Kennedys
Legal advice in black and white

CLOUD COMPUTING

Jillian Raw

Partner, Kennedys

http://www.kennedys-law.com/jraw/

Cloud Computing- what they say about it

- “the cloud will transform the information technology industry … profoundly change the way people work and companies operate”. The Economist.

- “Our industry is going through quite a wave of innovation and it's being powered by a phenomenon which is referred to as the cloud.” Steve Balmer, CEO Microsoft.

Cloud computing- what is it?

Cloud computing-what is it?

- Cloud computing, at the broadest level is the provision of computer resources as a service over a network, typically over the Internet.

- Computer resources range from raw processing power and storage such as servers to full software applications.

- It is a special form of outsourcing, in which parts of the IT environment are rented as a service, instead of being operated by the company itself.

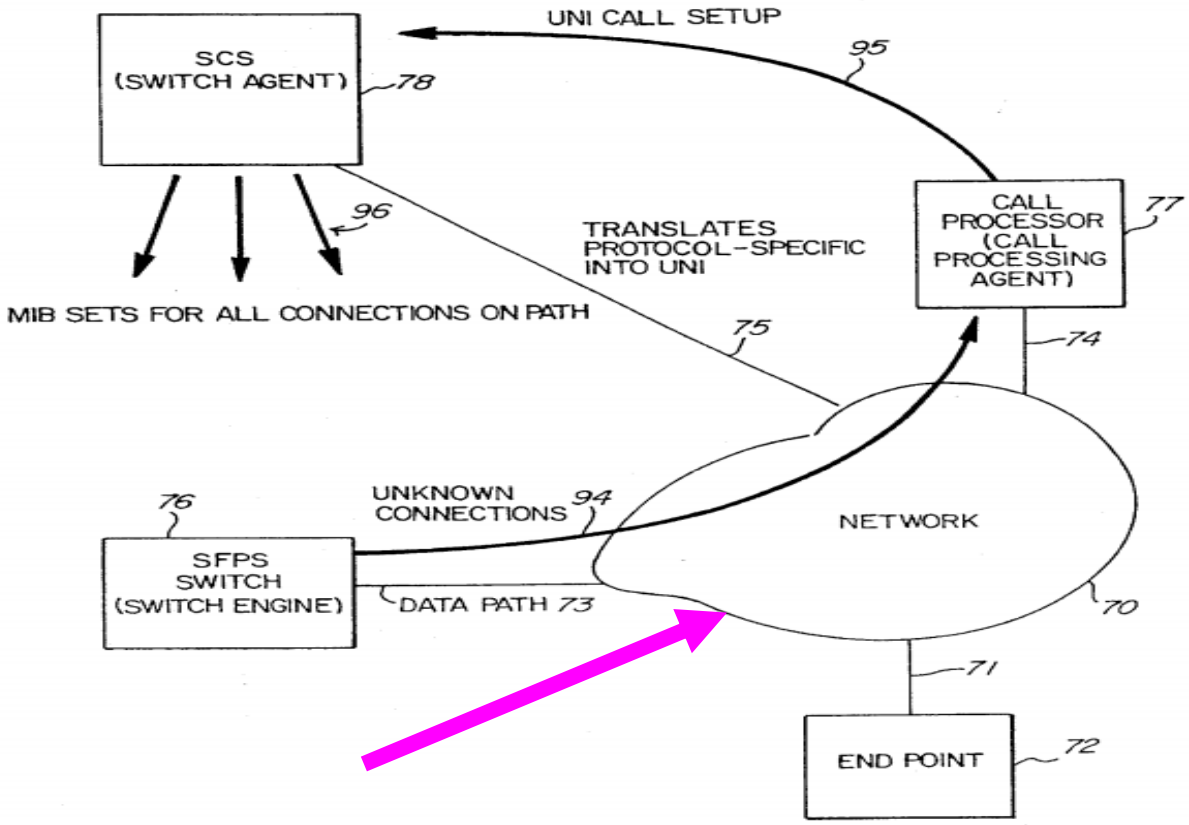
Cloud computing- what is it?

"The concept, quite simply, is that vast computing resources will reside somewhere up there in the ether (rather than in your computer room) and we will connect to them and use them as needed."

Jonathan Weber (The Times Online).

Cloud computing- why the “cloud”?

The term “cloud” refers to the Internet due to the practice of drawing a cloud shape **to depict the Internet** in computer network diagrams.

