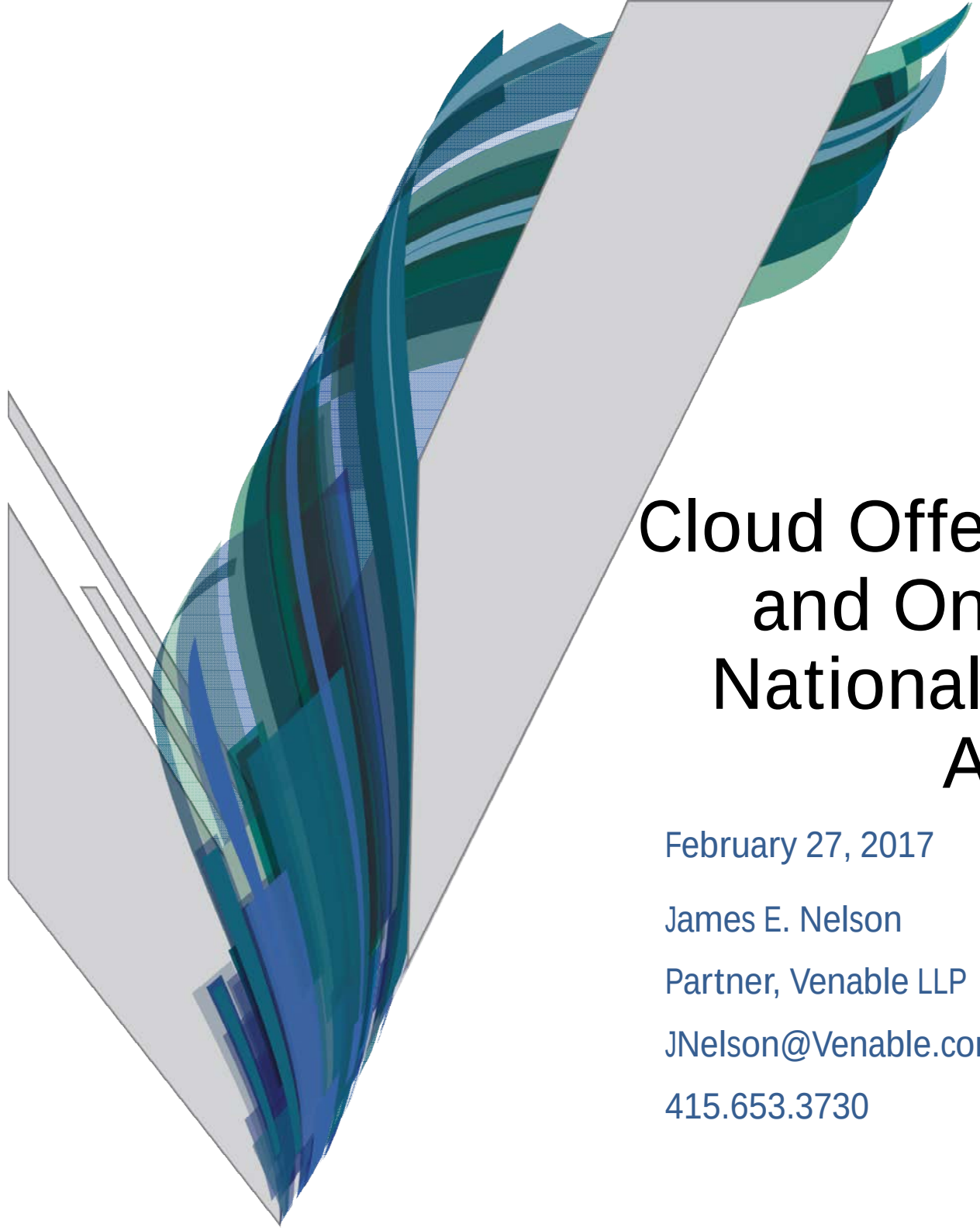


VENABLE LLP

Cloud Offerings, Cybersecurity and Online Contracting National Business Officers Association

