ABA

Defending Liberty
Pursuing Justice

2010 ABA Business Law Section
Annual Meeting – San Francisco, CA

Head in the Clouds, Feet on the Ground:

How In-house Counsel Can Get Ahead of the Clouds!

August 9, 2010, 8:00 a.m. – 10:00 a.m.

Program Chair:

Howie Wong | General Counsel | Toronto Community Housing Corporation

Panelist Biographies

Howie Wong

Howie Wong is General Counsel and Corporate Secretary with Toronto Community Housing where he leads a team that manages legal affairs, corporate governance and compliance & ethics matters. Toronto Community Housing is the largest landlord in Canada with over $6 billion of assets and 165,000 tenants. Prior to joining Toronto Community Housing in 2005, Howie was a M&A/corporate securities lawyer for over 18 years with Gowlings, a national Canadian law firm.

John Moss

Current

- VP, Deputy General Counsel and Head of Commercial Practices at salesforce.com

Past

- Senior Vice President and General Counsel at Intraware, Inc.
- Deputy General Counsel at Barra, Inc.
- Deputy General Counsel at MSCI Barra
- Corporate Counsel at Oracle Corporation
- Associate at Graham & James
- Associate, IP Group at Graham & James LLP (now part of Squire, Sanders & Dempsey L.L.P)

Education

- Stanford University Law School
- The Johns Hopkins University - Paul

Steve Young

Steve Young is a Senior Attorney in the Legal and Corporate Affairs department at Microsoft Corporation, where he provides primary legal support for the Windows Azure cloud computing service. Prior to joining Microsoft, Steve served as corporate counsel at the interactive television company Digeo, Inc., and before that he was an associate at the law firm of Fenwick & West LLP. Jon's practice is global and spans all areas of operations, relationships, transactions and disputes, focusing particularly on Privacy and Information Security, Records and Document Management, E-Discovery and Litigation Readiness, Electronic Transactions and Vendor Management. Jon also leads in community service. He has chaired community nonprofits. he now serves as Vice Chair of the Georgia Free Clinic Network and is helping to develop new educational programs. He regularly assists with strategic planning for new and established public and private ventures.

Jon A. Neiditz

Jon A. Neiditz is a partner in Nelson Mullins Riley & Scarborough's Atlanta office and founder and co-leader of the firm's Information Management Practice. Jon is known nationally for developing and implementing cost-effective information governance and management programs that address the risks, costs and opportunities associated with electronic information – including in communications, collaboration and networking technologies; cloud computing and e-records management. Jon's practice is global and spans all areas of operations, relationships, transactions and disputes, focusing particularly on privacy and Information security, records and document management, e-discovery and litigation readiness, electronic transactions and vendor management. Jon also leads in community service. He now serves as Vice Chair of the Georgia Free Clinic Network and is helping to develop new educational programs. He regularly assists with strategic planning for new and established public and private ventures.

Robin J. Lee

Robin J. Lee is a partner in the Technology Transactions Group of Cooley LLP, resident in the Palo Alto office. His practice focuses on the representation of both emerging growth and established information technology companies, with an emphasis on intellectual property and technology transactions. The scope of his practice includes drafting, negotiating, and providing strategic counsel on a variety of commercial technology agreements, including licensing, distribution, manufacturing and development arrangements for hardware, software, and services, as well as providing legal and strategic counsel regarding the use of free and open-source software. Mr. Lee earned a J.D. from the Yale Law School in 1999, where he was publisher of *The Yale Journal of International Law* and served as an editor and admissions committee member of the *Yale Law Journal*. In 1995, he received a B.A. in Political Science with highest honors from the University of California, Berkeley, where he was elected to Phi Beta Kappa. Mr. Lee currently serves on the board of directors of the San Francisco Bay Area InfraGard, an FBI-sponsored public-private partnership dedicated to promoting critical infrastructure protection and information security.

Cloud Computing Backgrounder

John Moss
SVP and General Counsel, Commercial
August 9, 2010

Disclaimer

My views are my own, and mostly but don’t always reflect those of salesforce.com

NIST’s 5 Essential Characteristics of Cloud Computing

On-demand self-service. Consumer can unilaterally and automatically provision computing capabilities without human interaction.

Broad network access. Available over network through heterogeneous client platforms (e.g., mobile phones, laptops, PDAs).

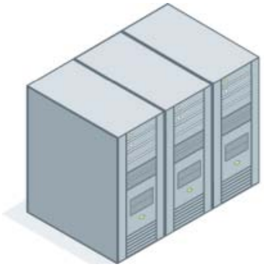
Resource pooling. Provider’s computing resources (e.g., storage, processing, memory, network bandwidth, virtual machine) pooled to serve multiple consumers using a multi-tenant model, with resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity. Capabilities rapidly and elastically scale up and down, and can be purchased in any quantity at any time.

Measured Service. Automatically control and optimize resource use by relevant metering (e.g., storage, processing, bandwidth, user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both provider and consumer.