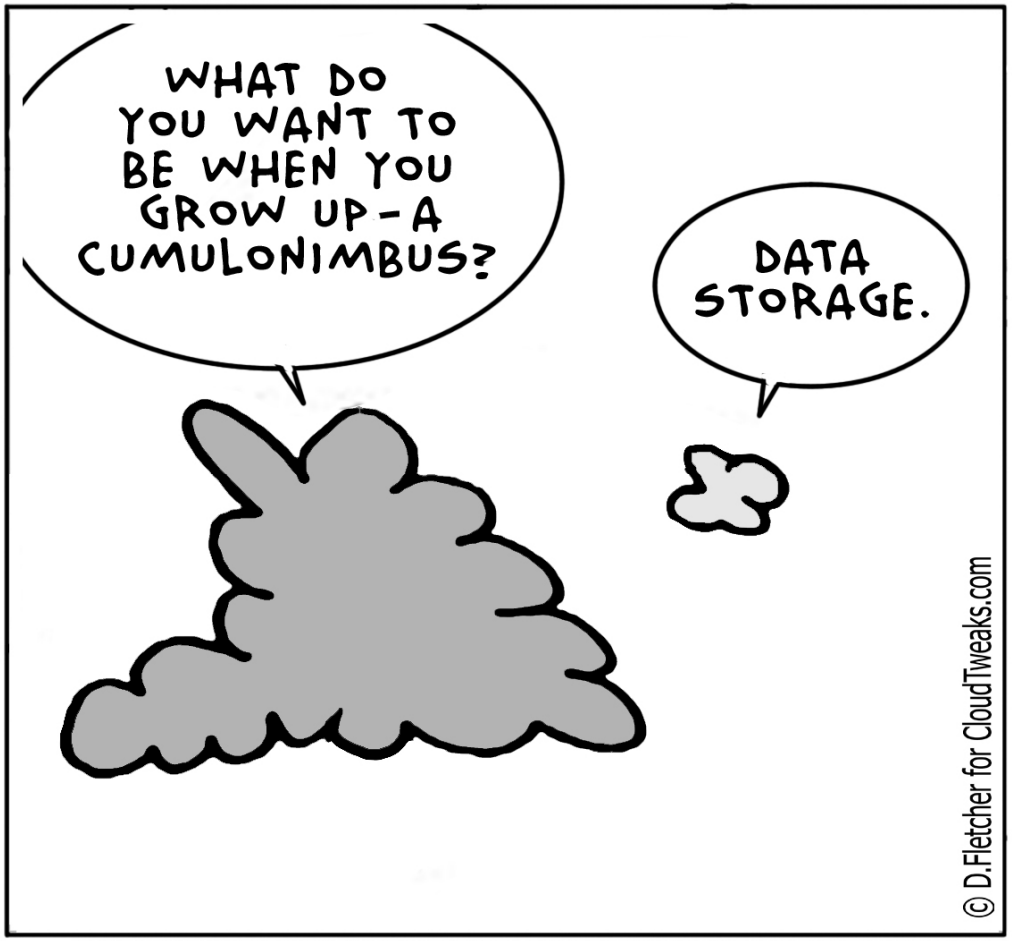


Cloud computing services

- Cloud computing is offered through a variety of services.
- The main types of services are:
  - Software as a service (**SaaS**)
  - Platform as a service (**PaaS**)
  - Infrastructure as a service (**IaaS**)

Infrastructure as a Service (IaaS)

- The provision of access to computer infrastructure over the network e.g. data storage or hardware.
- The service provider owns the equipment and is responsible for housing, running and maintaining it.



Software as a Service (SaaS)

