



Mason Hayes+Curran
Incorporating Arthur O'Hagan

Jeanne Kelly, Partner

Cloud Computing: The Legal Issues

14 June 2010

“One of the things we really need to watch out for is that we don’t hold cloud deployment back because we have some storyline about how ‘that’s too dangerous.’ I’m getting old enough to remember when that’s what they said about giving people PCs.”

- Tim O’Reilly, *“Navigating the New Cloud Era”*
23 March 2010



Introduction

- Cloud computing may be new...
- ...but that does not mean it is not regulated
- In fact the idea is not new
- Application Service Provider (ASP) - late 1990s
- SaaS/IaaS
- The *reality* is new
- Range of services



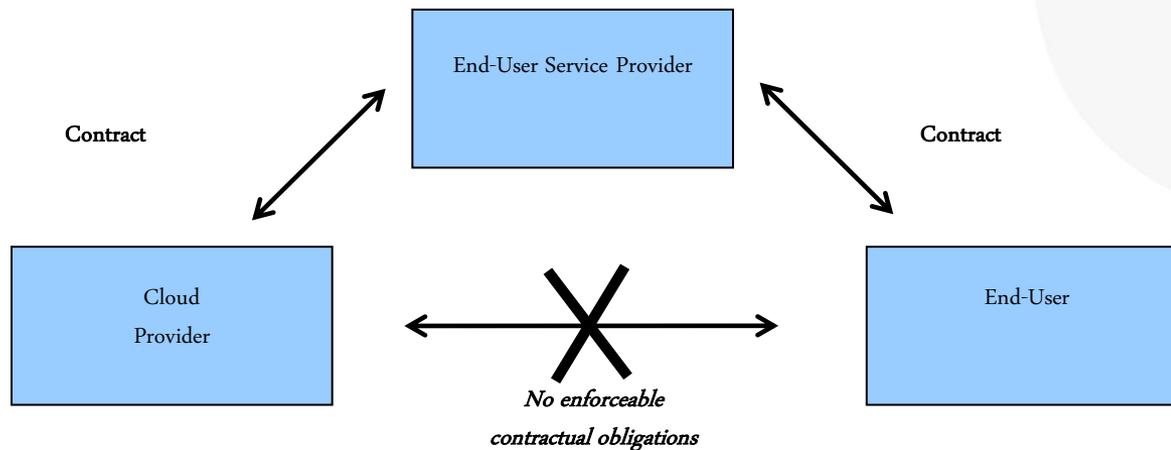
Content of Talk

- Scope of cloud computing
- Regulatory issues
- Contractual issues



Scope: Who is in?

- The Players:
 - Cloud provider
 - End-user service provider
 - End-user



Scope: Who is out? *Cloud computing vs. outsourcing*

- Superficial similarity: IT services delivered remotely
- Cloud services:
 - different targets
 - different payment models
 - no transfer of undertaking issues (TUPE) (employees)
 - data ownership issues
 - multilateral
 - “as-is” warranties
 - less purchaser control



Regulatory: Data Security (1)

- Top concern
- Loss of control – reliance on others (is the data backed up or not)
- Due diligence: business continuity plans



Regulatory: Data Security (2)

- Benefits:
 - loss of device \neq loss of data
 - data kept in highly secure data centres
- Implementing security is a technical matter
- Responsibility for security is a legal matter



Regulatory: Data Security and Data Protection

- Legal requirement to keep data secure
- Data controllers and data processors
- Contractual guarantees if personal data
- Data security breaches
- Encryption
- Discovery
- US Patriot Act / UK RIP Act



Regulatory: Data Retention

- Legal equivalent of hard and soft copies
- Cheapness of cloud storage
- Complex retention rules
- Data protection: only for as long as necessary
- Employment records
- Health and safety files
- Tax and related “tracing documentation”



Data Protection Law

- *Where is the data kept?*
 - locating data centres
- Transfer of data outside the EEA: need to consider:
 - Designated Country
 - Safe Harbor
 - Binding Corporate Rules
 - Model Form Agreements
 - Consent
- Opportunity for EU Companies, competitive advantage



Contract Issues

- Bargaining power – the whole spectrum
 - big player cloud providers
 - established end-user service providers
 - start up end-user service providers
 - big corporate end-users
 - SME end-users
 - individual end-users
- Standard form vs. individually negotiated



Contract Issues: Consumer Law

- Is the end-user a consumer?
 - Unfair Contract Terms Directive
 - Choice of law and jurisdiction
 - Section 2, Consumer Protection Act, 2007 (Ireland):
 - software is a 'good'



Contract Issues: Disclaiming Liability

- Even in B2B contracts: cannot disclaim liability for fundamental breach
- If contract is a contract for storage of data is loss of data a fundamental breach?
- Departures from traditional IT contracts
 - calculation of caps and liability
 - blurring of direct and indirect loss
 - mere “*as is*” software performance warranty



End-users: key tips (1)

- Are you getting genuine utility pricing?
- Can the service provider vary the price?
- Service Level Agreements: service credits & root cause analysis
- Versions and features
 - costs to upgrades and their costs?
 - guarantee of continued availability of certain features?
 - continued interoperability? – lack of uniform standards



End-users: key tips (2)

- Security
 - how is access controlled?
 - who has access?
 - how is data integrity controlled?
 - is your data kept separate?
- Internally: strong security policies
- Viability: due diligence, credit searches & chain of providers
- Tracking & auditing data: audit trails & recoverability



End-user: key tips (3)

- What happens if the provider goes bankrupt?
- Escrow: code and information escrow
- Provide for the exit in your contract:
 - ✓ Transition services
 - ✓ Format of data returned
 - ✓ No residue on vendor systems
 - ✓ Porting data between cloud providers
- Force Majeure: reasonable control
- Customer should own all its cloud based data



End-user service providers: key tips (1)

- Goal: continuous, reliable service
- Caught between cloud-provider and end-user
- Back to back risk management
- Contract can be used to build user confidence
- Ownership of data and code?



End-user service providers: key tips (2)

- Service level agreements
 - upstream / downstream
 - end-user: no more than in upstream contract
 - service credits: can help build customer confidence



Cloud-providers: issues (1)

- Data protection and regulation of data
- Transfer of data outside the EEA: need to consider:
 - Designated Country
 - Safe Harbor
 - Binding Corporate Rules
 - Model Form Agreements
 - Consent



Cloud-providers: issues (2)

- Where is the data kept?
 - locating data centres
- Providing access to customers and third party auditors
- Proprietary vs. open source?
- Extent to which liability can be limited
- Can cloud-providers be liable for information stored on their servers?



Conclusion

- Many of the concerns regarding security, reliability etc. can be dealt with by appropriate guarantees in the contract
- As market develops, may be a move away from blanket “*as is*” warranties
- Cloud computing is not *specifically* regulated, but that does not mean it is not regulated
- No case law-yet!



Q&A

- Tax matters
- Any questions?



Mason Hayes+Curran
Incorporating Arthur O'Hagan

Jeanne Kelly, Partner

Cloud Computing: The Legal Issues

14 June 2010