February 27, 2017

James E. Nelson

Partner, Venable LLP

JNelson@Venable.com

415.653.3730

Venable LLP

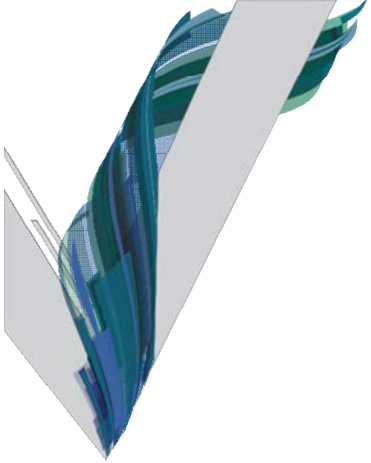
- Full-service law firm with over 600 attorneys practicing in:
  - Corporate and business law
  - Intellectual property
  - Government affairs
  - Complex litigation
- Headquartered in Washington, DC, with offices throughout the country, including New York, San Francisco, and Los Angeles

Highlighted Services:

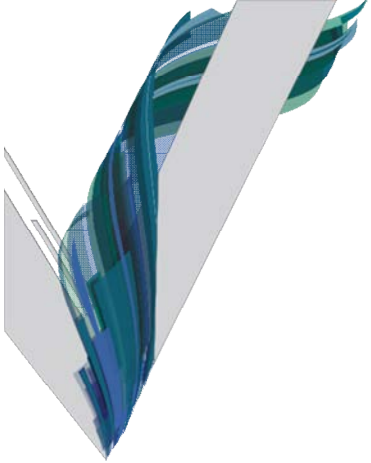
- Consumer Products and Services
- Education
- Healthcare
- Regulatory
- Technology
- Private Equity
- Privacy and Data Security
- Intellectual Property

Jim Nelson
Partner-in-Charge, San Francisco Office

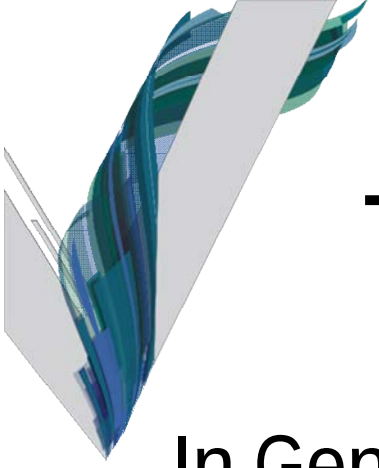
- Practicing in San Francisco and New York
- Highlighted areas of practice:
  - Technology Transactions and Outsourcing
  - Corporate
  - Privacy and Data Security
- Highlighted industries:
  - Technology-enabled companies
  - Education
  - Life Sciences and Pharma
  - Financial Services



Cloud Overview



What is the Cloud?



The Cloud Defined . . .

In General. . .

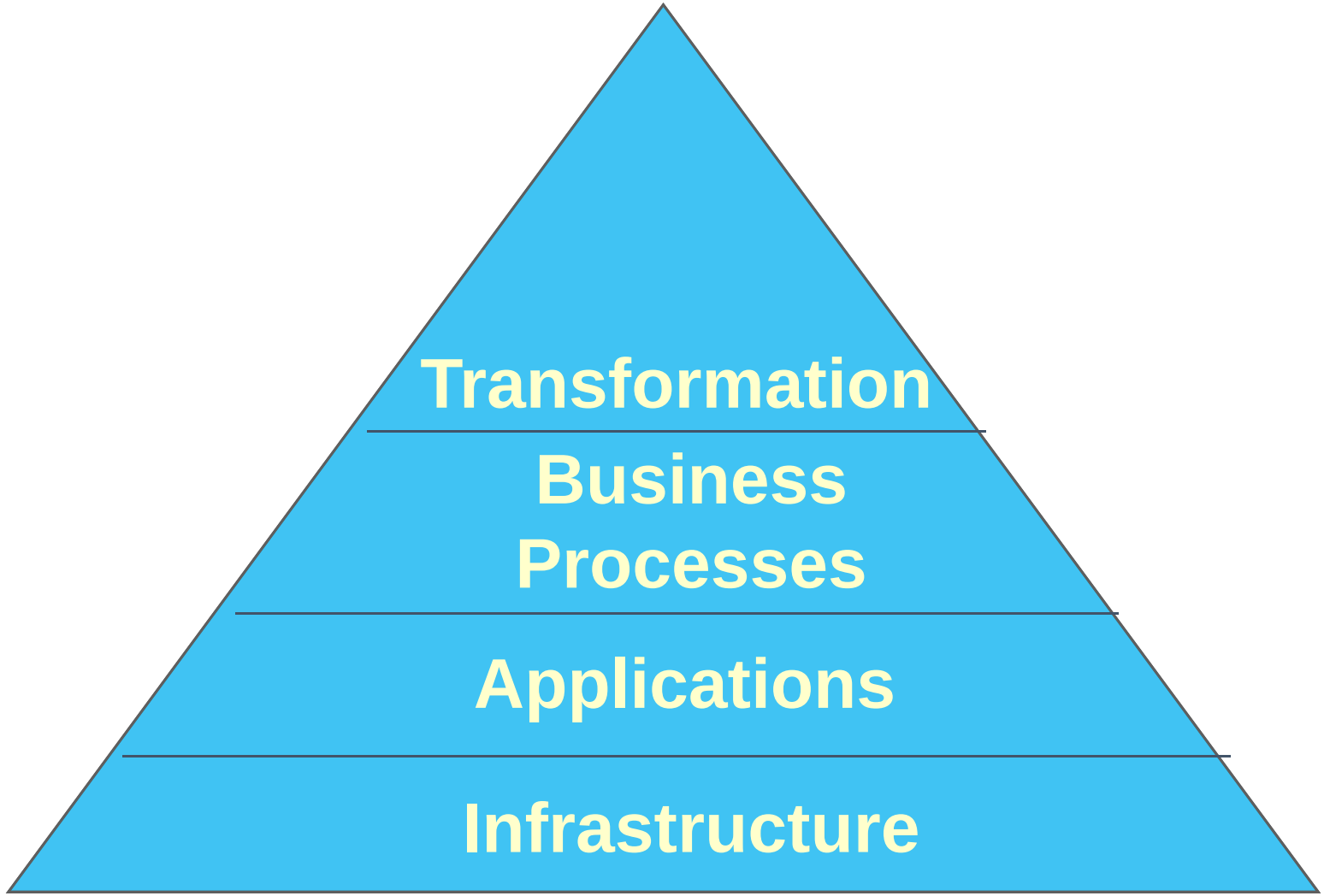
Cloud computing is a model for enabling **ubiquitous**, **convenient**, **on-demand** network access to a **shared pool** of **configurable computing resources (e.g., networks, servers, storage, applications, and services)** that can be **rapidly provisioned and released** with minimal management effort or service provider interaction.

