THE LAW OFFICE OF
RICHARD STEPHENS

Cloud Contracting: Key Commercial Terms

by Richard Stephens FBCS FCIArb
Fellow of the Society for Computers & Law

20 September 2016

e: richard@the-lors.co.uk

What are we talking about?

- **Some myths:**
  - Cloud contracting is exactly the same as outsourcing
  - You can't negotiate cloud contracts
  - Cloud contracts are always tilted wildly in favour of the supplier
  - Cloud is just a service – so it gets rid of some tricky legal technicalities
  - Cloud is just the same as the internet
  - Cloud is just the old idea of thin computing
- **Actually some of these things can be true(-ish) – but only sometimes, and not for all types of cloud contract**

The legal bit – the caveats

- **I won't be looking at regulatory or industry specific matters**
  - **Data protection throws up similar issues as in other contracts where your personal data threatens to be sent round the world**
  - **As with outsourcing (and other contracts), there may well be (almost certainly are) sector specific regulations and guidance e.g. the financial or healthcare sectors**
  - **There are many standards emerging as well to do with e.g. security**

What gets negotiated?

- **Interesting article in the Stanford Technology LR (Vol 16 No 1 Fall 2012) by academics from QMUL which named the six most negotiated points in Cloud contracts:**
  1. **exclusion or limitation of liability and remedies, particularly regarding data integrity and disaster recovery;**
  2. **service levels, including availability;**
  3. **security and privacy particularly regulatory issues under the European Union Data Protection Directive;**
  4. **lock-in and exit, including term, termination rights, and return of data on exit;**
  5. **providers' ability to change service features unilaterally; and**
  6. **intellectual property rights**

Are those clauses in the right order?

- I can understand lawyers would obsess over limits and exclusions of liability but …
- In practical terms, what users would notice most would be providers changing the service without notice and failure to keep to service levels
- Cloud transactions have become complex, and many providers are only aggregating a whole series of interlocking (or not) sub-contracts – the more parties there are, the greater the number of points of failure

What types of cloud are there?

- The US National Institute of Standards and Technology defines three separate cloud service types and also 4 deployment models
- It is worth taking a look at the NIST document – you can get it at the following location:
  - http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- Unfortunately, cloud is much hyped – true of the IT industry in general, nothing new under the sun!
  - The 90's saw the growth of Application Service Providers
  - cloudforce.com has been offering CRM software from the cloud since 1998

Type 1 – Software as a Service

- **SaaS is described by the NIST as follows:**
  - **"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings."**
- **A cloud infrastructure is described as follows:**
  - **"A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer."**

Type 2 – Platform as a Service

- **PaaS is described by the NIST as follows:**
  - **"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment."**

Type 3 – Infrastructure as a Services

- **IaaS is described by the NIST as follows:**
  - **“The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).”**

What's it worth?

- Lots of figures is you search on the internet e.g.
  - The global cloud computing market grew 28% to $110bn in 2015
  - Amazon Web Services generated $7.88bn with Q4 in 2015, up 69%
  - Global PaaS market projected to reach $7.5bn by 2020
  - By 2020, penetration of SaaS vs traditional software deployment will be over 25%, and packaged software will shrink to 10% of new enterprise installations
- Oddly, just searching for these things online, you will find actual and projected figures that are $10bns out – they can't all be right (or wrong) – but the total figures are probably very large and growing

A thought

- As you go from SaaS, through PaaS to IaaS:
  - The customer gets more control as you move along
  - The provider is doing more basic things as you move along
- This of course influences the contracts – the more basic the work done by the provider, the simpler the contracting model (potentially and normally)
- They are not mutually exclusive – people nowadays talk about the SPI model (i.e. involving SaaS, PaaS and IaaS)

Another thought

- NIST wrote its guide in 2011 – and even since then we have moved on
- So we could also talk about:
  - Data as a Service – organisations are moving towards "Big Data" solutions, and require data on demand
    - By way of example, the UN has created a data access and delivery solution based on cloud
  - Everything/anything as a Service ("XaaS") – really a collective term for the provision of services of all types over a network
  - Storage as a Service
  - Network as a Service
  - Monitoring as a Service