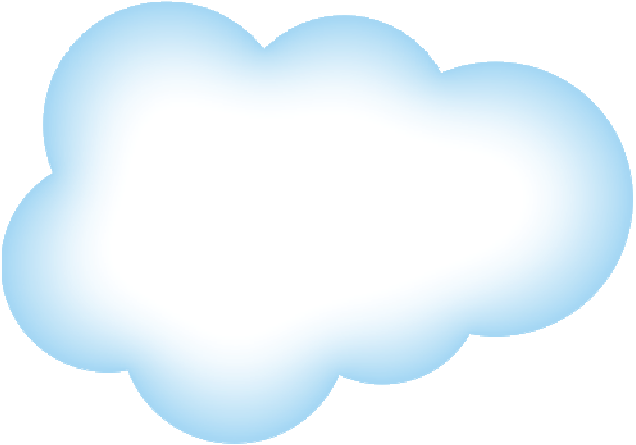
NIST Definition of Cloud Computing v15 http://csrc.nist.gov/groups/SNS/cloud-computing/

Cloud Computing is an Evolution



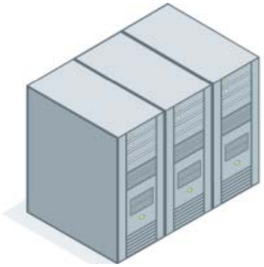
1960's
Mainframe

1980's
Client/server



Today
Enterprise Cloud Computing

Applications Moving to the Cloud



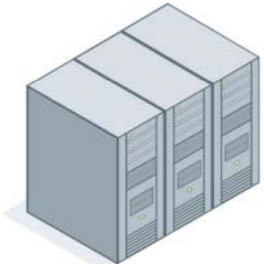
1960's
Mainframe

1980's
Client/server

salesforce apps
Google Apps
cisco
Adobe
OMNITURE
CITRIX
intuit
workday.
Concur click. done.

Today
Cloud Computing Applications

Platforms Moving to the Cloud



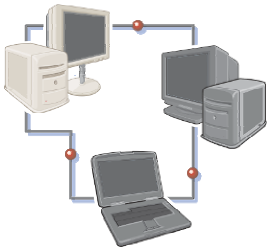
1960's
Mainframe

1980's
Client/server

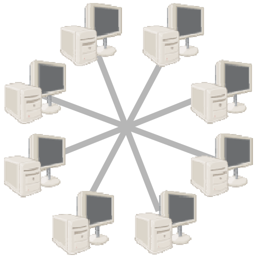
force.com development platform
Google
amazon web services
Windows Azure
IBM
facebook
twitter

Today
Cloud Computing Platforms

Collaboration Moving to the Cloud



1980's
Work Group
Computing



2000s
Intranet
Computing

chatter
Collaboration Cloud
facebook
twitter
Cisco webex
IBM LotusLive™
CITRIX

Today
Collaborative Computing

The Cloud Computing Model – Multi-Tenancy

Shared infrastructure (NIST “resource pooling”)

Rapid innovation

Real-time scalability (NIST “rapid elasticity”)

Automatic upgrades

Pay-as-you-go subscription model (NIST “metering”)

Available through any client platform (NIST “broad network access”)

Apps can be developed 5 times faster at half the cost - IDC

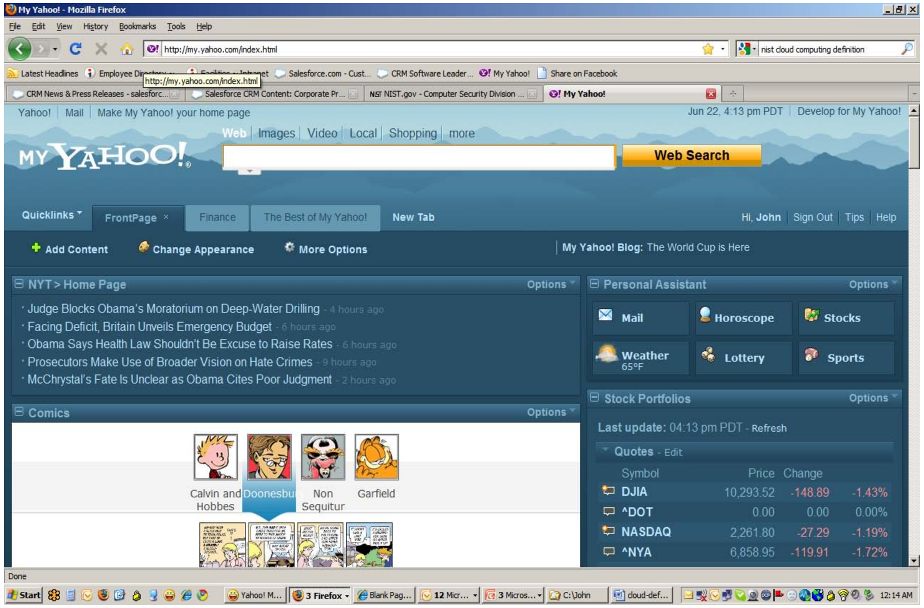
IDC White Paper sponsored by Salesforce.com: “Force.com Cloud Platform Drives Huge Time to Market and Cost Savings”, Doc # 219965, September, 2009