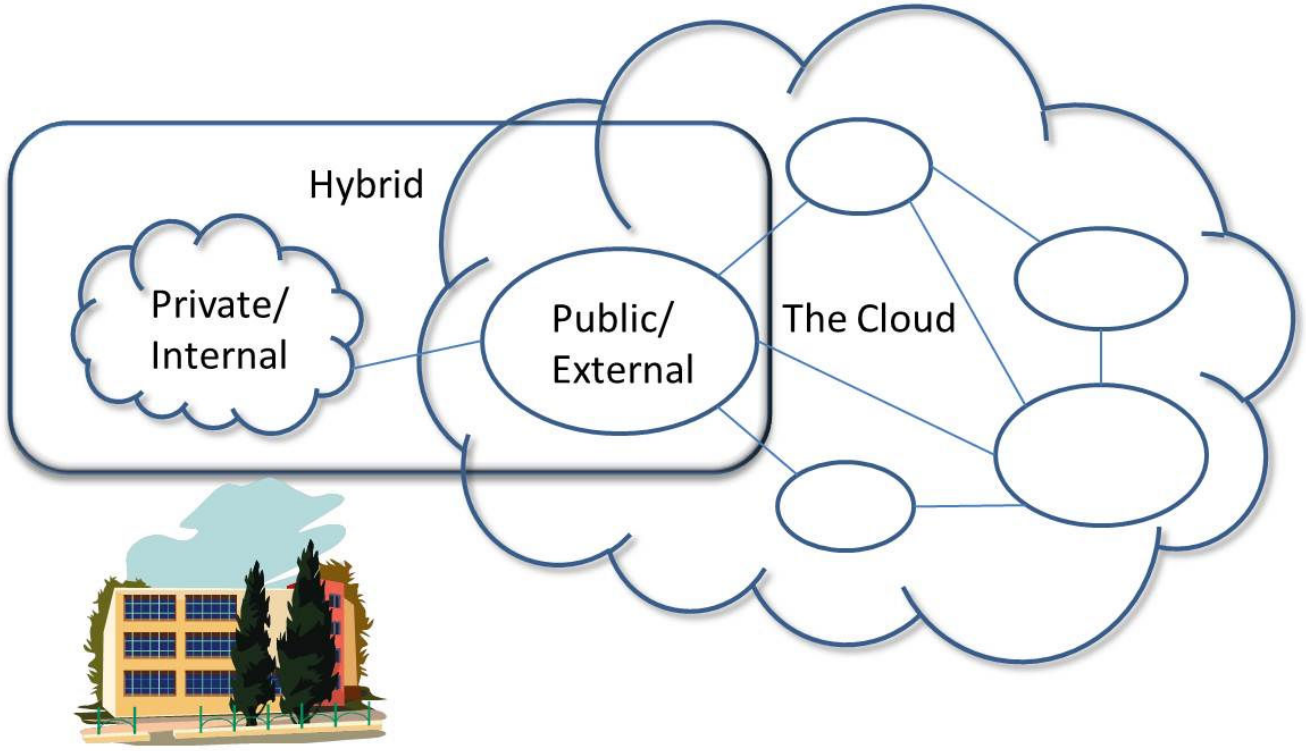
SaaS

- Provision of software over a network rather than being loaded onto a computer.
- Many of us here are SaaS users already.
- A sub-class of SaaS is “Storage as a Service” e.g. Dropbox.

Platform as a Service (Paas)

- The provision of computing platforms over the internet on which the user can develop and execute its own applications.
- Example: Google AppEngine.

How are cloud services delivered?



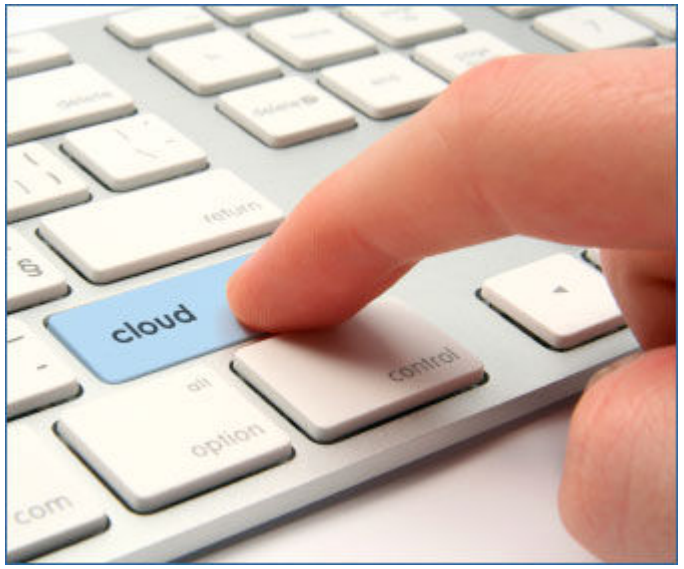
Cloud Computing Types

To the cloud

- Global cloud market is expected to grow to £77 billion by 2015 from £24 billion in 2011.
- By 2015 75% of US companies are expected to be using cloud services in one form or another.
- By 2015 at least 30% of Fortune 1000 enterprises will deploy at least one business critical system in the cloud.

To the cloud

- More than 50% of US businesses already use cloud computing services (Forbes, April 2013).
- A survey of 1,000 organisations in the EU found that 64% were current cloud users. (EU Commission Survey July 2012).



Cloud 9 - Benefits of cloud computing

1. The cloud is “elastic”. Cloud users only pay for the capacity they use, which can be altered to deal with fluctuations in demand.

