ICT managed services and "cloud computing"

Patrick Sefton | Principal, Brightline Lawyers

BRIGHTLINE LAWYERS

Technology | Intellectual Property | Brand

ICT – a longer view (for context)

- series of disruptive revolutions…
- 1980s: PC revolution
  - end dominance of centralised computing
  - empower individuals and workgroups
- 2000s: Internet revolution
  - 3.4% of GDP
    21% of GDP growth (in mature countries)
    10% increase in productivity for SMEs

Now – **two** further huge changes

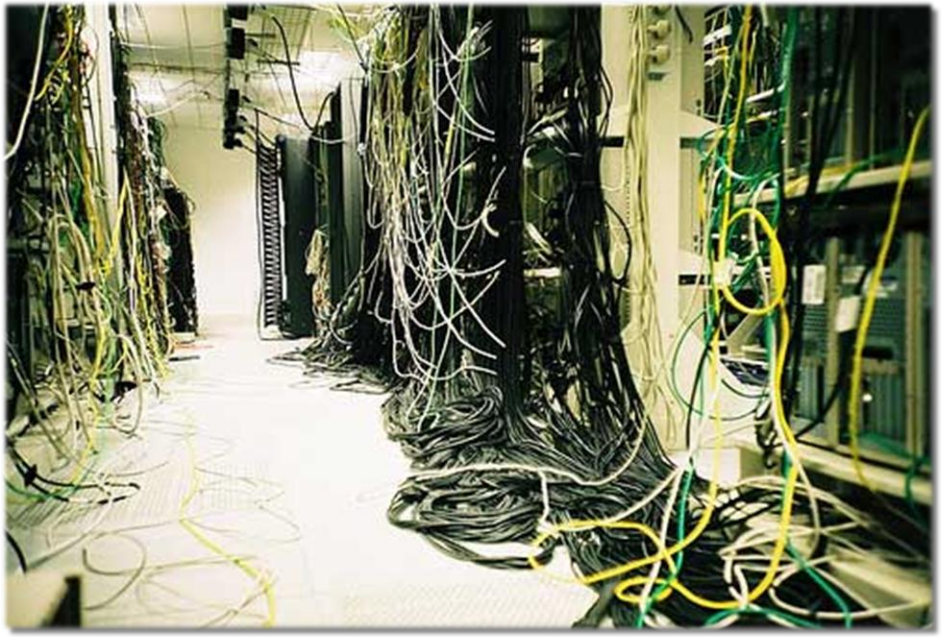
(1) Mobile

- mobile (smartphone/tablet) shipments exceed notebook/desktop since Q4-2010
- 1B smartphones/tablets now in use
- mobile internet users to exceed desktop users by Q1-2014

and at the same time …

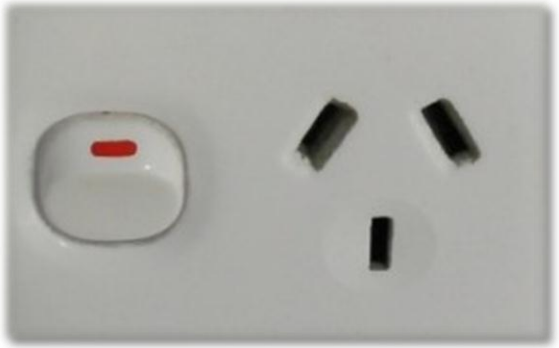
(2) “cloud computing”

- many different names
  (but only slightly different meanings)
- broad definition:
  - ICT capability
  - provisioned remotely, delivered as a service
  - with abstraction of detail



← less of this

more like this →



…

...connected to these →

What does this mean?

- Two major shifts concurrently:
  it's going to be quite a ride
- mobile:
  - consumers (clients?) increasingly expect service 24x7 from palms of their hands
- cloud:
  - we are back to centralised computing again
  - there are significant **opportunities** and **risks** in re-organising to use cloud services

Opportunities – cost reduction

- reduce local IT headcount, servers, storage, licence costs, depreciation/replacement cost

Product Name	Type	Cost (/user/month)
Google Apps	Productivity & docs, email, calendar, contacts	$5
Microsoft Office 365	Email, calendar, contacts, office web apps, doc storage, collaboration tools	$8
Salesforce	Customer relationship management	$21-$180
Rocket Matter	Legal practice management	$50
Clio	Legal practice management	$25-$50
LawRD	Legal practice management	$19
Gomatters	Legal practice management	$8-$16

Opportunities – cost predictability

- the cost is predictable (subject to agreement) and certainly more predictable than in-house costs
- there is not usually an additional cost for upgrades (check with the provider)

Opportunities – ubiquity

- nature of cloud services is to be available anywhere there is internet connectivity
  - mobile devices
  - out-of-office locations
- reduce “synchronisation” issues
- improve security
  - fewer copies
    particularly on notebooks, data sticks