Multi-Tenancy Affects Key Legal Issues

- **Security:** Logical vs physical separation of data, risk of catastrophic breach
- **Reliability:** Multi-tenancy is its own SLA
- **Limitation of liability:** Vendor worst-case-scenario dramatically different than single-tenant or on-premise

Metadata Makes Customization Easy

- Cloud apps tend to be customizable
- Customizations stored at database layer as “metadata”
- Code upgrades don’t break customizations



My Yahoo! Blog: The World Cup is Here

- Judge Blocks Obama’s Moratorium on Deep-Water Drilling - 4 hours ago
- Facing Deficit, Britain Unveils Emergency Budget - 6 hours ago
- Obama Says Health Law Shouldn’t Be Excuse to Raise Rates - 6 hours ago
- Prosecutors Make Use of Broader Vision on Hate Crimes - 9 hours ago
- McChrystal’s Fate Is Unclear as Obama Cites Poor Judgment - 2 hours ago

Last update: 04:13 pm PDT - Refresh

Quotes - Edit

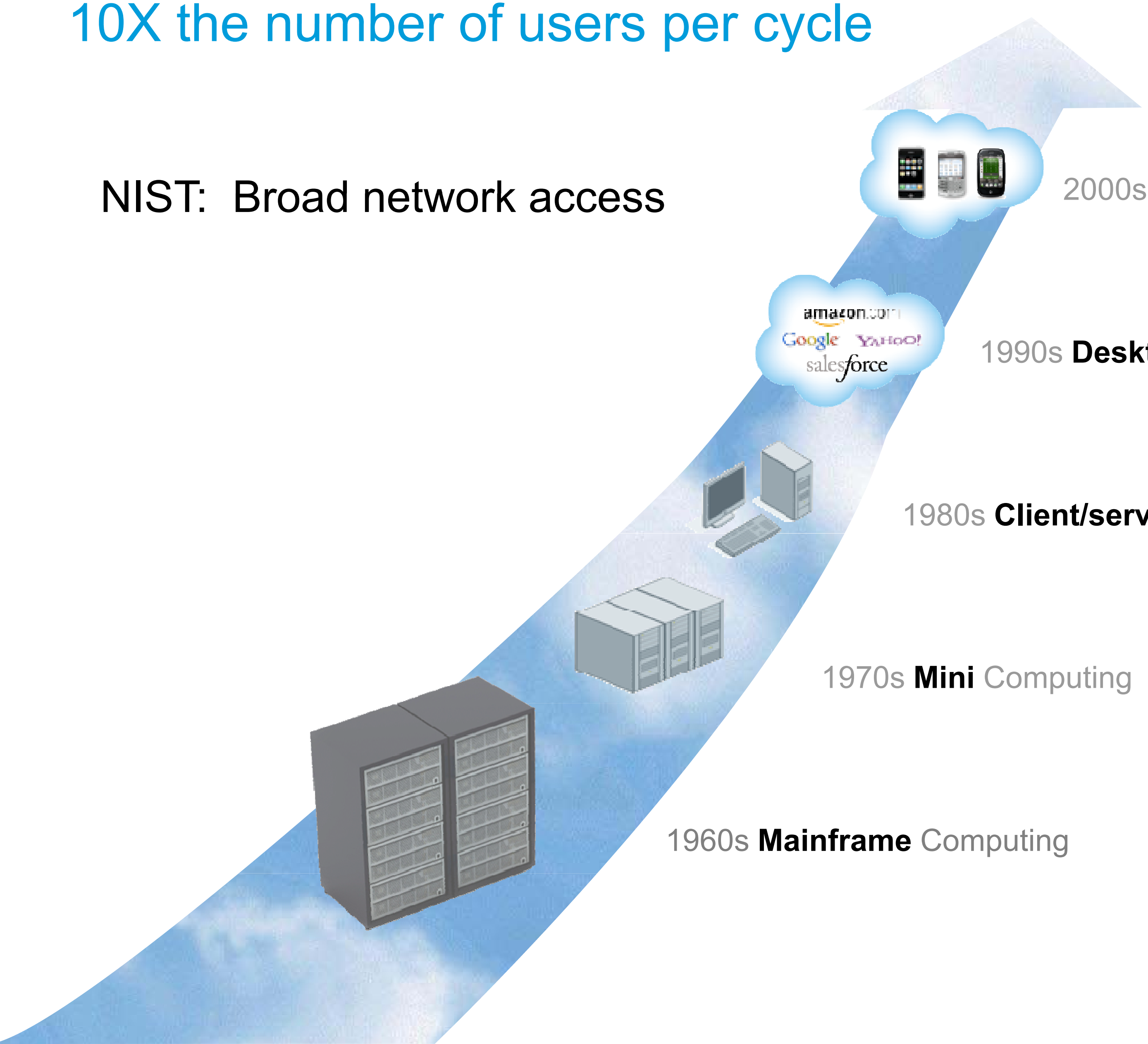
Symbol	Price	Change	
DJIA	10,293.52	-148.89	-1.43%
^DOT	0.00	0.00	0.00%
NASDAQ	2,261.80	-27.29	-1.19%
^NYA	6,858.95	-119.91	-1.72%