– National Institute of Standards and Technology

Typical Cloud-Based Business Functions

- Typical business function areas:
  - Finance and Accounting
  - Student Records
  - HR
  - IT
  - Customer Support/CRM
  - But moving up the scale on level of complication . . .
- Generally NOT core value-drivers of the business
  - Special issues if you do (e.g., IP, Confidentiality, Restrictive Covenants)

Evolution of Cloud-Based Functions



Cloud Service Delivery Models

- Infrastructure as Service (IaaS)
- Platform as Service (PaaS)
- Software as Service (SaaS)

Infrastructure as Service (IaaS)

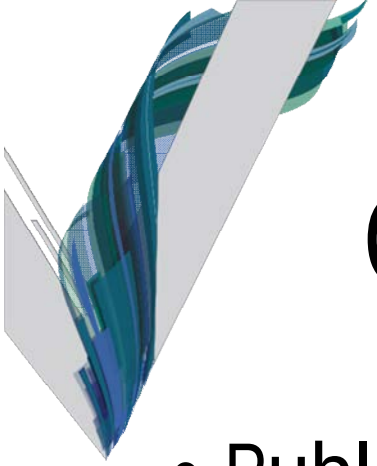
- The user is purchasing access to the Cloud provider's hardware to build and run systems and applications of the user's choice
- Example: Rackspace
- Advantages Include: Greatest control and customizability

Platform as Service (PaaS)

- This model allows the user to install and configure any number of software application on the cloud provider's servers and operating systems.
- Example: Microsoft Azure
- Advantages Include : Standard foundation (hardware and operating systems), but greater flexibility for the application and database layer.

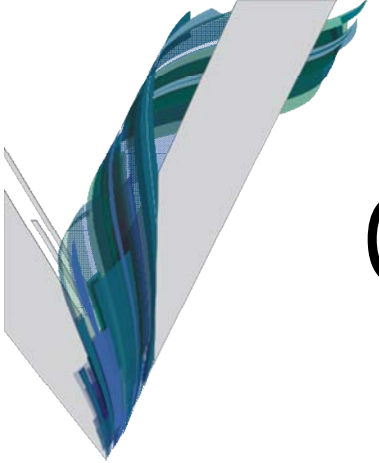
Software as a Service (SaaS)

- The user gets on-demand, ubiquitous access to current version of software application.
- Example: Salesforce.com
- Advantages Include: Cheaper to acquire and lower total cost of ownership, flexible and remotely available.



