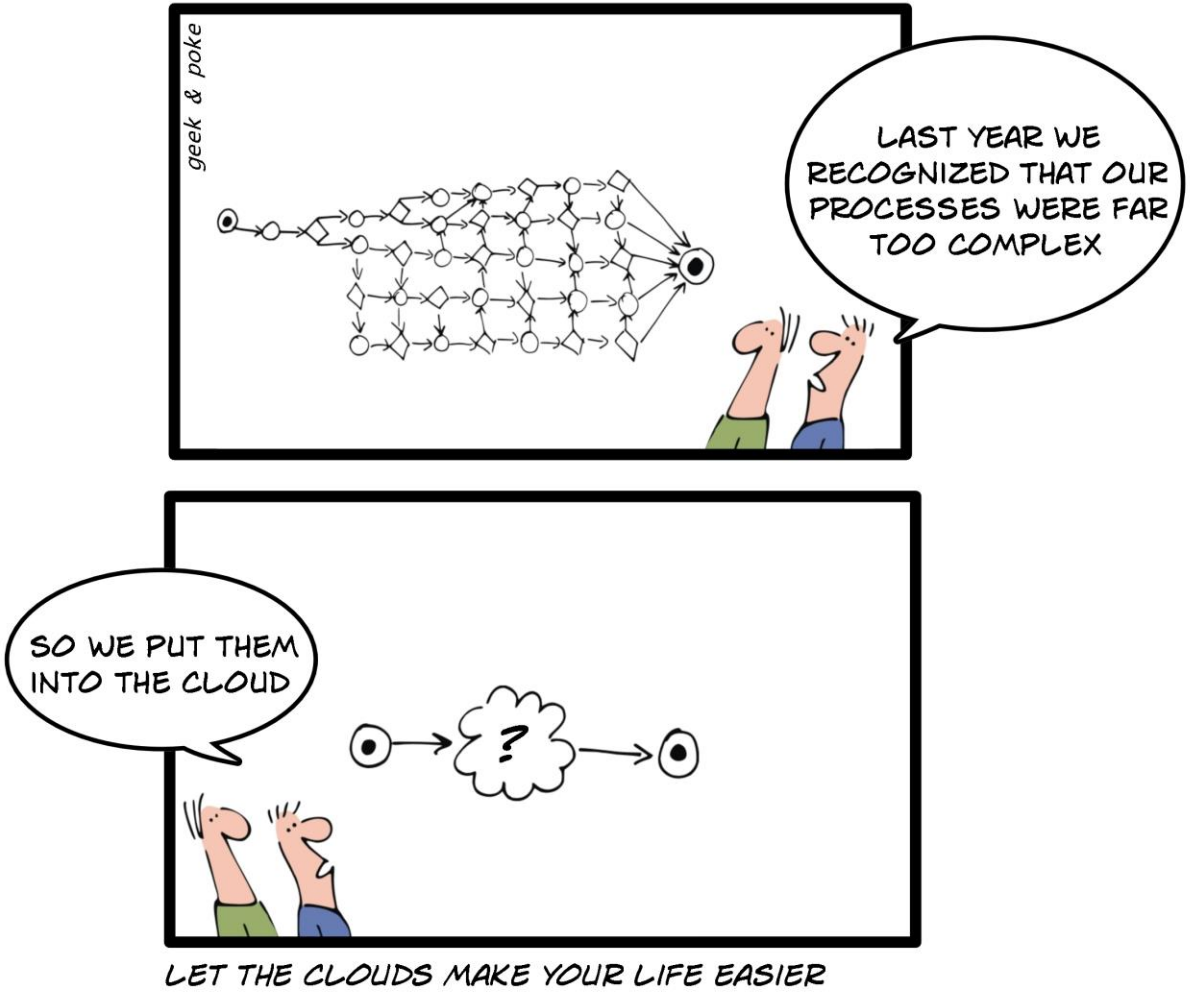
1. Other general pre-contractual due diligence eg -
    1. provider creditworthiness
    2. testing data portability / export, pen testing
2. Post-contract monitoring / checking
    1. audit rights
    2. monitoring tools
3. Don't forget -
    1. network connectivity !
    2. backups
    3. is encryption possible ?
    4. help your lawyers (nature of data, eg personal data; details of intended use)

Key tensions

- “Guaranteed” liability / security
  - ➢ should be possible – but will cost !
  - ➢ cf cheap / free public cloud model

- Control of supply / contract chain
  - ➢will big players be the winners ?

Cloud - making life easier?


geek & poke
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.

Queen Mary University of London

Centre for Commercial Law Studies

Forecast: cloudy and changeable… but bright!

- Putting data / processes into clouds may save money, improve flexibility / agility and facilitate risk management – but it may also have unintended consequences
- Physical location may still be highly significant in virtual environments
- Sophistication and flexibility of cloud providers is highly variable
- Risks of compelled disclosure and other disruptions are real
- Regulators will take a while to get comfortable with clouds, laws will take a while to become cloud-appropriate
- Adoption of cloud services looks set for continued rapid growth
- Cloud contracts are evolving already in response to competitive positioning, customer demands and regulatory / judicial intervention

The way forward?

- User awareness / education
  - guidance + risk assessment checklists
  - self-help - encryption, backup
  - pushback – user demand, market competition
- The future
  - laws / regulation - price vs liability
  - certifications ?
    - devil in detail…incentives for providers ?
  - 3-tier cloud ?

More information

- Cloud Legal Project papers (free download) http://cloudlegalproject.org/Research

Thanks for listening!

Any questions…

w.k.hon@qmul.ac.uk

cloudlegalproject.org

@kuan0 | kuan0.com

Queen Mary
University of London
Centre for Commercial Law Studies