- Removing pain from upgrades → more frequent upgrades → faster innovation

Trends: Ten-Year Computing Cycles

10X the number of users per cycle

NIST: Broad network access



2000s **Mobile** Internet Computing

1990s **Desktop** Internet Computing

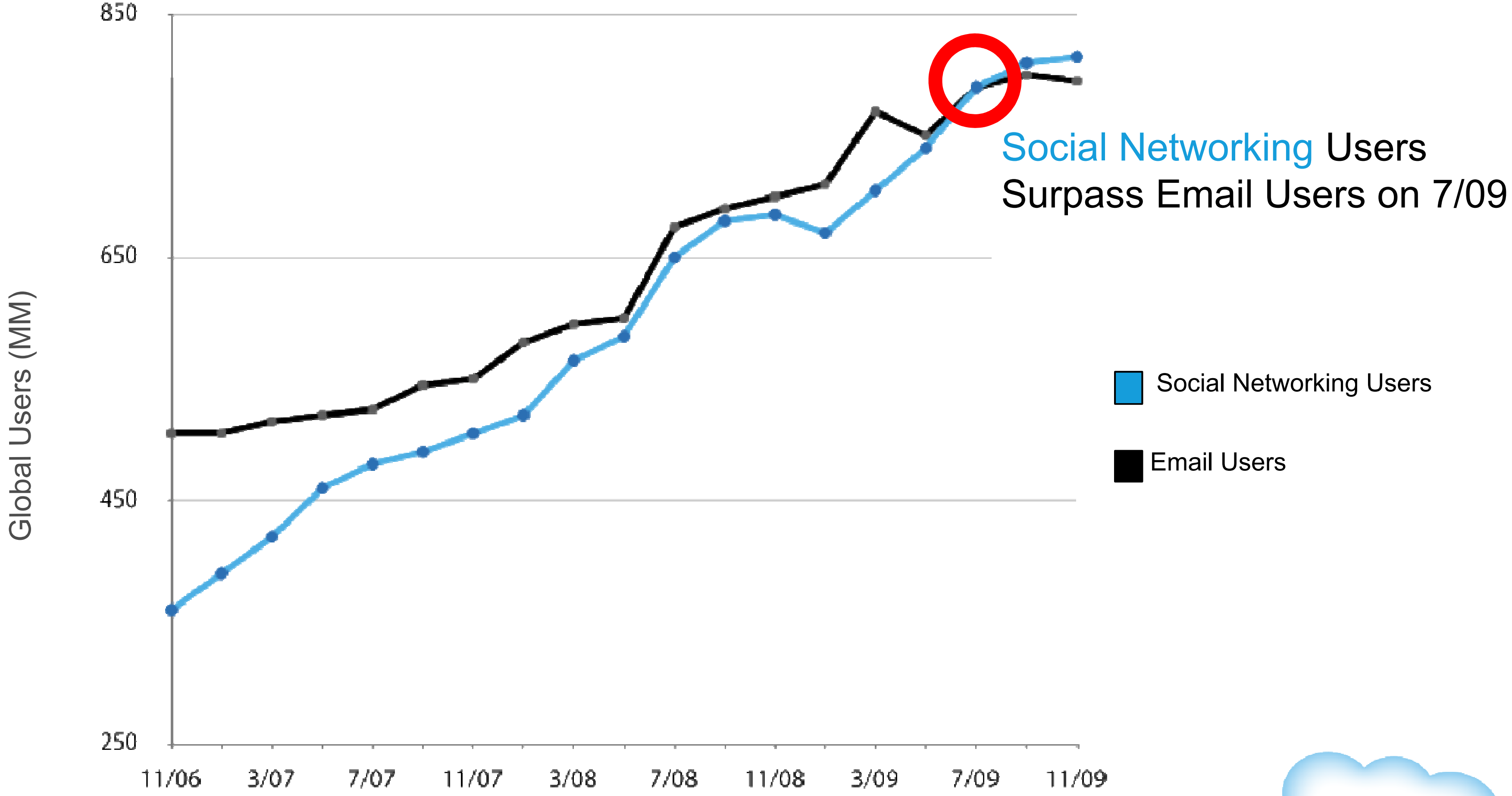
1980s **Client/server** Computing

1970s **Mini** Computing

1960s **Mainframe** Computing

Trends: 2009 - Social Networking Surpasses Email

Communication has moved to the cloud



Social Networking Users Surpass Email Users on 7/09