Opportunities – service levels

- replication, redundancy, scale, dedicated organisation = higher quality service
  - eg, both Microsoft and Google offer 99.9% availability, even on low-end cloud products
  - ie, down no more than 43 minutes/month
  - *much* better than the average for in-house systems
  - should include SLA expectations in services agreement, though will not be a stop-loss

Opportunities – service abstraction

- great technology is invisible
- allows users (ie, lawyers & support staff) to get on with what we're good at
- cloud technologies are particularly good for abstracting those details
  - only have to make sure one thing's working (ie, internet connectivity, usually)
  - best case, everything else "just works"

Choosing a provider

- **scale** drives internet businesses
  - provide a "scalable" standard service at a low price
  - very low direct interaction
  - high level of automation / self-help
  - smaller providers may provide more personalised assistance

Choosing a provider

- smaller/custom providers may use larger providers as "back end" components
  - eg, AWS, AppEngine, Azure
- if service provider will not itself host, then find out who will host and where
  - privacy and security arrangements depend on data centre as much as service provider
  - understand what's going on (with data, at the start, "you don't need to know" is unhelpful)

Choosing a provider

- compliance and certification – formal standards for data centres
  - ANSI/TIA-942 or *Uptime Institute* "Tier" certification: Tier 4 is the most stringent
  - might also see PCI DSS (credit-card standard) or FISMA/HIPAA (US federal regulatory standards for government and health)
  - ISO/IEC 27000 is an information security standard for all types of organisation
  - other customers?

Issues – data sovereignty

- the Big Issue with cloud services
- your data (and your clients') does not reside on your own infrastructure
  - right and continuity of access
  - security / confidentiality
  - compliance
  - jurisdiction

Right and continuity of access

- address in services contract
- contract should allow access / take copy / periodically obtain copy of data
- should be provided in an appropriate exchange format
  - may be different from provider's own internal format, which may be proprietary
- should address insolvency, control change

Security / confidentiality

- *Legal Profession (Solicitors) Rule 2007* Rule 3 – Confidentiality
  - prohibits disclosure of confidential client information without client authorisation
  - may need to amend retainer to provide for authorisation to use service provider
  - service provider should (of course) itself be bound to strict confidentiality obligations

Information privacy compliance

- NPP4 Data Security: must take reasonable steps to protect personal information
  - should be reflected in service provider agreement
- NPP9 Transborder data flows: o'seas recipient must be bound by similar privacy law
  - should take care to determine which jurisdiction the data is located/stored in, if not Australia
- NPP compliance generally should be reflected in provider agreement in specific terms

Information privacy compliance

- Concerns about government access
  - "library records" provision of *USA PATRIOT Act* allows access to records of entities located in the US, or which are US-based
  - *Bank of Valletta v NCA* [1999] FCA required an Australian branch of a foreign bank to produce o'seas documents in Australian criminal proceedings
  - Australia is party to a number of mutual legal assistance treaties allowing access to data for the purpose of criminal investigations

Encryption & destruction

- contract should provide
  - encryption on-disk and on-the-wire
  - data will be entirely deleted (including backups) when the agreement ends
- difficult to police: have to trust contract and behaviour of the provider
- frequently hear of used PC's and drives bought with old data still present

Issues – disaster recovery

- contract should identify provider's DR plan
  - any size organisation should have one
  - less material for Amazon, Google, et al who have multiple redundant data centres
- and YOU should have a DR plan
  - in the case the provider just suddenly disappears
  - cf MegaUpload

Liability and risk allocation

- difficult to avoid ICT industry-standard terms on liability and risk
  - cap on total liability, typically related to the price (best case, a multiple of the price)
  - exclusion of consequential loss
  - breach of SLAs (eg, uptime) typically results in service credit
  - possibly indemnity from liability to others

Changing providers

- ensure you have your data (backup) in hand before advising of change
- could include “transition out” terms in agreement, but difficult to contract for genuine assistance
- have appropriate notice periods
- some providers notoriously unhelpful

Other risks for lawyers: privilege

- confidentiality critical to the preservation of privilege in client correspondence
- agreement should contain:
  - strict confidentiality provisions
  - provisions dealing with what the provider must do if documents are sought from it, or if relevant legal action is threatened against it (ie, contact you immediately!)

Other risks for lawyers: liens

- if file in someone else's hands, more difficult to enforce your lien
- agreement with supplier should prevent supplier from delivering file directly to client, or subject to approval only
- some providers seek lien over data to secure own payments: obviously high risk

Thank you

Patrick Sefton
Principal, Brightline Lawyers
Ph 07 3160 9249
Mob 0407 756 568
patrick.sefton@brightline.com.au

BRIGHTLINE
LAWYERS
Technology | Intellectual Property | Brand