Legal Implications of Cloud Computing

Allison Stanfield
28 August 2014
Presentation Topics

- Presenter / e.law overview
- What is Cloud Computing?
- Risks in Cloud Computing
- What are the Legal Issues?
- Privacy considerations
- How to conduct due diligence
- What are the security issues?
- Regulatory compliance issues
- Discovery issues
- The USA: special mention
The Presenter

Allison Stanfield

- Founder of e.law
- Awards for innovation in e.courts, Telstra BWA finalist
- Formerly practising lawyer, retains unrestricted practising certificate
- Writes and speaks regularly on topic of digital evidence
- Undertaking PhD on the authentication of digital evidence

e.law

- Founded in 1999, 15 years in operation
- Provides end-to-end digital evidence services
- Evidence collection to presentation in court (e.courts)
- Provides cloud based solutions for lawyers to access and review evidence, within Australia
What is Cloud Computing?
What is offered?

- Cloud computing can comprise:
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- Or a combination of each of these
What is Cloud Computing?

How does it work?

► Users can “rent” server space in order to store data
► Provides a cost effective method to store data:
  ► No internal infrastructure costs
  ► No software costs
  ► No IT staff to manage infrastructure and software licensing
► The cost effectiveness comes in server space being available in a “virtual” environment
► The Cloud vendor can move data from one place to another for load balancing, thereby increasing efficiency in data storage capacity
Risks in Cloud Computing
What to consider

- The Contract does not provide adequate protection or remedies
- Privacy breaches
- Security breaches at data centre
- Loss of Data
- Loss of Control over the Data
- Insolvency of the Cloud Provider
- Disaster recovery
- Termination and subsequent data migration
- Local versus offshoring
Risks in Cloud Computing

Mitigating against the risks

- Due diligence is the key
- It’s all about the Contract
- Cost versus control: usually less cost means less control
What are the Legal Issues?

- Control of the data
- Location of the data: jurisdiction
- Cross border enforcement
- The Contract
- Privacy considerations
Legal Issues: Control of the data

Who has control?

- Is it like storing boxes in a warehouse?
- Recent cases say that electronic information is intangible and incapable of being “owned”
  - English Court of Appeal held that a database was an intangible asset and the law did not regard this as property; accordingly it is not subject to a chose in action
- *Dixon v The Queen* [2014] NZCA 329
  - NZ Court of Appeal had to determine whether a digital video recording was “property” and capable of being stolen: the court said while the hard disk could be stolen, the information stored upon it could not
- Compare the law of intellectual property and intangible assets
Legal Issues: Location of the data

Jurisdiction

- Who has jurisdiction over the data?
- Recent decision of New York District Court:
  - US District Judge Loretta Preska, ruled that Microsoft had to turn over a customer’s emails stored in a data centre in Ireland to the US Government.
  - Microsoft, along with other US companies, had challenged a criminal search warrant for the emails, saying that federal prosecutors cannot seize customer information that is held in foreign companies.
  - The Judge ruled that the warrant lawfully required the company to hand over any data it controlled, regardless of where it was stored.
  - “It is a question of control, not a question of the location of that information”: Judge.
  - Microsoft intends to appeal.
Legal Issues: Location of the data

Jurisdiction

- In Australia, there may be limitations to storing data offshore.
- APRA requires notification of any transfer of data offshore by financial services institutions (*Financial Sector (Collection of Data) Act 2001* (Cth); *Form ARF 321.0 Statement of Financial Position (Offshore Operations)*).
- Some government departments have a blanket prohibition on the transfer of data offshore.
- Enforcing remedies available in Australia may not be available in overseas locations.
- Exposure to investigative powers of offshore police/regulatory authorities.
- Finding a nexus between the dispute and the court in which the dispute might be brought.
Legal Issues: Cross-border enforcement