More definitions – deployment models

- **“Cloud” has become a ubiquitous term bandied around by all and sundry – sort of coming to be synonymous with “internet”, but that is not right**
- **NIST comes to the rescue again by describing the different deployment models available to organisations**

Model 1 – Private cloud

- **NIST describes private cloud as follows:**
  - **“The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.”**

Model 2 – Community cloud

- **NIST describes community cloud as follows:**
  - **"The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises."**

Model 3 – Public cloud

- **NIST describes public cloud as follows:**
  - **"The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."**

Model 4 – Hybrid cloud

- **NIST describes hybrid cloud as follows:**
  - **"The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."**

Another thought

- **Again it can be seen that these different models provide for different scales of involvement by the provider with an individual customer**
  - **This will have a knock-on effect on the complexity of the contract**
  - **The more tailored the model for the particular customer, the more the terms of the contract are up for negotiations (potentially and normally)**

So what makes cloud uniquely cloud?

- **There are some essential characteristics – though the key throughout is flexibility:**
  - **On-demand self-service – customers get what they want when they want it**
  - **Broad network access – cloud comes over a network, and you access it by thin or thick platforms**
  - **Resource pooling – the provider provides computing resources to various customers, with different physical and virtual resources dynamically assigned**
  - **Rapid elasticity – capabilities can be scaled up and down on demand**
  - **Measured service – resource usage is monitored, controlled and reported, leading to pay-per-use or charge-per-use bases of payment**

So what would you be thinking of before taking the plunge?

- As the world turns to the cloud, one truism (it's not necessarily true …) is that pre-contract DD is more important than the contract itself
- Quality (contract: SLA) – so often security along with legal concepts like data protection are given the priority, but what about the basic user experience?
  - Speak to existing customers, understand network and bandwidth limitations
  - Get a grip on the support arrangements
- Data (contract: BC/DR, limits of liability)
  - What are the back-up arrangements?

So what would you be thinking of before taking the plunge? (ctd)

- **Personnel (contract: personnel and security vetting)**
  - Have the provider's personnel been security vetted? When? How?
  - Interview key/senior personnel and reject those deemed unsuitable
- **Physical security (contract: the security schedule)**
  - Physical examination of the premises
- **Technical security (contract: the security schedule)**
  - Factor into the type of cloud – do you want co-location with other customers on the provider's equipment or at the same premises? Or do you want a private cloud? Do you understand the technical solution?
- **Termination (contract: termination assistance)**
  - Test the process prior to contracting/acceptance

What would CIOs and CTOs make of all this?

- **Before moving to the cloud, you need to get a handle on some concepts:**
  - **They need to understand current and future demand**
  - **What are the issues around cloud services and existing systems?**
  - **How does the proposed cloud interact with other cloud services?**
  - **What are the risks in the provider's contract (limited or excluded liabilities)**
  - **What is the status of regulatory compliance (data protection, financial sector)**
  - **What are the ongoing arrangements (governance, support, SLA's, step-in)**
  - **Portability – especially for data**

Sign here and press down hard …

- One myth is that cloud contracts are basically non-negotiable
  - Probably true for a start-up providing a completely standard service at a massively discounted rate
  - Also probably true for a contract with a major provider where you do not have purchasing clout
  - But remember that much cloud is not just a standard service – it could be the provision of a completely private cloud, in which case, everything is up for grabs and the terms will be as tailored as the service itself
  - If you look at standard terms, you will normally find
    - Very low limits of liability related to the charges
    - Worse still, complete exclusions of liability for loss of profits, loss of data, costs of reconstructing data

