

Forensic Technology and the Cloud

DuncanPowell

RESTRUCTURING • TURNAROUND • FORENSIC

12 October 2017

Liability limited by a scheme approved under Professional Standards Legislation



Peter Lanthois

Partner

Office: (08) 8223 8107
Mobile: 0407 258 959
Email: planthois@duncanpowell.com.au

Peter has been overseeing the Forensic department since June 2014, he has over 33 years accounting experience, four of which were in commerce with a major Australian firm. Since 1987 he has specialised in corporate insolvency with several established firms.

Peter thrives on the challenges his profession provides and has developed wide ranging industry knowledge including specialty areas such as education and indigenous affairs.

He has proven skills in both formal and informal insolvency appointments and has conducted reviews for major Australian banks and financiers as well as providing consulting services to a number of government departments and major corporate entities. He has extensive experience in investigating and analysing the affairs of both solvent and insolvent companies, the quantification of losses or damages for legal claims and acting as an expert in litigation matters.



Briston Talbot

Associate Director

Office: (08) 8223 8114
Mobile: 0439 806 906
Email: btalbot@duncanpowell.com.au

Briston is responsible for the management and delivery of Forensic Technology services, including computer forensics and e-discovery and has over nine years' experience in accounting and restructuring matters and five years' experience in providing Forensic Technology and investigative services.

Briston's restructuring experience includes the review, investigation and restructure of organisations from small business owners to publicly listed organisations on behalf of secured lenders, creditors and stakeholders. He strives to work with stakeholders and organisations to achieve the best possible outcome for all.

During his career, Briston has also been responsible for the investigation of computer based information which includes the forensic investigation of corporate fraud, financial crime and intellectual property (IP) theft. This has included supporting investigations of regulatory bodies and the DuncanPowell restructuring team through the acquisition and analysis of forensic images.