🟦 Social Networking Users

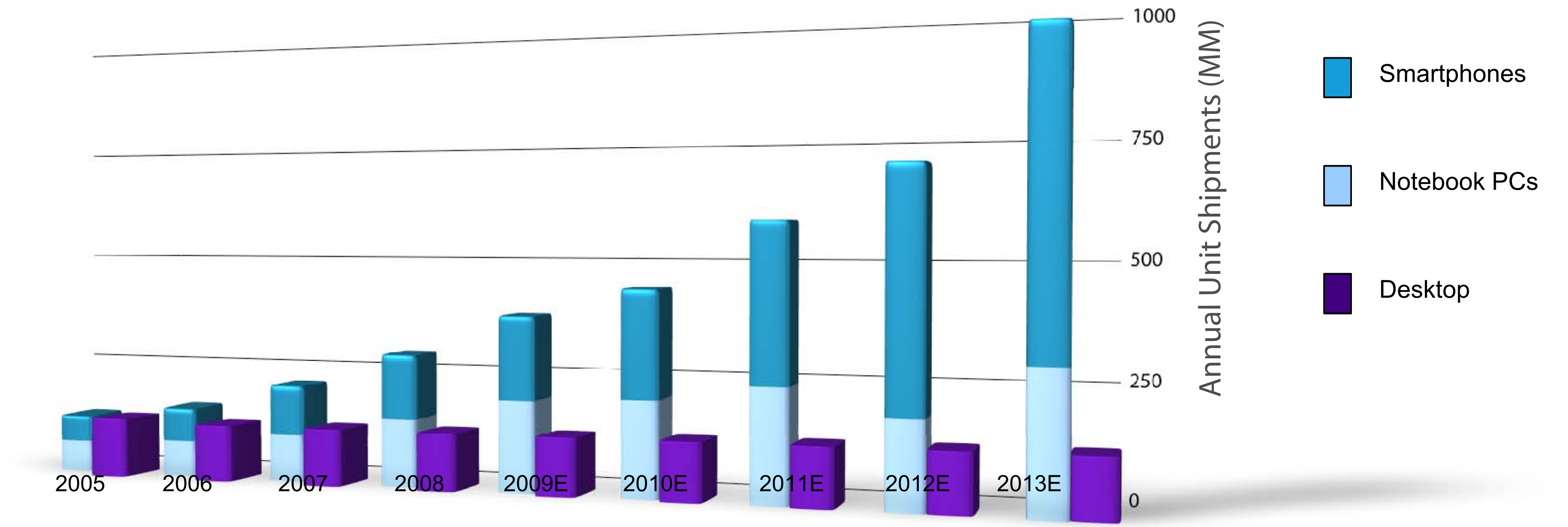
⬛ Email Users

Source: Morgan Stanley Internet Mobile Report, December 2009
Data is for unique, monthly users of social networking and email usage.

Trends: Next Generation Devices Changing How We Access the Internet

Device Shipments

"Broad network access"



Source: Morgan Stanley Internet Mobile Report, December 2009

Head in the Clouds:
Platform and Infrastructure Cloud Services

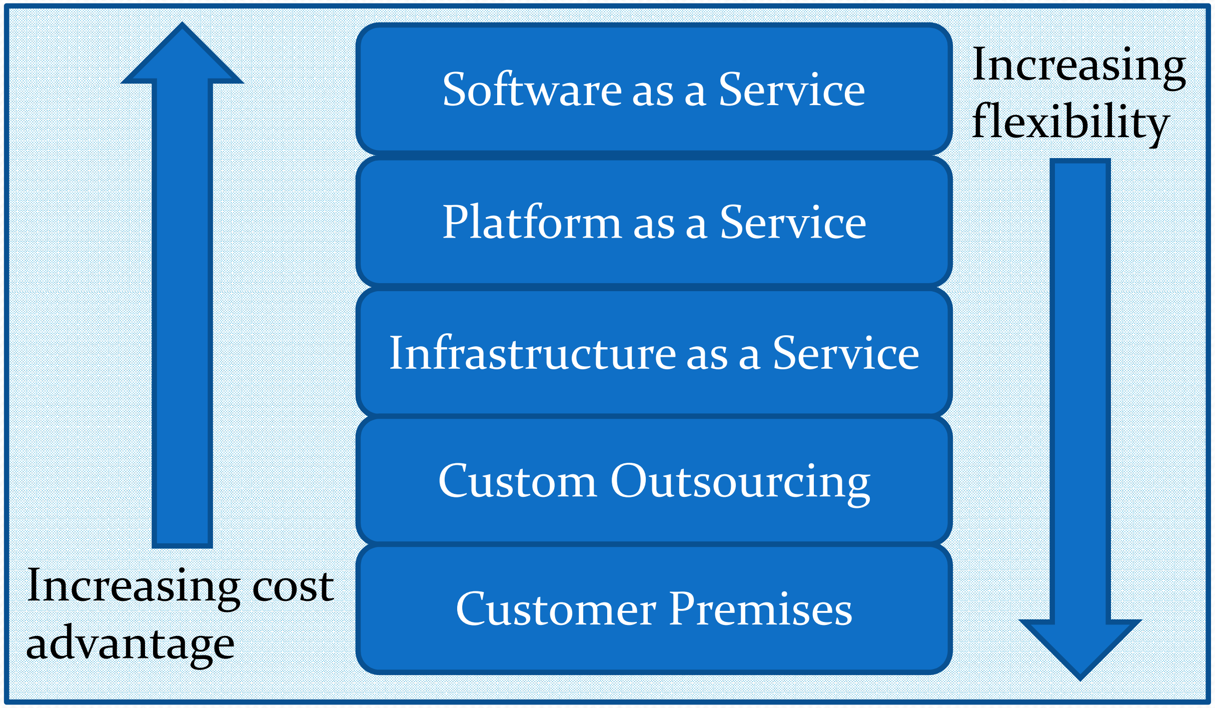
Steve Young, Microsoft Corp.
August 9, 2010