Cloud Deployment Models

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud



Cloud Computing Benefits

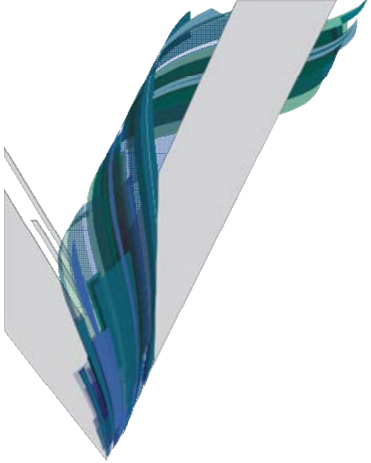
- Choice and Flexibility
- Cost savings and efficiencies
- Access to greater computing power
- Earlier access to new technologies
- Better security
- Better system redundancies

Cloud Computing Challenges

- One to many architecture
- Everything in offering is “Standard”
- Lack of transparency on delivery
- Access to data
- Concerns on cross-border transfers
- Ability to support customer’s compliance/reporting needs

Unique Concerns

- Requirements that cannot be fixed by negotiation
  - Selecting the right service provider is critical
    - Check references
- Know the exit going in
  - Know what transition out will be like
  - Ensure you have what you need when you leave (e.g., data)
- Know from where the services are being delivered
- Know that audit and security requirements can be met



Contracting Process

Assemble the Team

- Business – Who owns the functions now?
- Technical – How are functions performed?
- Operational/Governance – How are functions managed?
- Compliance – What are organizational compliance obligations?
- Financial – What does it cost to deliver?
- Legal – What is our current risk in operations and delivery?

Assemble Information and a Plan for Acquisition

- How do we operate today?
  - How our we receiving services now?
  - What is our existing cost?
  - What is our existing security level?
  - What is our existing disaster recovery/business continuity?
- Formal RFP vs. Informal Selection Process
- Consider a third party advisor or skilled attorney
- Consider a cloud computing template or checklist

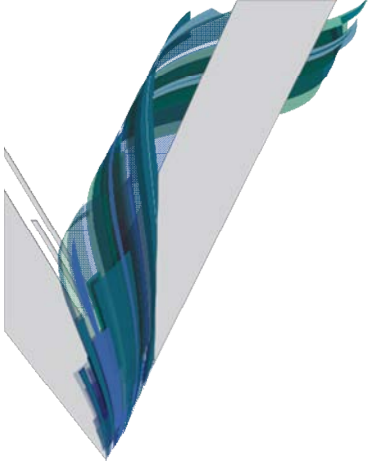
Negotiate and Contract

- Customer often is heavily reliant on the service provider
  - Customer often has little or no capability to perform functions itself once it moves to the cloud

- In a sense, all you (the customer) have is a contract
  - The contract documents the services, the obligations, and the means to achieve the customer's objectives
  - Critical to "get it right," especially the key provisions

Types of Contracts

- Browsewrap
  - A simple hyperlink on the page or encountered as a user accesses the product
  - Enforceable, though courts are suggesting some discomfort with this approach to enforce meaningful terms
- Clickwrap
  - “I accept”
  - Enforceable
- Signed Agreement
  - Still be best way to negotiate and document an agreement or understanding
  - Don’t let vendors drive form over substance with PDFs or other immutable documents. Know up at the beginning if an agreement will be negotiable



Contract Terms

Cloud Contract Terms

- Service Description
- Change Control
- Service Levels
- Governance/Personnel
- Pricing
- Warranties
- Indemnification
- Limitation of Liability
- IP Ownership
- Data Flow, Location and Access
- Contract Performance Audit
- Compliance/Audit
- Disaster Recovery/Business Continuity
- Termination Assistance

Services Description

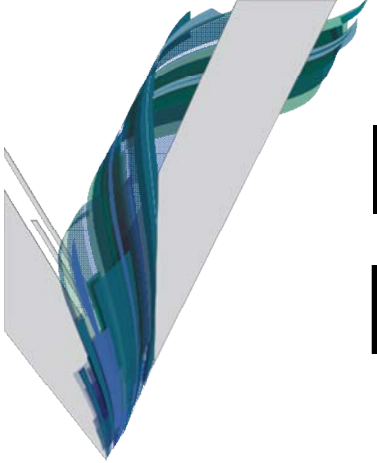
- Should include:
  - Services described in a services schedule
  - Services described in the displaced budget
  - Services included in job descriptions displaced by moving to the cloud, if any
- Services description should tie directly to pricing
- Time here is time well spent. . .
  - Allocate risk
  - Confirm parties agree who, what, where, how and when services are being provided