Legal interlude

- **What happened to UCTA?**
  - **Section 3(1) Unfair Contract Terms Act 1977 applies where one party "deals" on the other's written standard terms of business**
  - ***Watford Electronics v Sanderson* [2001] EWCA (Civ) 317**
    - ***"… In circumstances in which parties of equal bargaining power negotiate a price for the supply of product under an agreement which provides for the person on whom the risk of loss will fall, it seems to me that the court should be very cautious before reaching the conclusion that the agreement which they have reached is not a fair and reasonable one."* (para 54)**
  - ***Pegler v Wang* [2000] EWHC Technology 137 (25th February, 2000) – an odd case on its facts, but it has recently been endorsed as the correct approach in Commercial Management v Mitchell [2016] EWHC 76 (TCC), again raising the question of whether it is better to negotiate or stay silent**

Focusing on some of the detail – pricing

- **Payment - periodic**
  - **There is a basic choice between periodic or usage-based charging models (or a combination of the two)**
    - **In general, periodic charges are commoner**
    - **Providers often offer different packages e.g. platinum, gold or silver depending on what is included in the service**
    - **The user must then examine the small print – maximum number of users, storage, bandwidth limitations**

Pricing (ctd)

- **Payment – usage**
  - **Usage based models are obviously of interest for the customer, which may not know what is going to happen in the future so only wants to pay for what is used:**
    - **As against which, usage based models can make cloud unpredictable for the customer in terms of budgeting for the future**
    - **INDICATIVE VOLUMES – means that providers will want to play with other clauses e.g. rates, termination for convenience, redeployment of kit**

More thoughts on pricing

- **Like bill shock in a mobile phone contract, nothing is free and you need to look at the small print**
  - **Providers have to make a profit, and the description of the service (platinum, gold or silver etc) often disguises what is in or out of scope**
  - **Much will depend on the small print – so a customer may find itself being charged extra for**
    - **Storage – if a customer goes beyond a set threshold**
    - **Support – if a customer wants 24/7/365**
    - **SLA – if a customer wants tight performance guarantees, it is unlikely to come free**
  - **All this should be anticipated in the contract, not left to demand e.g. there is no point buying the bronze package and then pleading for support on Christmas Day**

Focusing on some of the detail – pricing

- **Indexation**
  - This also has an impact on the "Term" as defined and the customer's right to continue from year to year, as opposed to having a gun held to their head as the provider hikes the price at the time of renewal
  - Otherwise, providers offer some sort of indexation related to RPI or CPI or perhaps these days by reference to some index based on the IT industry
    - IT industry indexes can often be higher than consumer based indices
  - It also affects other clauses – in many standard contracts, the provider will try to slip in a right to suspend or terminate the service against non-payment: unlikely to be acceptable for a minimal delay in payment

Focusing on some of the detail – quality

- **Service quality**
  - This will inevitably be measured by some sort of SLA, perhaps with a service credit regime
  - They become more important for cloud as against outsourcing or just licensing
    - In an outsourcing, you already know what the service is and you hope to improve it – you have something to judge it by
    - In a licence, you can test the software and form a judgment
    - Cloud is (nearly) always a jump in to the (relative) unknown
  - For this reason, other clauses which might be regarded as boilerplate are rather more important in cloud – e.g. audit, governance, the provider's obligation to report all breaches, step-in, change control
  - Security becomes a subject in its own right

Focusing on some of the detail – quality

- **Service availability**
  - This can be assessed in a number of ways
    - On the provider's servers
    - At the connection between the cloud and the customer's infrastructure
    - On the customer's end user devices (PC, tablets, smartphones etc)
  - The provider will normally start by measuring service by reference to its servers, but this is not of course a realistic test for a typical customer
  - If some other point is chosen, then the provider will normally start to argue for various exclusions e.g. public internet, bandwidth limitations on the customer's network and so on