2. Avoids the expense of purchasing and maintaining hardware and software.

3. Eliminates the physical presence of servers on-site and with them security and maintenance.

Cloud 9 - Benefits of cloud computing

4. Permits data to be portable, transferable and instantly accessible.
5. Permits the use of “big data”.
6. Supports the deployment of mobile computing devices and applications on a large scale.

Storm Clouds

What can go wrong in the cloud?

1. Cloud attacks

- The cloud is hacked into and data is stolen or security is breached.
- Clouds are attractive targets because of the volume of data stored and multiple users on the same system.
- Cloud security standards? The Gauntlet Cloud Hacking Contest September 2013.

What can go wrong in the cloud?

2. Cloud Outage

YEAR	CLOUD PROVIDER	LENGTH OF OUTAGE
2007	Navisite	1 week affecting 165,000 company websites, who were unable to access their date or trade on-line.
2009	Amazon Data centre	48 hours as a result of lightening strike.
2011	Yahoo mail	6 hours causing a disruption to 1 million users.
2012	iCloud	30 hours affecting 2 million users.
	Windows Azure Storage	77 hours.
	Amazon WebServices	20 hours.
	Centercorp	3 hours. Dozens of US hospitals lost access to patient records.

What can go wrong in the cloud?

3. Data Loss/Leakage and Inadequate recovery

- A significant risk.
- The cloud user is ultimately accountable for complying with relevant data protection laws regardless of whether the data is stored in a cloud.
- 1824 out of 3200 companies had lost data in the cloud. *Symantec Survey 2013*.

What can go wrong in the cloud?

4 . Cloud Provider Disputes

- Data ownership and use disputes.
- Because cloud data may be stored in proprietary format it may not always be possible to export the data in a non-proprietary format to enable re-use by the users.
- A cloud user may face considerable difficulty recovering and re-formatting its data.

What can go wrong in the cloud?

5. Bad cloud

- Cloud user may end up in bad cloud company
- Risk of the data no longer being available if the cloud provider's equipment is seized or its business closed down.

Cloud Insurance- a silver lining?

- Growing market of cloud specific insurance.
- For Cloud providers:
  - Cover against liability claims for outages and data loss.
  - Cover for the costs of dealing with an outage (technical issues, back up and data restoration).
  - Cover for the costs of dealing with a security breach or being hacked into.
  - Cover for damage to the cloud's infrastructure.

Cloud Insurance- a silver lining?

- For Cloud users cover can include:
  - Loss of income caused by outages.
  - Costs incurred procuring services from a new provider e.g. cloud provider goes insolvent.
  - Costs incurred as a result of data breaches.
  - Costs incurred to recover or reformat data.

Underwriting Cloud Providers

ISSUE	UNDERWRITING QUESTIONS
Security	Does the cloud provider comply with industry accepted practices and certifications such as ISO 27001?
Security	Can the cloud provider provide an appropriate 3rd party security assessment?
Security	What audits are carried out to check data security? At what frequency and by whom are these audits carried out by?
Security	Where are the cloud provider's data centres located? What physical security arrangements are in place?
Integrity	How often data is backed up?
Integrity	Does the cloud provider uses a remote storage server to back-up data?
Integrity	In the event of an outage or data breach is a recovery plan in place? What level of onsite IT expertise is available?

Underwriting Cloud Providers

ISSUE	UNDERWRITING QUESTIONS
Availability	What percentage of uptime/service availability has the cloud provider attained over the past 12 months?
Availability	How quickly can the cloud provider restore data from a back-up if it suffered a data loss?
Availability	What length of outages were suffered by the cloud provider over the past 12 months? And what was the reason for the outage(s)?
Availability	What contingency arrangements are in place to deal with power failures and hardware malfunctions?
Availability	What capacity arrangements does the cloud provider have to deal with high usage demand?

Underwriting Cloud Users

ISSUE	UNDERWRITING QUESTIONS
Cloud Provider	Which cloud provider is to be used?
Cloud Provider	Is more than one cloud provider to be used? Are different cloud providers to be used for different types of cloud services?
Cloud Provider	Where is the cloud provider's services located?
Cloud Provider	Does the cloud provider comply with industry accepted security practices and certification?