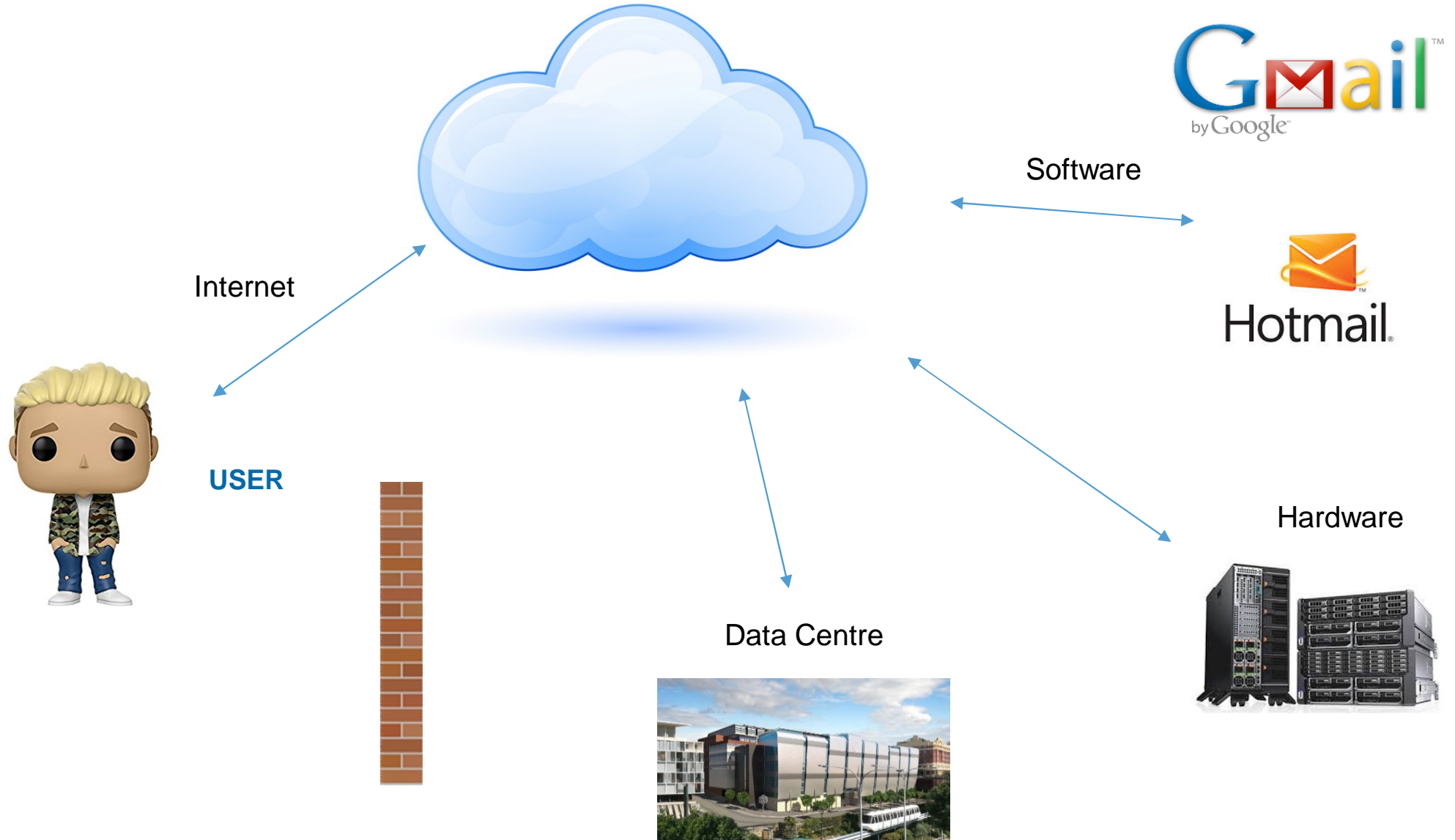
The Cloud

- What is it?
- What does it look like?
- Service Levels
- Organisational structure
 - The result of the cloud
 - Scenario
- Where is the information
- Why is this good for an investigation
- Evidence collection possibilities
 - Limitations
 - How can computer forensics help
 - Questions

In simple terms, Cloud computing is using the internet to access someone else's software running on someone else's hardware in someone else's data centre.



So what does this look like?



Software as a Service (SaaS)

A user uses software applications made available from a cloud provider. Usually the user interacts with SaaS applications using a web-browser.

An example of SaaS is the Google Apps suite offered by Google. Users can use the suite to deploy email, make use of Google Docs and Calendar.

All data generated by the use of the applications is stored in the cloud



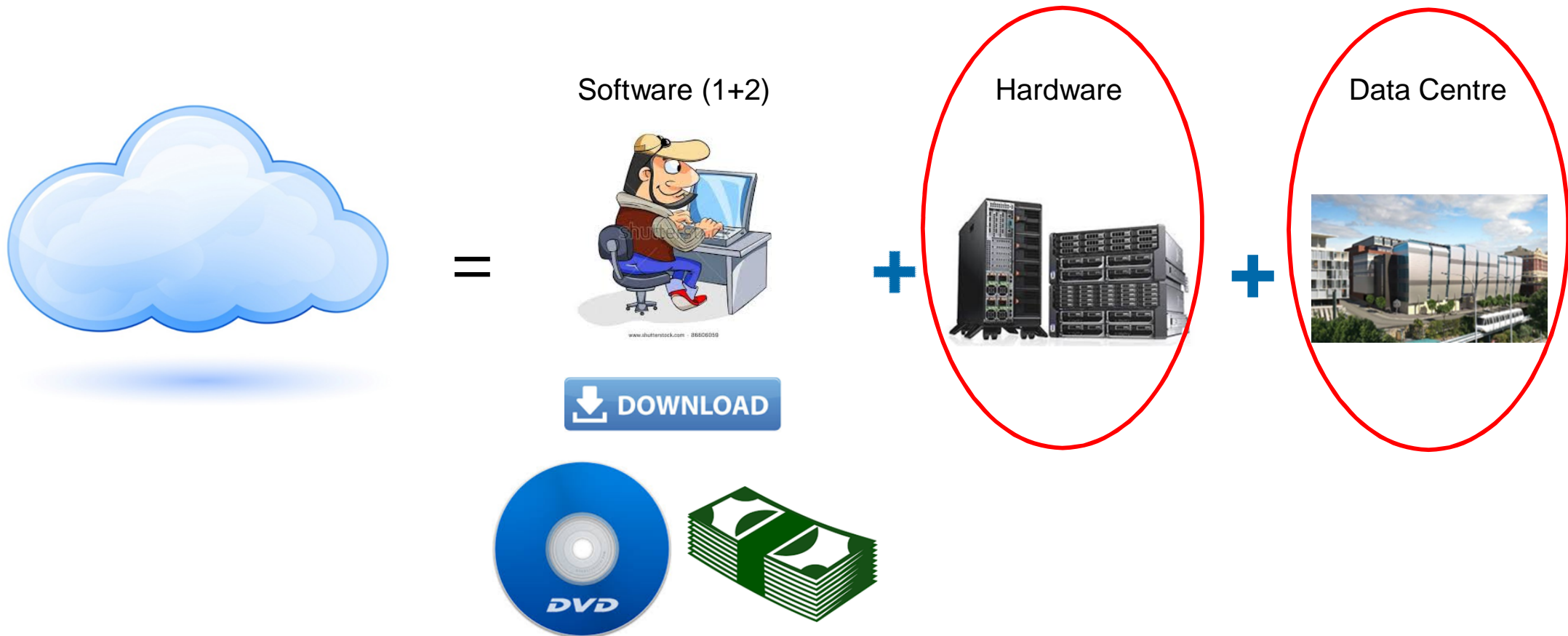
Platform as a Service (PaaS)