Focusing on some of the detail – quality

- **More wrinkles on service availability**
  - **Providers may well offer 24/7/365 support, but this is often accompanied by a much larger downtime before service credits are incurred – 6 hours' downtime overnight is not necessarily a problem, but during the day, it could well be**
  - **If the customer's need is only for normal working hours, then this could be a better bet – with less downtime before service credits are incurred**
  - **Global contracts could be more complex with requirements for "follow the sun" support around the daytime, and "follow the moon" provisions for patching**
  - **Cloud contracts are normally replete with all sorts of reasons why the provider can suspend service or deny access – sometimes reasonably (e.g. for security), but other times not**

Focusing on some of the detail – ruses

- The experienced provider could well try to pull a few tricks
  - As a customer don't fall for the quick response times e.g. 100% of calls answered within 4 seconds (but the provider sets up an answerphone service …) or fail to make a distinction between fix and workaround
    - Even if they answer the phone, who is going to answer it and what are they going to do?
  - Many cloud contracts refer out to "policies" e.g. the Acceptable Use Policy, but this can be a way of the provider providing additional limitations on the service

Focusing on some of the detail – remedies

- **Service credits**
  - Providers may – reluctantly – offer up a service credit regime but customers should check whether this is said to be the exclusive remedy, as the amounts can be derisory compared with the actual losses
  - The law is now unlikely to regard service credits as unenforceable penalties
  - While service credits are all very nice, customers should really be worried about the practical impact on the service – and what is going to happen to remedy it
    - What is the reporting and remediation plan
    - What are the consequences of continued failure – customers normally seek to introduce some definition of "critical service failure" leading to a right to terminate without penalty

Focusing on some of the detail – termination

- **Service levels/credits and termination**
  - **Customers will want the right to terminate against failure to achieve satisfactory performance – both parties will be concerned to agree this in great detail**
  - **Typically, you will find customers seeking to negotiate a specific right to terminate if:**
    - **Performance over a given period falls below a stated level**
    - **Service credits to at least a stated level are paid over a certain period**
    - **The same service level is not met for an agreed number of consecutive months**

Focusing on some of the detail – IPR

- **IPR**
  - Cloud is really about services, so IPR may not be an important issue in the context of IaaS or PaaS, but is certainly an issue in SaaS
  - Where software is served to the customer's users, there will be licensing provisions
    - Normally restrictive, and limited to the customer's own internal business purposes and not for use as a bureau or timesharing
    - The licence is normally for the software as provided by the provider and one key issue is whether the user has to upgrade or can elect to stay on an old version
      - Cheaper for training
      - A safer bet after the software has bedded in at the customer
      - The provider will usually seek to move its customers onto the latest version to avoid increasing costs

Focusing on some of the detail – OSS

- **IPR (ctd)**
  - Cloud providers frequently resort to use of open source software, as it is invariably cheaper and already exists without further extensive development
  - One issue here relates to the obligation for a provider to provide source code
    - Most will not want to – but OSS licences vary in this regard
    - The GPL v3 requires source code to be provided where it is "conveyed" to a licensee, but "conveyance" as defined does not include provision over a network
      - However, see other licences, such as the Affero GPL, which does include internet/network access as a conveyance and would require disclosure of source to such recipients
  - Providers often require a licence to use the customer's data – technically, they will be copying it, but customers should check the breadth of the licence

Focusing on some of the detail – data

- **Data and acceptable use policies**
  - Providers often take a "one size fits all" approach to AUP's, and will
    - Provide for a complete exclusion of liability with regard to the content itself, and will often seek an indemnity from the customer with regard to content (e.g. in case it is defamatory or otherwise illegal)
    - Seek a wide-ranging right to take down or delete data in the event it is defamatory or infringes a third party's IPR
  - Customers normally push back on this – and ask for
    - A notice that data is being deleted
    - An indemnity against data being deleted unnecessarily
  - Note that AUP's often have other "provisions" in them which most customers would want to push back on e.g. use of customer data

Focusing on some of the detail – risk

- **Limitations and exclusions of liability**
  - A sort of uneasy truce has developed between providers' lawyers and customers' lawyers in the IT world in general
    - There is a sort of recognition that a provider's liability should be limited to what it receives e.g. liability is limited to 100%/110%/125% of the previous year's charges
    - There used to be a recognition that some types of loss were excluded e.g. loss of profits or of data (though there has been considerable pushback on this in recent years)
  - The issue with many cloud contracts is that providers are providing a fairly standard, commoditised service for relatively low income/profit, as against which the customer may be entrusting its high-value data/business to the provider's tender mercies
  - A mismatch!