What are Platform and Infrastructure Cloud Services?

- Generally no user interface
- Unfinished services that are not useable by end users until a customer has added something to them
- Platform: operating systems, database systems, other “platform software”
- Infrastructure: data center, power, networking, virtual hardware

Why Do Customers Use Platform and Infrastructure Cloud Services?

- Allows greater level of flexibility compared to “Software as a Service”
- More economical than running dedicated hardware on premise, but generally not as much as “Software as a Service”



Increasing cost advantage

Software as a Service

Platform as a Service

Infrastructure as a Service

Custom Outsourcing

Customer Premises

Increasing flexibility

Conflicting Expectations

- Some customers are familiar with custom outsourcing arrangements, and expect public cloud providers to offer the same degree of flexibility.
- Unlike an outsourcer who builds systems to suit each customer's needs, a typical cloud provider has built a generic shared service in which all customers get the same thing.
- Public cloud providers do not have the flexibility of outsourcers, but custom outsourcing is generally more expensive.
- It helps for all parties to have the same expectations about the service before negotiating.

Privacy and Security Challenges

- Unlike “Software as a Service” offerings, a provider of platform or infrastructure service generally has little or no idea what a customer’s application does or what data is being stored.
- Some regulatory frameworks assume cloud providers will ensure security and privacy are sufficient for the type of data.
- Such a provider may not be able to ensure compliance with every regulation that might apply to any data (e.g. HIPAA, GLB, state security requirements, EU Directive on Data Protection).

Privacy and Security

- Platform and infrastructure providers often look to customers to determine whether their specific needs (including regulatory compliance) are met by the services offered.
  - A provider may say, for example, “this service is not HIPAA compliant, so don’t include patient health records in data stored here.”
- This creates opportunities for cloud providers to offer niche services that meet regulatory compliance requirements in certain industry segments (e.g. HIPAA).