Underwriting Cloud Users

ISSUE	UNDERWRITING QUESTIONS
Usage	What services will be used for the cloud? Iaas, SaaS, PaaS?
Usage	What type of data will be sent to the cloud? Commercially sensitive or proprietary or personal data?
Usage	What type of cloud will the data be stored in? Will different types of data be stored in different types of cloud? And what type of due diligence will be carried out (if any) to audit the type of data sent to the cloud?
Usage	Will the cloud provider produce a copy of the user's data in a readable and portable format if the cloud user decides to move to another cloud?
Availability	Has an outage been experienced with the user's cloud provider in the last 12 months?
Availability	What effect will an outage have on business operations? What percentage of sales/transactions/services is wholly reliant on cloud based services? What disaster plans are in place if it is not possible to access the cloud?

Traditional Insurance Response

First Party Loss Example

As a result of a cloud outage a company is unable to access its data or use software in the cloud. This prevents the company from operating, causing it to lose income.

Traditional Insurance Response

- Some courts in the US have expressed the view that data is not property susceptible to damage.
- "We fail to see how information can be said to have a material existence, be formed of out of tangible matter, or be perceptible to the sense of touch. To be sure the information is stored in a physical medium, such as magnetic tape…but the information itself remains intangible" Ward Gen Ins Serves Inc v Employers Fire Ins. Co (Cal. App. 2003)
- Also simply because data cannot be accessed does not necessarily mean it is damaged.

Traditional Insurance Response

- BI cover is typically restricted to cover loss of income as a result of "*damage to property at the insured's premises.*"
- The cloud would ordinarily not be located at the Insured's premises.
- A Contingent Business Interruption Loss claim is likely to encounter the difficulty of proving that the loss of data or access to data is damage within the meaning of the policy.

Traditional Insurance Response

However, many traditional policies:

(1) Exclude computer or data related losses.

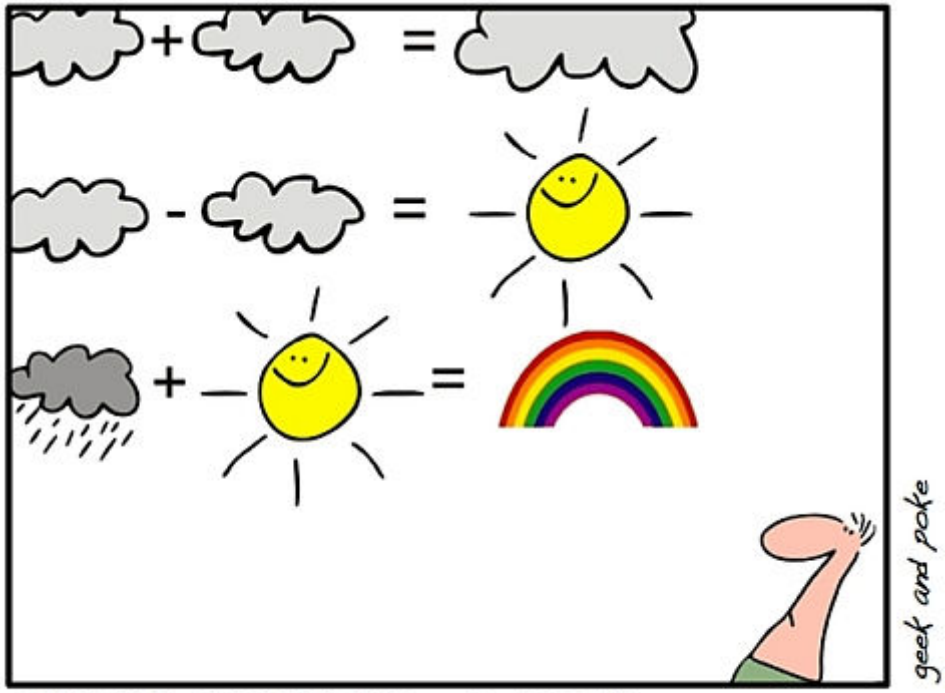
(2) Have low limits of cover.

(3) Are subject to time deductibles typically of 24 to 72 hours. The average cloud outage is only about 7 hours. So many policies might be of little value to an insured.

Will a general cyber policy respond?

- Even a general cyber policy might not be adequate to deal with cloud issues.
- Cyber policies often refer to a “computer network” or “system”.
- But whose “computer network”?
  - If defined as the “insured’s network” it is unlikely to cover losses in the cloud.
  - If defined as including e.g. outsourced IT service providers” it might include the cloud.
- However, the “network” might be geographically limited.
- Increasingly, general cyber policies are specifically excluding coverage for losses arising at cloud level.

The End



SIMPLY EXPLAINED – PART 17:
CLOUD COMPUTING