

# Cloud Computing: Managing the Legal Risks

**Jacqueline Klosek**

**June 23, 2009**

# Agenda

- Privacy and Data Security Concerns
- Protection of Corporate Assets and IP
- Jurisdictional Issues
- Export controls
- Tax Implications

Don't put anything in the cloud you wouldn't want a competitor, your government or another government to see.”

World Privacy Forum Report on Cloud Computing and Privacy  
<http://www.worldprivacyforum.org/cloudprivacy.html>

# Legal Concerns for Cloud Customers

- Terms are often unilaterally dictated by the provider and are usually very protective of the provider
  - Unilateral modification rights
  - Limits on liability
  - Lack of indemnities/warranties
  - Lack of strong security commitments
  - Reservation of rights to respond to subpoenas and other requests
- Example:
  - “you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content.”

# Key Questions to Consider

- Can the data at issue be legally shared with the provider and stored in the cloud?
- What are the providers' policies with respect to stored data?
- What measures does the provider have in place to ensure those policies will be maintained?
- Can you be sure you are meeting your legal obligations and contractual commitments when storing data in the cloud?
- What rights does the cloud provider have with respect to the stored data?
- Where is the data stored?
- What happens when the provider is acquired by another entity? Or faces bankruptcy?

# Privacy and Data Security Concerns

- Legal Issues impact Company's ability to store certain data in the cloud and govern conditions of storage
  - Laws and Regulations: HIPAA/HITECH Act; GLB Act state laws
  - Other Legal Requirements: privacy policies; contractual commitments; professional secrecy obligations; legally privileged information
- Legal liability; breach of contract claims; fines and penalties; loss of customers and negative publicity are possible results
- State laws and HITECH Act may require company to notify customers upon breach of data security

# Privacy and Data Security Concerns

- International data capture, storage and maintenance
  - Ultimate location of data may be overseas
  - Local privacy laws may apply
  - Many foreign policy laws are more restrictive than those in U.S. and may limit cross-border data transfers
  - Attachment may be permanent

# Privacy and Data Security Concerns

- **Government and Third Party Access to Information**
  - Third parties may be able to access information stored in the cloud more easily than when it is stored with the original owner
  - User policies may determine expectation of privacy and therefore define the scope of Fourth Amendment protection. See *Warshak v. U.S.* (6th Cir. 2007)
  - Computerized/programmed scans (e.g. for viruses or pornography) versus right to monitor content

# Jurisdictional Issues

- Data may be moved from jurisdiction to jurisdiction
- Impact on privacy and legal compliance
- Export control issues
  - Criminal and civil penalties up to \$1M or 10-20 years in prison
  - May lose exporting privileges
- Applicable Law?
  - Law of storage location
  - Choice of Law provision

# Protection of Corporate Assets and IP

- Trade secrets
  - Uniform Trade Secrets Act requires a reasonable effort to maintain secrecy of trade secrets
  - Subpoena of cloud provider by third party of trade secret
- Pre-existing confidentiality obligations
- Data ownership issues

# Tax Implications

- Constitutional requirements for taxation:
  - Substantial nexus
  - Fairly apportioned
  - No discrimination against interstate commerce
  - Fairly related to services
- Is location of a cloud provider sufficient to establish a “substantial nexus”?
  - New York and Amazon.com case
  - At least eight other states considering following New York’s lead

GOODWIN | PROCTER

Questions?

Jacqueline Klosek

(212) 459-7464

[jklosek@goodwinprocter.com](mailto:jklosek@goodwinprocter.com)