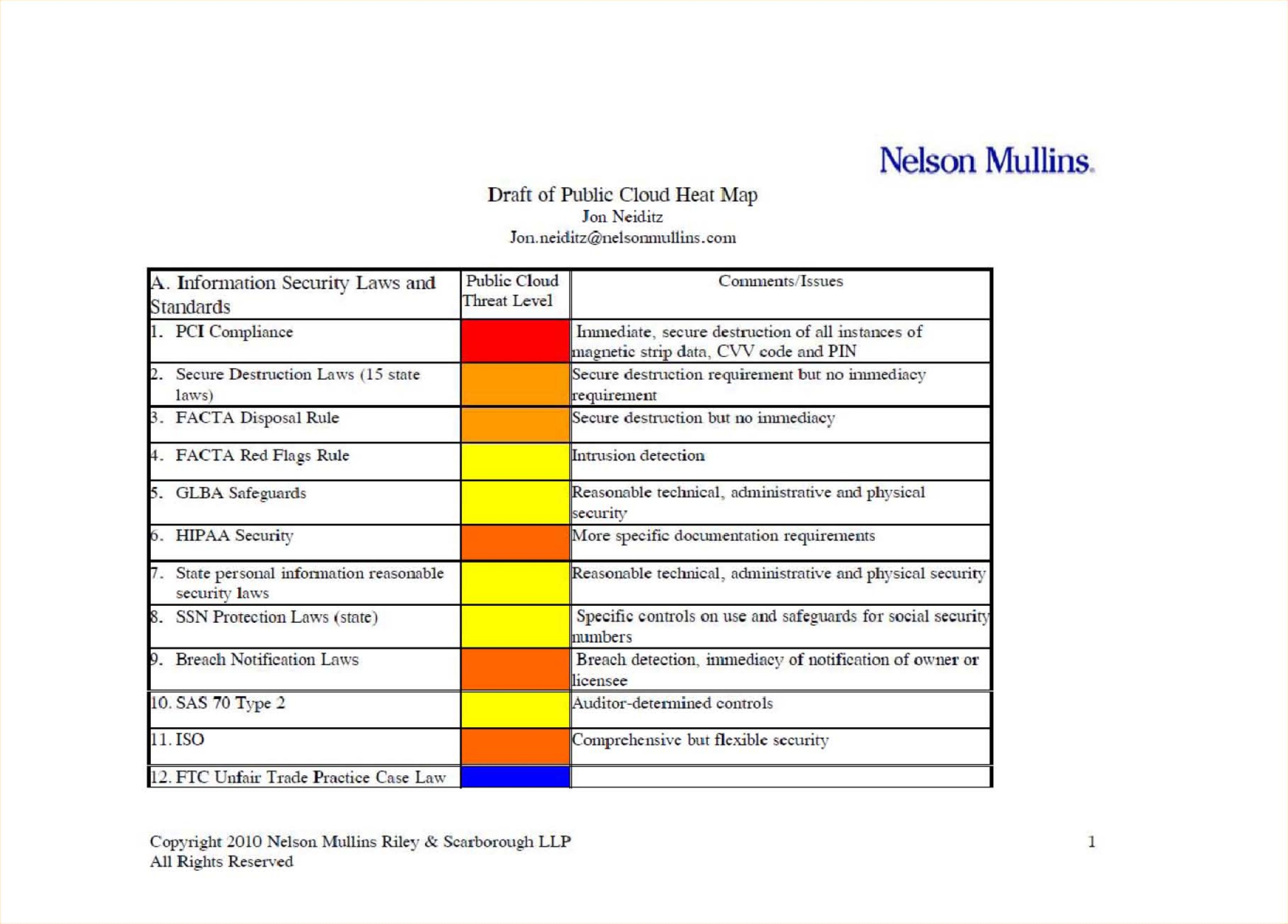
Privacy and Security

What do generic (non-niche) platform or infrastructure cloud service providers do to assure customers about privacy and security?

- ISO 27001 auditing
- SAS 70 auditing
- US Department of Commerce / EU "Safe Harbor" Program
- Transparent sharing of information about security and privacy practices