Application programming interface (API) for users to create and host custom-built or bought applications. An example of PaaS is Microsoft Azure or Amazon Web Services



Infrastructure as a Service (IaaS)

Is the leasing of virtualised computing resources such as processing power, volatile memory and persistent storage space to host virtual machines.



Private cloud

The infrastructure is operated solely by the organisation who owns the cloud.

Community cloud

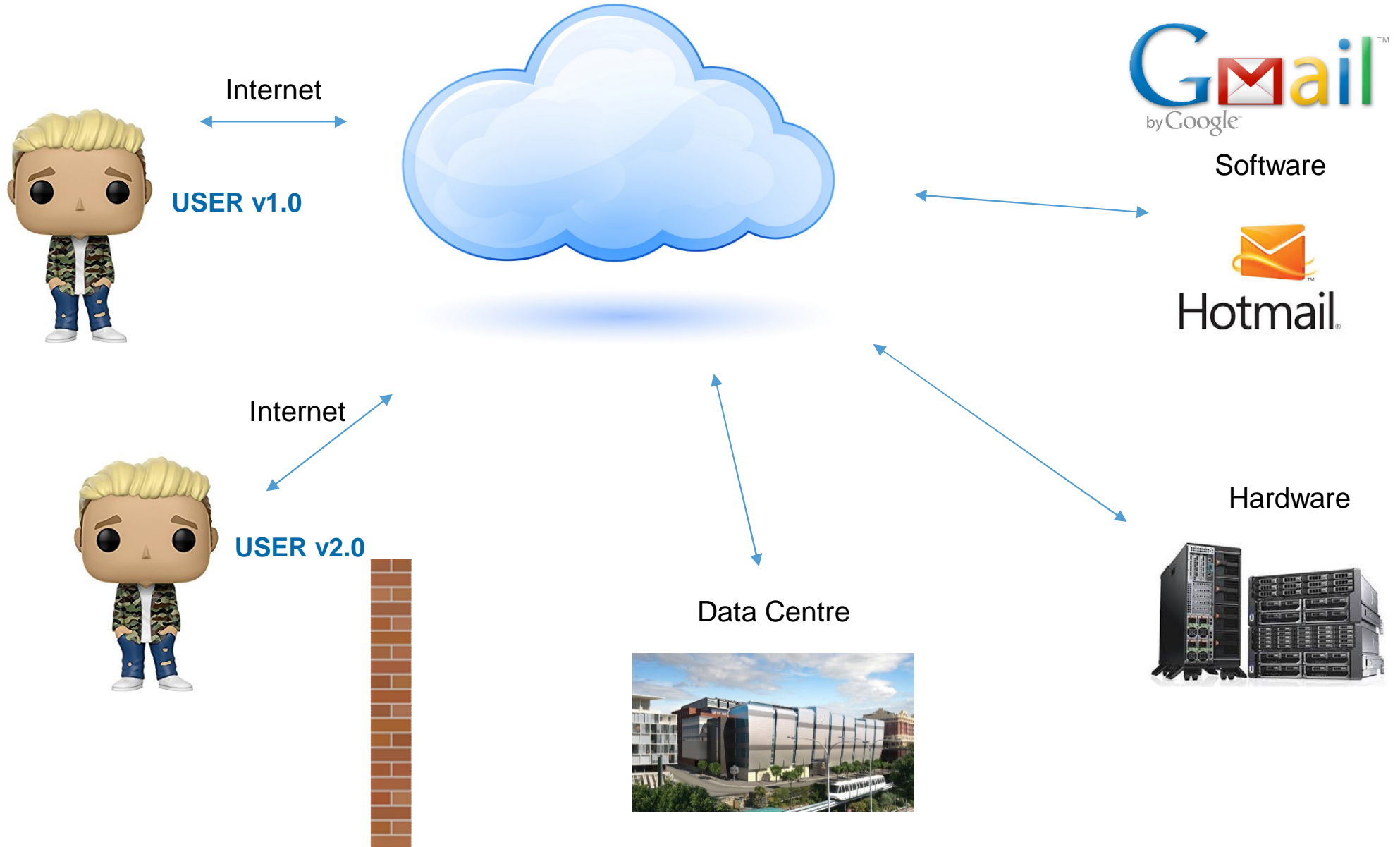
Is shared between several organisations

Public clouds

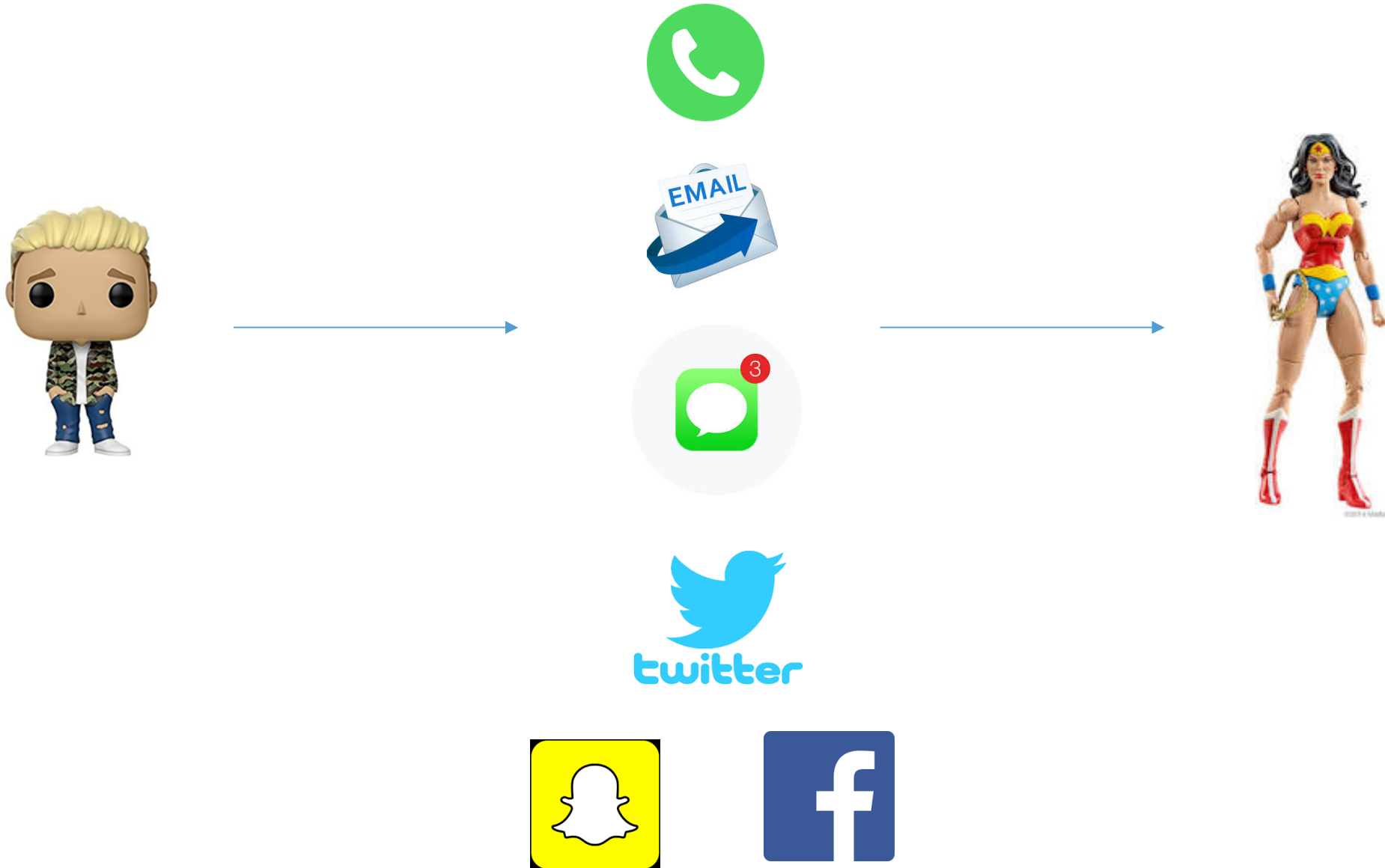
Will usually be owned by a provider organisation, which will maintain the cloud facilities in one or more corporate data centres. The administrative control of the cloud resources will therefore reside with the provider, rather than the user.