Issues

➤ Privacy
  ➤ Lack of consistency in data privacy laws across jurisdictions makes compliance difficult to monitor
  ➤ Some jurisdictions do not recognise a general right to privacy
  ➤ The recently released Exposure Draft, if enacted, will introduce vicarious liability so that if a business holding personal information discloses information to a cloud provider, it may be vicariously liable for any misuse of that personal information by the offshore entity

➤ Offences
  ➤ Offences are not consistent across jurisdictions
  ➤ Offences in one jurisdictions may not be enforceable in another jurisdiction
Legal Issues: The Contract

What to look for

- What does the contract cover: infrastructure, software, support?
- Liability for damages for interruptions in service
- What services are covered and between what hours?
- Access to the data in the event of loss
- Integrity of the data
- Location of the data
- Termination: avoid vendor “lock-in”, check other grounds of termination
- Insolvency events
- Data retention – how long will data be stored before it is deleted by Vendor? Is there a charge for retention?
- Ensure backups to local hard drives can be effected
- Intellectual property rights
- Security
- Disaster recovery & local backups
- Migration of data
Privacy considerations

Australian principles

- Australian Privacy Principles are only relevant in Australia.
- **Privacy Act 1998** (Cth)
  - Personal Information – s.4
    - ...information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
  - Includes biometric data
  - s.4.(2) Personal information includes such things as an individual’s fingerprints, retina prints, body samples or genetic characteristics.
- Schedule 1 of the **Privacy Act 1988** (Cth), contains thirteen Australian Privacy Principles
- Health data – such as medical records are subject to the **Health Records and Information Privacy Act 2002** (Cth).
Privacy considerations

Australian principles

➢ Private organisations
  ➢ Australian Privacy Principles (APPs)
  ➢ Approved Privacy Codes – Pt.3AA

➢ Cth government agencies
  ➢ Information Protection Principles (IPPs) – s.14
1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information
Privacy considerations
Australian Privacy Principles

➢ Australian Privacy Principle 8 deals with trans-border data flows:
  ➢ An entity in Australia may only transfer personal information about an entity or an individual to someone (other than the entity or the individual) who is in a foreign country only if certain criteria are satisfied

➢ Australian Privacy Principle 11 on Security of Personal Information:
  ➢ An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure
Privacy Considerations

What are the remedies for breach?

- Complaint to Privacy Commissioner – s.36
  - Privacy Commissioner powers – s.52
  - Apology
  - Change in practices
  - Order for access / amendment / deletion
  - Compensation (incl. injury to feelings or humiliation)
Privacy Considerations

Common Law

- No right to privacy at common law
  - “Any person is entitled to look over the plaintiff’s fence and to see what goes on in the plaintiff’s land. If the plaintiff desires to prevent this, the plaintiff can erect a higher fence”: *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 per Latham CJ at 494

- *Grosse v Purvis* [2003] QDC 151:
  - Queensland District Court found a breach of privacy to have occurred as a result of the defendant stalking the plaintiff over a prolonged period.
  - Skoien SDCJ took what he viewed as “a logical and desirable step” and recognised “a civil action for damages based on the actionable right of an individual person to privacy”.

- Skoien SDCJ identified the following elements of a breach of privacy:
  - A willed act by the defendant
  - Which intrudes upon the privacy or seclusion of the plaintiff
  - In a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities
  - Which causes the plaintiff detriment in the form of mental psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which she is lawfully entitled to do
Privacy Considerations

International

- United States
  - Nearly all US states now recognise either a statutory right to privacy or at common law

- European Union
  - The European Convention on Human Rights (ECHR) contains a right to private and family life, home and correspondence
  - It is interesting to note that in April 2014 European Union rejected wide data retention laws that would force telephone companies to keep citizen’s communications data for up to two years

- United Kingdom
  - *Data Protection Act 1998*
  - ‘English law knows no common law tort of invasion of privacy’: *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920 at [272]

- Canada
  - There is no common law tort of invasion of privacy in Canada. British Columbia (1968), Manitoba (1970), Saskatchewan (1974), and Newfoundland and Labrador (1981)—have statutory causes of action for invasion of privacy