Service Levels

- Objective is not to cover every possible failure
  - Start broad and focus as need be
- SLAs should be:
  - A manageable number
  - Objective
  - Measureable
  - Verifiable
- Often tied to governance for adjustment over time
- SLAs might or might not have credits (i.e., solely reporting)
- Tied to pricing

Intellectual Property

- Buckets:
  - “Your Stuff”
  - “My Stuff”
  - “New Stuff”
  - “Some Other Person’s Stuff”
- Drive discussion based on real facts and needs



Intellectual Property – Discussion Drivers

- Customer's Interests
  - Value for fees paid
  - Not having to pay twice for something that's needed after the deal is done
  - Advantages over competition
  - Protection of client's confidential information

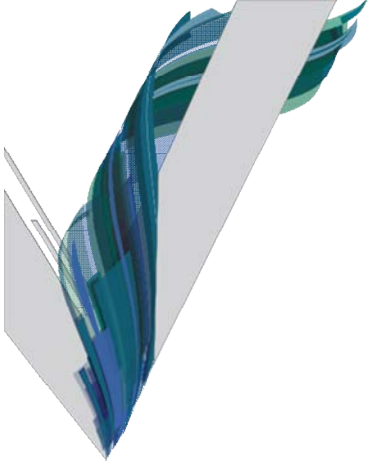
- Service Provider's Interests
  - Ability to grow their business (especially in a shared services environment)
  - Desire to serve other clients in the same sector
  - Avoid undue or unintentional interference with future business operations

Additional Key Business Terms Not to Overlook

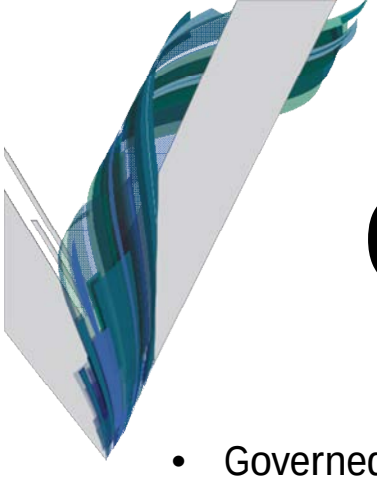
- Governance
- Security
- Compliance
- Audit
- Termination Assistance

Liability/Indemnity – Considerations

- What are the greatest exposures in connection with the service?
- How will the customer's overall risk profile be affected by the services or deliverable?
- Is one of your goals to reduce risk?
- What is your risk tolerance?
- Who is in a better position to mitigate the risk?
- What is the relation between risk and pricing – e.g., high-revenue custom cloud services versus low-cost/margin commodity cloud services?

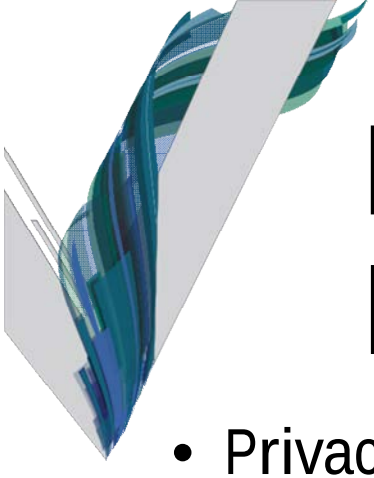


Privacy



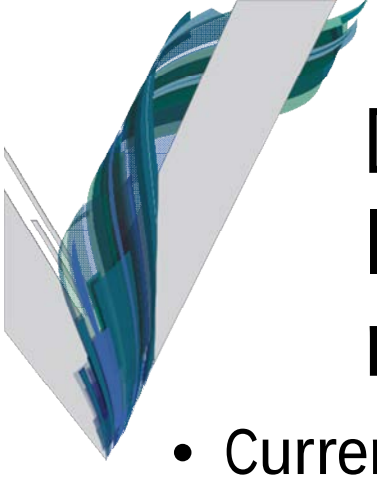
General Considerations

- Governed by a patch work of federal, state and local laws as well as industry standards.
  - Key Laws and Standards at Issue:
    - FCRA-For Consumer Finance Information
    - HIPAA-For Personal Health Information
    - HITECH-For Personal Health Information
    - GLB-For Banking-related Information
    - Various State Data Breach Laws
    - Federal Rules of Civil Procedure (Discovery in Litigation)
    - PCIDSS-Industry Standards for Protection of Payment Card Information
    - Data Export Restrictions
    - Patriot Act
  - General Requirements:
    - Limit access on an “as needed basis”
    - Allow access and review by data subject
    - Allow updating by data subject
    - Provide notice of data loss to data subject (often includes credit monitoring obligations for some period of time)



