Cloud law challenges

COSC349—Cloud Computing Architecture

David Eyers

Learning objectives

- Understand that cloud computing is **multi-jurisdictional**
- Appreciate that **regulation of cloud technology** is emerging more slowly than then technology itself
  - … and **may well be inconsistent** across jurisdictions
- Outline how users' rights about their **sensitive data** are increasingly being protected by regulation

Cloud computing poses legal challenges

- Law and regulation apply to many aspects of cloud
  - **Business contracts**—money changing hands → lawyers
  - **Handling of data**—rights and responsibilities → lawyers
  - **Government control**—local policy requirements → lawyers
- There are **many stakeholders** in cloud interactions
  - Provider, DC, tenant, client, … plus further delegation targets
- Cloud computing is "**frontier country**" in terms of law
  - Changes in what's possible faster than regulation can keep up

Law lagging technology—cloud services

- **Outsourcing** is well established and well understood
  - Outsourcing in traditional business: **contract carefully written**
    - Clear outsourcing organisation and target organisation
    - Documentation of timing or other means to measure success
- Cloud outsourcing **relationship can be dynamic**
  - Automatic selections from a marketplace? short-lived; *ad hoc*
- Consider the amount of time large court cases take
  - Slow speed and high detail; legal processes very expensive

Jurisdiction—where law applies

- Jurisdiction has many levels:
  - International aspects: countries or entities like EU
  - Within a given country: *e.g.*, US federal, state and local
  - Across different types of regulation: *e.g.*, tax law

- International law is likely to be particularly complex…

- Cloud computing **involves many jurisdictions**:
  - Providers must respect law in different jurisdictions (simultaneously)
  - State of law may take time (& judgements) to become clear

Additional cloud outsourcing complexities

- Delegations and outsourcing **can be multi-stage**
  - Dropbox's SaaS over AWS PaaS; Heroku's PaaS over AWS IaaS
  - Apple uses Google, Microsoft and Amazon cloud services

- What is the priority for **liability and responsibility**?
  - Where the cloud **computing** is done?
  - Where responsible **company** is based (or say they are based)?
  - Where the **data** is stored?
  - The jurisdiction of the **owner** of the data?

Stakeholders' approaches to law & its risks

- Cloud providers' approach (compliance / avoid risk):
  - **Disclaim everything** (also true of software licenses)
  - Handle each **jurisdiction** / negotiate **special arrangements**
  - Use **technology to avoid liability** in the first place

- Regulatory bodies' (*e.g.*, government) approaches:
  - EU **GDPR**—General Data Protection Regulation
  - US **CLOUD Act**—Clarifying Lawful Overseas Use of Data Act
  - EU **Digital Services Act**, **Digital Markets Act**, coming **AI Act**

AWS Service Terms & Customer Agreement

- AWS Service Terms is a 40,000+ word document
  - (Otago PhD theses have a maximum length of 100,000 words)
- AWS Customer Agreement includes phrases such as:
  - "We … make **no representations or warranties of any kind** … regarding the service offerings."
  - "Disclaim all warranties … that any **content will be secure** or not **otherwise lost or altered**."
  - "[we'll not] be **responsible for any compensation**, reimbursement, or damages arising in connection with … any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or **failure to store any of your content or other data**."

Amazon GovCloud

- Pragmatic organisation of **different service contract**
  - Allow US government organisations to be sure of compliance
  - Also those defined relative to US Govt., such as contractors
  - Mechanisms keep data in USA; also run entirely by US citizens
- **Technically an AWS region** (in the USA) complying with:
  - US International Traffic in Arms Regulations (ITAR)
  - Fed. Risk & Authorization Management Program (FedRAMP),
  - Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Impact Levels 2, 4, and 5

GDPR

- Empowers **EU citizens** when in the EU
  - Get information about processing of your personal data
  - Obtain access to personal data held about you
  - Ensure that errors in personal data are corrected
  - Request personal data be erased
  - Request restriction of processing of your personal data
  - Object to use of personal data for marketing
  - Receive your personal data in machine-readable format
  - Learn decisions using automated processing of your p.d.

GDPR

- Most cloud users are not EU citizens within the EU… but it's just **too hard to make that distinction** practically
  - Partitioning EU and non-EU would have to operate across all data storage and data processing platforms—expensive
  - Also, many other jurisdictions may introduce similar regulations
- GDPR rights are being **exercised against social media**
  - … but not so much against general cloud services, *etc*.
- Also, GDPR more used by governments than citizens
  - *e.g.*, citizens are empowered, but larger parties actually act

US CLOUD Act

- Aims to improve **US access to data** stored in other jurisdictions, *e.g.*, for law enforcement
- Cloud providers **required to disclose data** they see if:
  - US has jurisdiction over target entity;
  - Entity is electronic comms. or remote computing service;
  - Target entity has possession, custody or control over data;
  - Local enforcement authorities obtain legal access to data

- … GDPR & CLOUD Act **incompatible when introduced**

NZ situation

- Soon (?) to gain **Microsoft Azure + AWS regions in NZ**
  - Previously NZ only had good, smaller local clouds, but…
    - were **not big-player-equivalent** services; **not required to host locally**

- Sensitive NZ cloud workloads typically run in Australia:
  - but then NZ inherits Australian Government side-effects, *e.g.*,
  - recent AU law regarding **access to encrypted data**:
    - "The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia,"—Turnbull (2017)
  - AU **social media law**: criminalises hosting abhorrent content

Cautionary tale: the demise of Code Spaces

- Code Spaces provided code hosting—used AWS
- Their **cloud architecture seemed very good**
  - Used EBS with snapshots; S3 for backups; …
- Attacker got access to their AWS control panel
  - Extortion demands made by attacker to Code Spaces' staff
  - Code Spaces changed AWS password
- **Attacker had backup credentials** and took action:
  - Deleted EC2 instances, EBS volumes and snapshots; S3 buckets
- Worth asking: **what's the worst that could happen**?