Hybrid cloud

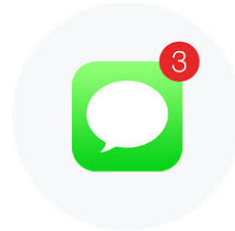
Is a composition of two or more of the above deployment options



- Presents a security issue.
- Replicate: Subject to legal implications with username and password you could access User v1.0 information. Which could include:
 - Emails
 - Social media
 - Photos
 - Full backups of mobiles, tablets and laptops
 - Bank details
- Thoughts around two step verification



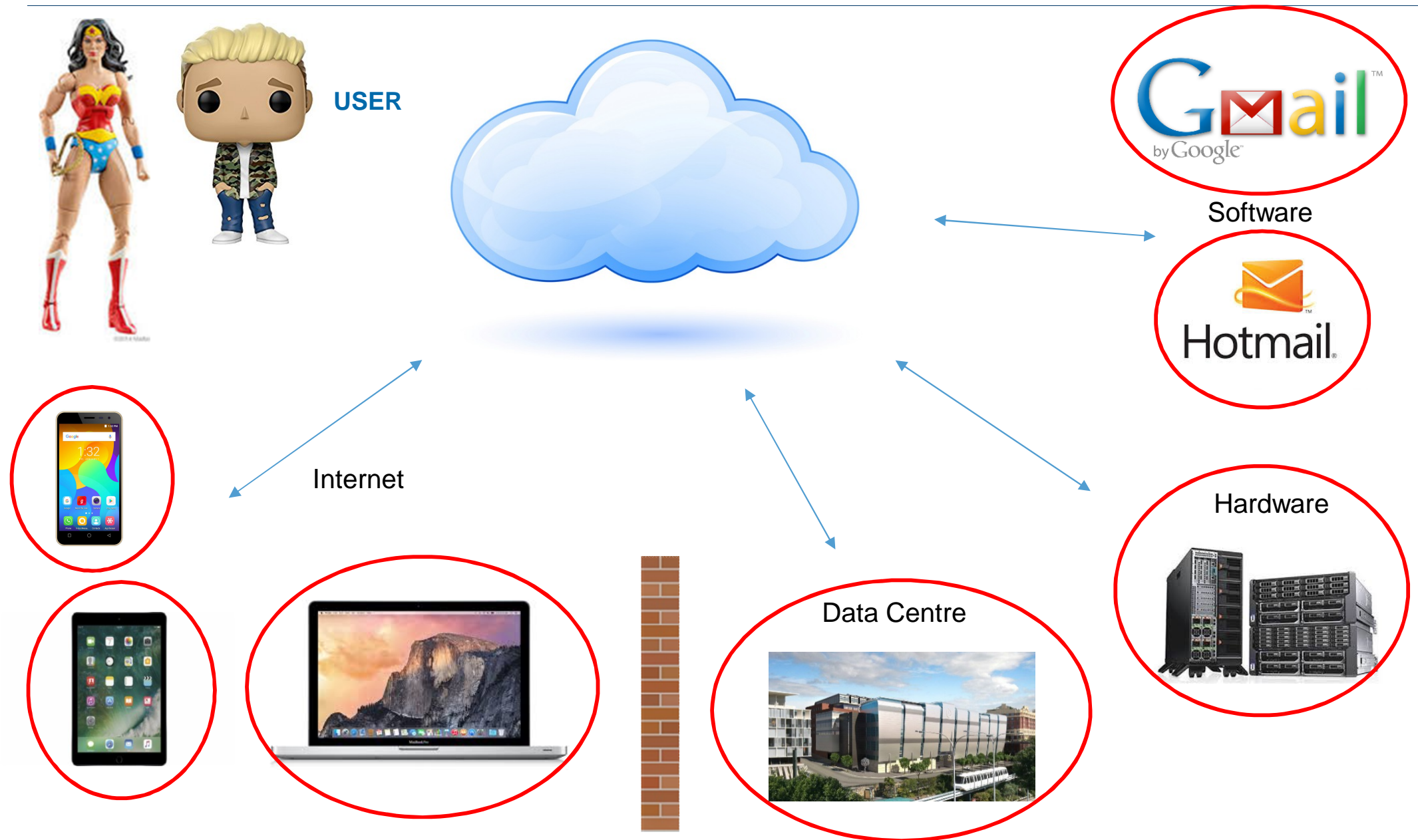




So where is the information?



