



**Driving Innovation  
Through the Information  
Infrastructure**

**SPRING 2011**



# **Don't Get Lost in the Cloud: Legal Risks and Implications of Cloud Computing**

Milton L. Petersen

Partner - Information Technology Practice Group  
Hunter, Maclean, Exley & Dunn, P.C.

(912) 238-2629

[mpetersen@huntermaclean.com](mailto:mpetersen@huntermaclean.com)

[www.huntermaclean.com](http://www.huntermaclean.com)

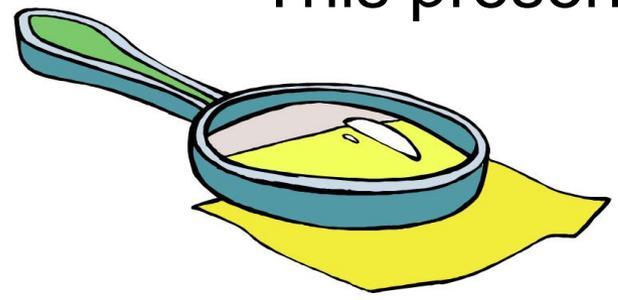
# Nephophobia



- an irrational fear of clouds

This presentation is to make you

**AWARE**



**NOT**

To dissuade or scare

- External sourcing is becoming the rule, not the exception

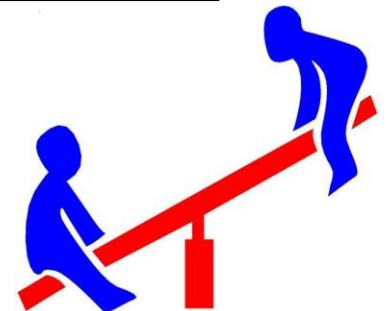


# Overview

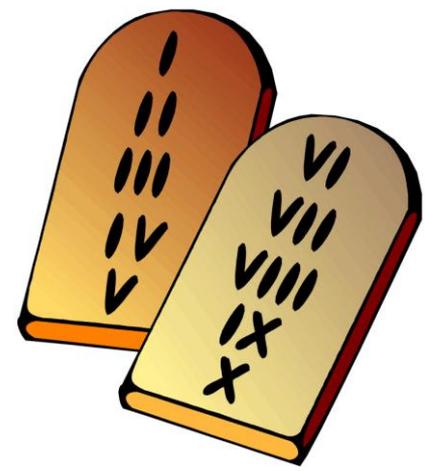
- Due diligence
- Data privacy and security
- eDiscovery / litigation holds
- Service level agreements
- Other contractual provisions

# Due Diligence

- Identify prospective service providers
- Review and compare:
  - Pricing
  - Functionality / features
  - Customer experiences / feedback
    - User groups, conferences, etc.
    - Online searches
  - Form agreements / standard terms
    - Use to distinguish among vendors
- Assess potential leverage



# Form Agreements / Standard Terms



- Look for firm commitments
  - “Vendor shall / shall not ...”

## **Not** wiggle-room

- “Vendor shall strive or endeavor to ...”
- Goals, targets, objectives, etc.

- Levels of efforts

- Recognized standards
  - Commercially reasonable efforts
  - Best efforts



# Data Privacy and Security

- Represent some of the primary legal risks of cloud computing
  - Cloud customers no longer have physical control of data
    - But still are legally responsible (and potentially liable)

# Data Privacy and Security (cont'd)

Regulatory concerns include:

- HIPAA and HITECH
  - Health care
- Gramm-Leach-Bliley
  - Financial services
- Sarbanes Oxley
  - US public companies
- FTC enforcement actions
- State data privacy laws
- Export control regulations
- EU Data Protection Directive



# Data Privacy and Security (cont'd)

## Assess Risks:

- What data will be stored?
  - Any personal data?
    - Individuals from what states or countries?
  - Will data be encrypted?
- Where will data be stored?
  - Can you specify or limit locations?
- Who will have what rights to data?
- Who can access data?
- When / how will data be returned?



# Data Privacy and Security (cont'd)

## Applicable standards

- **SAS70**
  - Type II Reports
  - Correction of deficiencies
- **SSAE 16**
  - Designed to supersede SAS70
  - Reporting on controls at a service organization
- **ISAE 3402**
  - International standards
  - Assurance reports on controls at a service organization

# Data Privacy and Security (cont'd)

## Standards / Certifications

- ISO/IEC 27001
  - Security management system

## Compare vendors / terms

- Data security policies
- Audit rights
- Customers need:
  - Operational visibility
  - Customer validation of controls

# Data Privacy and Security (cont'd)

- Other issues:
  - Specific security measures
  - Data retention
  - Data backups
    - Frequency
    - Remote storage
    - Access by customer?
    - Copies to customer?
  - Disaster recovery



# eDiscovery / Litigation Holds

- Legally required provision of copies of data or retention and preservation of data
  - Applicable regardless of industry
  - Failures to comply may be severe
  - Especially applicable to email, document collaboration, etc.