Focusing on some of the detail - trends

- **What therefore is happening in cloud contracts?**
  - For the standard ones which are not negotiated, customers might well be surprised at just how little liability the provider is accepting
  - For the bespoke ones, the customer is king and many customers with the clout are imposing their terms on desperate providers
    - No exclusion of loss of profits etc
    - Unlimited liability for data protection breaches and security breaches - quite an undertaking where a provider is providing a service for limited profit to e.g. a bank in the City whose profits are vast greater, and for whom a security breach could expose it to great liabilities which it would seek to pass on
  - In this sense, cloud contracts are moving away from outsourcing contracts where providers are still digging in on these issues

Focusing on some of the detail – termination

- **Termination (and data)**
  - This is one area where things are much simpler than outsourcing contracts
    - Unlike an outsourcing, less likely in practice to be any sort of TUPE situation (not impossible by any means though)
    - Because the provider is likely providing the infrastructure and the software too, there are no complicated provisions about assets
  - The one thing the customer is worried about is DATA
    - What are the provisions for termination assistance – these will be like those of an outsourcing contract, period of assistance and exit plan production/maintenance
    - The customer will be concerned to get the data transferred and assistance in understanding it

What is your contract going to look like?

- **A checklist – none of this is exhaustive! Just typical ...**
  - **Pre-contractual DD:**
    - **Ownership of infrastructure**
    - **Licensing considerations**
    - **Locations for provision of the service**
    - **Relevant certification to do with e.g. security**
    - **Reference sites and existing customers**
    - **Data format – what is required for onboarding and what would happen on termination**
    - **Personnel of the provider**
    - **Provider's business plan and proposed developments**
    - **Compatibility with customer's existing and proposed systems and other cloud providers**

The contract

- **Checklist (ctd)**
  - **Scope and pricing:**
    - **What does the pricing cover – usage, storage, bandwidth**
    - **What is extra – licences, support, services**
    - **Features of the support offered**
    - **Are premium services required e.g. support out of hours?**
    - **Volume discounts and what happens if volumes decrease**
    - **No right to suspend even against non-payment**
  - **Onboarding**
    - **Timescales and costs of implementation, configuration and training**
    - **Acceptance (and rights to terminate, refund)**

The contract

- **Checklist:**
  - **Ongoing service**
    - **Governance – audits, regular meetings, step-in (?)**
    - **Service levels and reporting (including of breaches, failures)**
    - **Service credits and rights to terminate**
    - **What the customer must do e.g. AUP**
    - **Compliance with regulatory environment, change of law, change control**
    - **Dependencies (the provider may use these as "hidden" exclusions)**
  - **When it all comes crashing down**
    - **Provider's BC/DR processes**
    - **Escrow of software and data**

The contract

- **Checklist:**
  - **Data**
    - **Ownership and confidentiality, to be transferred on termination or on demand in an agreed format**
    - **Not to be deleted even if the account is dormant or has been dormant for an extended period, unless agreed notice is given**
    - **Not to be used by provider for its own purposes, duty to report e.g. subject access requests**
  - **Termination**
    - **Pricing and availability of termination assistance**
    - **Exit plan production**
    - **Data format and transfer**

The contract

- **Checklist**
  - **When it has all gone horribly wrong**
    - **Warranties, compliance with law and regulations applicable**
    - **Limitations and exclusions of liability**

THE LAW OFFICE OF
RICHARD STEPHENS

Thank you

Comments and feedback are welcome:

t: +44 20 7470 8767
e: richard@the-lors.co.uk