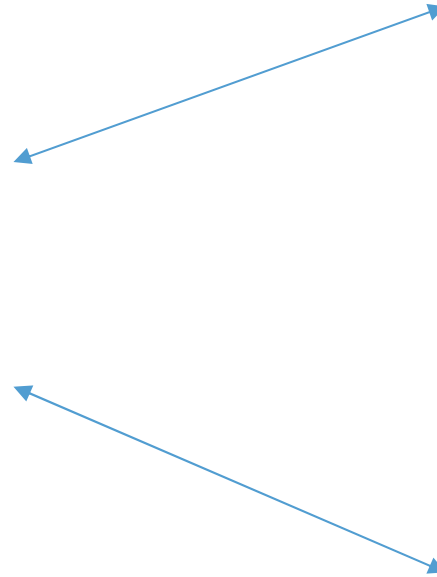
So where is the information?



So why is the cloud good news for an investigation?

Nobody likes losing information – so what do we do?





Google Drive

iCloud - can go to your icloud: www.icloud.com

Dropbox

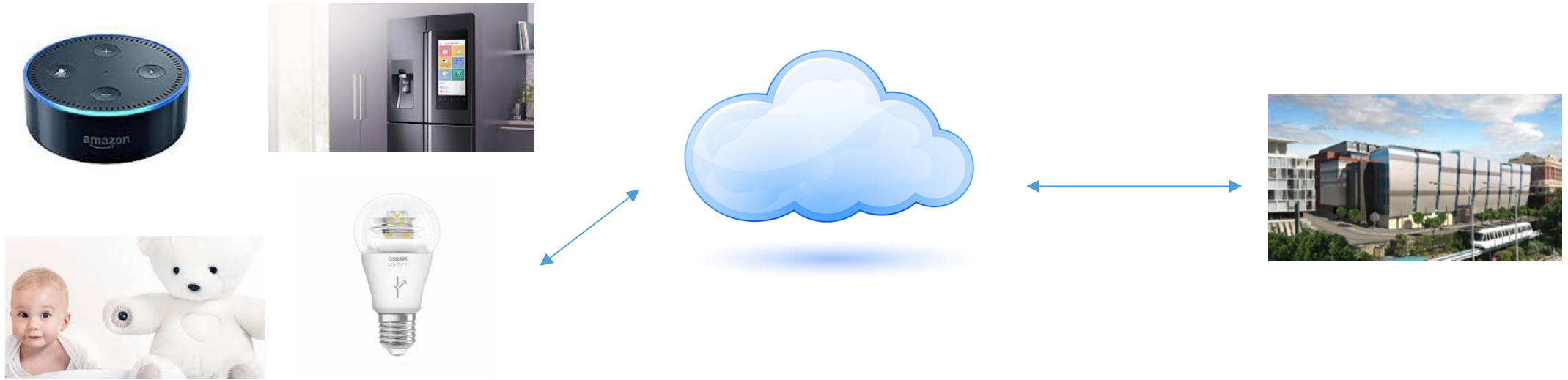
Personal items



Cloud information



Cloud - the door to other issues and possibilities – Rise of IoT



Brings about the possibility of other evidence items to consider:

Samsung SMART TV

– with voice recordings

SMART globes

– switch lights on and off

Voice digital home assistant

– Google Home, Amazon Echo (still to come in AUS)
and Apple speaker (still to come in AUS)

Security issues

– unsecured devices can be monitored
– website can search for these devices www.Shodan.io

Software – Cloud based

- Owned and operated by a third party
- Location (might be a foreign country)
- Security settings – need username and password
- Rights of access

Hardware – Cloud based

- Owned by a third party
- Rights of access
- Location (might be in a foreign country)
- Limitation regarding recovery deleted items

- Chain of custody
- Privacy issues
- Cross border issues
- Ownership issues
- Repeat the process (if required)

- Tools to help collate the information and put it into a format that is readable, can be investigated and is presentable
- Identify possible evidence options
- Potentially save possible electronic information
- Save time and costs through tools
- Help preserve and present information for client, court etc (depending on scope of work)