# eDiscovery / Litigation Holds (cont'd)

- Notification by service provider
  - Prior to disclosure
  - Unless prohibited by law
- Duties for service provider to cooperate and assist
  - Additional costs?
- Access to or provision of data
- Retention or preservation of data

# Confidentiality

- Definition
- Meaningful obligations
- Downstream obligations
  - Subcontractors, employees
- Permitted uses and disclosures
- Required / compelled uses and disclosures
  - Notification
    - Unless prohibited by law
  - Right to contest / obtain protective order
- Return or destruction
  - Secure method of destruction



# Performance-Related Risks

- In addition to data-related risks,



there are also many performance-related risks



# Service Level Agreements

- Common service levels:
  - Availability / uptime
    - Percentage of time application or service “up” and available for use
  - Internal response time
    - Mainly for applications (SaaS)
    - Average elapsed time in which transactions complete
    - Typically excludes network time



# Service Level Agreements (cont'd)

- Things to consider:
  - Required levels of performance
    - A small percentage of a big number may still be a big number
    - Averages may be misleading
  - Metrics / calculations
    - Frequency of calculation
    - Exclusions / exceptions
  - Visibility / reports



# Service Level Agreements (cont'd)

- Service credits
  - Added days of service
  - Percentage or flat amount of fees
    - May vary considerably among vendors
  - May not cover actual damages
  - Caps
    - Percentage of monthly fees
  - Automatically applied or only if requested?



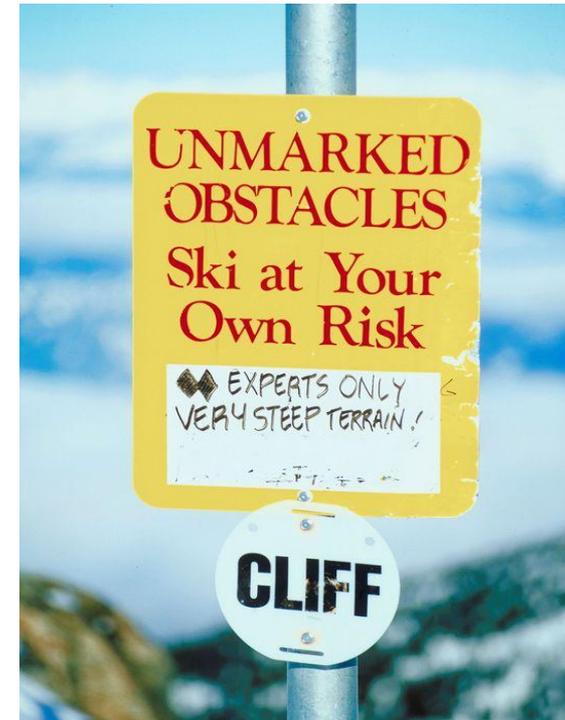
# Service Level Agreements (cont'd)

- Sole and exclusive remedies
  - Service credits may not cover actual damages
  - Customer should be able to terminate
    - Chronic / recurring failures
    - Provision of data
    - No additional cost



# Other Contractual Provisions

- Many other contractual terms allocate risk between the parties
- Be aware of risks, even if better terms can't be negotiated



# Other Contractual Provisions (cont'd)

- Description of services
  - What must the service provider do?
- Warranties
  - Authority
  - Basic services warranty
  - Software applications
  - No malicious code



# Other Contractual Provisions (cont'd)

- Indemnification
  - Intellectual property
  - Security breaches
- Insurance
  - Cyber-insurance coverage
- Audit rights
  - Fees
  - Compliance





# Other Contractual Provisions (cont'd)

## Limitations of Liability

- Cap on direct damages
  - Reasonable and mutual
- Exclusion of indirect damages
- Exceptions
  - Breaches of confidentiality
  - Security breaches
  - Indemnities



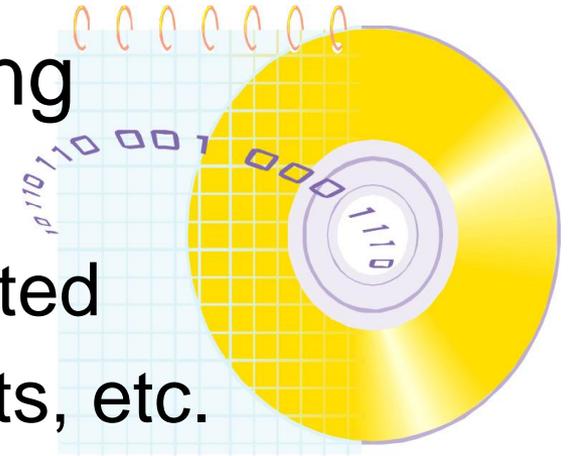
# Other Contractual Provisions (cont'd)

## Term and Termination

- Length of term
  - Caps on renewal fees
- Termination rights
- Transition assistance
- Data portability
  - Data + metadata
  - Return or export capability

# Other Contractual Provisions (cont'd)

- Data rights
  - All rights should belong to cloud customer
    - Data provided or created
    - All summaries, extracts, etc.
    - Metadata
  - Service provider may only use as necessary to provide services during the term



# Don't Get Lost in the Cloud:

## Legal Risks and Implications of Cloud Computing

- Questions?

Milton L. Petersen

Partner - Information Technology Practice Group  
Hunter, Maclean, Exley & Dunn, P.C.

(912) 238-2629

[mpetersen@huntermaclean.com](mailto:mpetersen@huntermaclean.com)

[www.huntermaclean.com](http://www.huntermaclean.com)