Legal / Regulatory Concerns - Practical Steps

- Privacy
  - Sensitive data management -- identify which data meets compliance and security requirements
  - Data protection and obfuscation -- prevent leakage of personal or commercially sensitive data
  - Cloud utilization management -- control unauthorized cloud adoption
  - Cloud compliance management -- ensure cloud utilization is compliant with government and corporate regulations
  - Audit and reporting controls -- provide details about data use for support and compliance
- Location
  - Data location management -- control where personal or commercially sensitive data is at all times
  - Application data access controls -- ensure cloud access to corporate data is controlled
  - Application integration management -- bring multiple cloud applications into the enterprise simultaneously
  - Data access, migration, and recovery -- avoid application and vendor lock-in, ensure data is owned and managed by and at the direction of the enterprise (as data controller), not by the cloud vendor (as data processor).
- Security
  - Application access management -- prevent unauthorized access to the cloud systems and data, control data transfers
  - Threat monitoring and management -- identify hack attacks on or coming through a cloud vendor
  - Attack identification and prevention -- actively prevent known attack vectors
  - Cloud application disaster recovery -- assist with business continuity during cloud outage
  - Cloud application migration -- avoid vendor lock-in by keeping data in house at all times
  - Cloud application redundancy -- use more than one cloud to improve SLAs

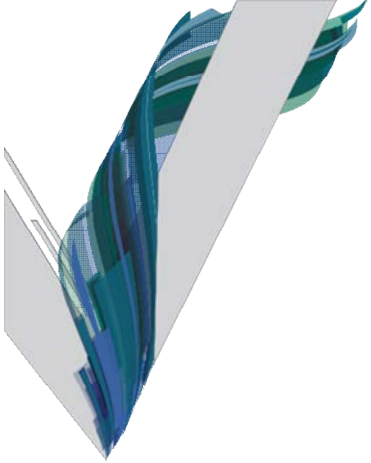


Data Protection & Data Security in the US Implications of getting it wrong – i.e. we really should care

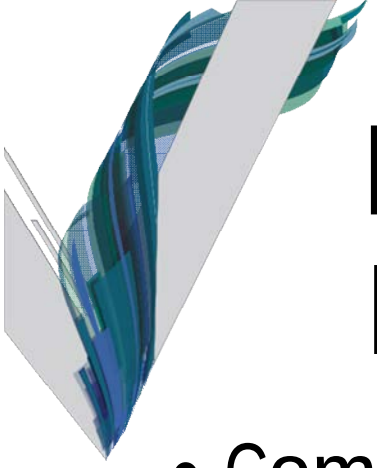
- Current situation
  - Patchwork of laws makes compliance more challenging
  - Consideration of having preemptive federal legislation
  - Until then, know the sources for information on privacy compliance
  - Know that laws generally apply to where the data subject is located and where the data is located
- Most Risky Information
  - PHI-Personal Health Information
  - PII-Personally Identifiable Information
- Penalties
  - Fines
  - Credit Monitoring Services
  - Support of a customer hotline
- Other Damages
  - Reputation

Solutions

- Consider whether all data should be going to the cloud
- Confirm whether you have rights to treat data as you will be handing it to a cloud provider
- Have a standard security addendum to include or use as a reference document



Potential Litigation



Potential Litigation Impacts of Moving to the Cloud

- Companies that store data in the cloud or which use cloud based applications may face complications when seeking to preserve and produce data from the cloud.
- Factors outside the party's control could impact that party's access to data.
- The data stored in the cloud may be subject to legal and regulatory restrictions of which the company may be unaware.
- Data may change physical locations (EU v. US)

Possession, Custody or Control in the Cloud

- Under F.R.C.P. 26 a party to a litigation is required to preserve relevant documents and information that is under its possession, custody or control
- Courts have held that data in the hands of a third party is under the possession, custody or control of the party to a litigation if that party has the practical ability to obtain the information (e.g. Flagg v. City of Detroit, 252 FRD 346, E.D. Mich. 2008)

Solutions

- Make sure access to data is part of your contract requirements
- Consult an attorney early

Questions?

James E. Nelson
Partner, Venable LLP
JNelson@Venable.com
415.653.3730