- New Zealand
  - In *Hosking v Runting* a majority of the New Zealand Court of Appeal recognised a common law tort of privacy
Due Diligence

What to look for

➤ How will the data be stored and in what format?
➤ Where will the data be stored?
➤ Who has access to the data?
➤ If data is replicated to more than one site, where are the sites and how is this done?
➤ What are the technical controls?
➤ What is the security around the data centre? Does it comply with ISO27001?
➤ See the documentation and ask for test results
➤ Visit the data centre
➤ Use the system on a trial basis
➤ Carry out reference checks
Security Issues

Practical checks

- **Physical security**: check physical security at data centre
- **Data security**: check the hardware and software security deployed at the data centre e.g. firewalls
- **Encryption**:
  - Is encryption done for the whole of the data flow or only at certain points?
  - What if keys are lost? How can data be recovered?
- **Auditing**:
  - Request certifications, confirm how regularly these are done
  - Are random penetration tests undertaken
Security Issues
ISO 27001

1. Risk Assessment
2. Security Policy: management direction
4. Asset Management: inventory and classification of information assets
5. Human Resources Security: security aspects for employees joining, moving and leaving an organisation
6. Physical and Environmental Security: protection of the computer facilities
7. Communications & Operations Management: management of technical security controls in systems & networks
8. Access Control: restriction of access rights to networks, systems, applications, functions and data
9. Information systems acquisition, development and maintenance: building security into applications
10. Information Security Incident Management: anticipating and responding appropriately to information security breaches
11. Business Continuity Management: protecting, maintaining and recovering business critical processes and systems
12. Compliance: ensuring compliance with information security policies, standards, laws and regulations
Regulatory Compliance
What to look for

- APRA standards and guidelines
  - Requires consultation before offshoring data
- Business continuity & best practice:
  - Continue operations following loss of cloud services
  - Confidentiality and integrity of sensitive data
  - Compliance
- Privacy legislation
  - APP 8
  - APP 11
- Corporations legislation
In whose possession, control or custody is the data?

If possession comes down to “ownership”, international case law presents issues in determining possession of intangible property as described above.

The contract may determine who owns or controls the data.

What if the user will not provide user names and passwords to access data stored in the Cloud?
Even if data is obtained from the Cloud, it still must be examined in accordance with the Electronic Discovery Reference Model.
Information must be relevant so if third party subpoenas are required, parties need to show relevance and also that the scope of discovery is limited to avoid unnecessary cost and delay

Information on social media is capable of being discoverable

No Australian cases of which we are aware

USA judges have struggled with logistics of making social media information discoverable: no definitive way forward

- Judge’s have privately reviewed the information in advance to determine if it should be disclosed (*Offenback v Bowman* 2011 WL 2491371 (M.D. Pa. June 22, 2011))
- Judges have become “friends” with a party to determine if private Facebook posts were relevant (*Barnes v CUS Nashville LLC* 2010 WL 2265668. (M.D. Tenn.))
- Judges have required parties to turn over physical access ie usernames and passwords, for social media accounts to the other party (*Largent v Reed* 2009 1823 (C.P. Franklin Nov. 8, 2011))
- A court has fined both a party and his lawyer for “cleaning up” a Facebook page to remove harmful posts and pictures (*Lester v Allied Concrete Co* 736 S.E.2d 699 (2013))
USA Patriot Act

- Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001
- Purpose to target terrorism
- Not intended to grant unfettered access to data
- Applies to any company with a presence in the USA regardless of where data is held
- Other counties: Mutual treaties

Stored Communications Act

- A valid subpoena issued in relation to a criminal investigation can compel disclosure of basic subscriber records
- A search warrant showing probable cause can compel disclosure of stored contents of any account including messages, photos, videos etc
- Facebook makes it clear in their “data use policy” that information may be disclosed pursuant to a legal request including those outside of the USA
Contact Details

➤ Allison Stanfield
➤ CEO
➤ e.law International
➤ (02) 8114 1717
➤ a.stanfield@elaw.com.au