Public Cloud Heat Map

Jon A. Neiditz
Nelson Mullins Riley
& Scarborough LLP

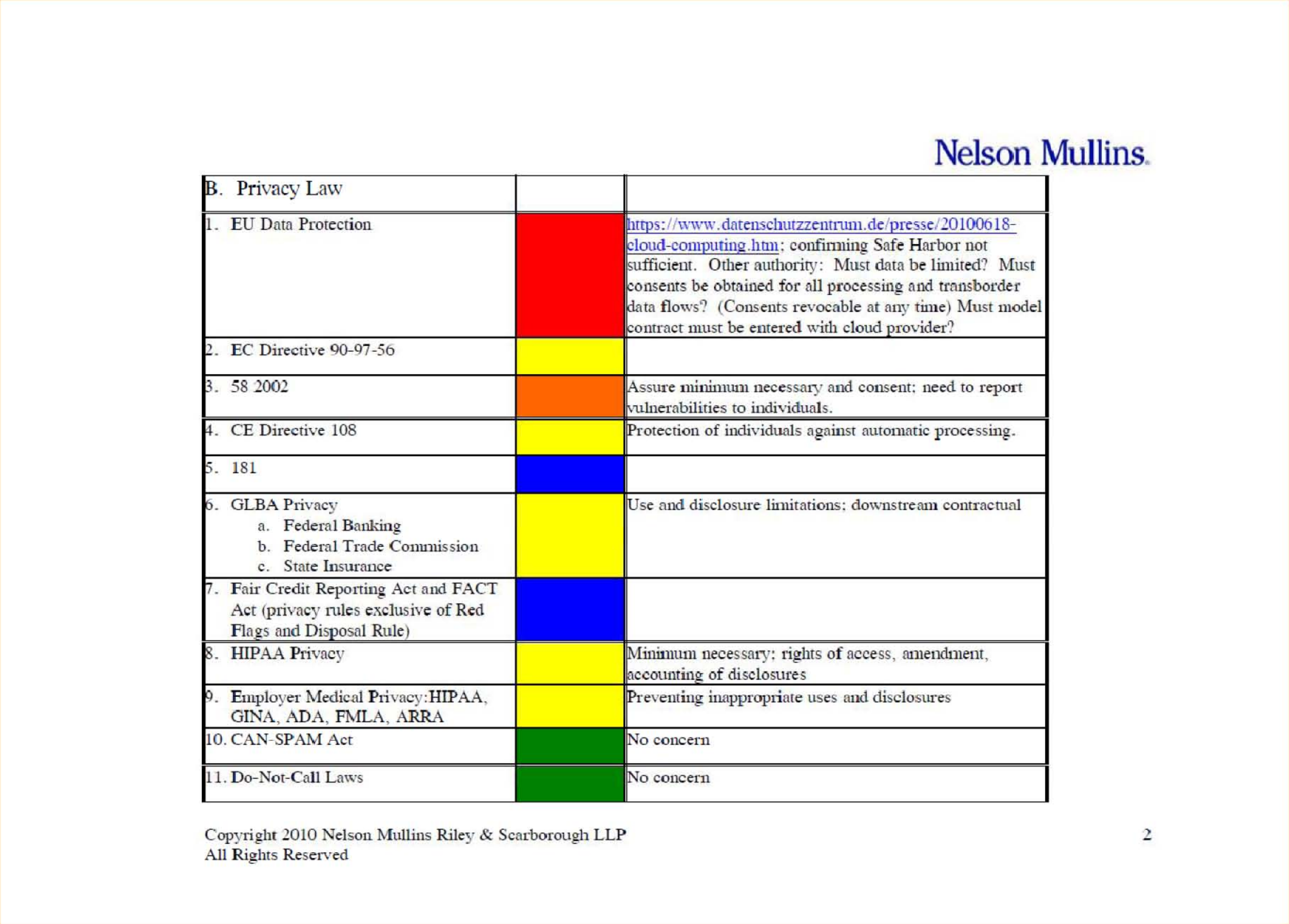


Nelson Mullins.

Draft of Public Cloud Heat Map

Jon Neiditz
Jon.neiditz@nelsonmullins.com

A. Information Security Laws and Standards	Public Cloud Threat Level	Comments/Issues
1. PCI Compliance	🟥	Immediate, secure destruction of all instances of magnetic strip data, CVV code and PIN
2. Secure Destruction Laws (15 state laws)	🟧	Secure destruction requirement but no immediacy requirement
3. FACTA Disposal Rule	🟧	Secure destruction but no immediacy
4. FACTA Red Flags Rule	🟨	Intrusion detection
5. GLBA Safeguards	🟨	Reasonable technical, administrative and physical security
6. HIPAA Security	🟧	More specific documentation requirements
7. State personal information reasonable security laws	🟨	Reasonable technical, administrative and physical security
8. SSN Protection Laws (state)	🟨	Specific controls on use and safeguards for social security numbers
9. Breach Notification Laws	🟧	Breach detection, immediacy of notification of owner or licensee
10. SAS 70 Type 2	🟨	Auditor-determined controls
11. ISO	🟧	Comprehensive but flexible security
12. FTC Unfair Trade Practice Case Law	🟦	



Nelson Mullins.

B. Privacy Law		
1. EU Data Protection	🟥	https://www.datenschutzzentrum.de/presse/20100618-cloud-computing.htm; confirming Safe Harbor not sufficient. Other authority: Must data be limited? Must consents be obtained for all processing and transborder data flows? (Consents revocable at any time) Must model contract must be entered with cloud provider?
2. EC Directive 90-97-56	🟨	
3. 58 2002	🟧	Assure minimum necessary and consent; need to report vulnerabilities to individuals.
4. CE Directive 108	🟨	Protection of individuals against automatic processing.
5. 181	🟦	
6. GLBA Privacy a. Federal Banking b. Federal Trade Commission c. State Insurance	🟨	Use and disclosure limitations; downstream contractual
7. Fair Credit Reporting Act and FACT Act (privacy rules exclusive of Red Flags and Disposal Rule)	🟦	
8. HIPAA Privacy	🟨	Minimum necessary; rights of access, amendment, accounting of disclosures
9. Employer Medical Privacy:HIPAA, GINA, ADA, FMLA, ARRA	🟨	Preventing inappropriate uses and disclosures
10. CAN-SPAM Act	🟩	No concern
11. Do-Not-Call Laws	🟩	No concern

Nelson Mullins.

12. Junk Fax Prevention Act	🟩	No concern
13. Anti-Wiretapping Laws	🟦	
14. Electronic Communications Privacy Act	🟦	
15. Privacy Act of 1974	🟨	Fewer available exceptions than HIPAA and GLBA
16. FTC Cases "Deceptive Trade Practices" Case Law	🟧	Posted privacy policy issues; cloud "back end" may undermine represented practices
17. State and Federal Drivers' Privacy Protection Acts	🟨	Disclosure issues from intrusions
18. COPPA	🟦	Inadvertent or maliciousaccess issues (when the information was obtained from children by a commercial website)
19. FERPA	🟦	Inadvertent or malicious access issues
20. AIDS, Mental Health, Substance Abuse Information (state laws)	🟨	Inadvertent or malicious access issues
21. State Genetic Testing Privacy	🟨	Inadvertent or malicious access issues
C. E-Discovery and Investigations		
1. Willingness and/or obligation of cloud vendor to cooperate with customer in responding to discovery, investigations and preservation obligations	🟧	Willingness and ability and to resist production in accordance with customer wishes; compelled and permitted disclosures under the ECPA
2. Ability of vendor to comply with preservation (hold) and production requirements imposed on it	🟧	Willingness and ability to preserve and/or produce all instances of Electronically Stored Information (ESI); ; mitigation of production but not preservation duties under Rule 26(b)(2)(B) of FRCP

3. E-record and e-document retention/destruction programs supported?	🟨	Need to assure secure destruction rather than deactivation?
4. Preservation of replications and other redundancy	🟧	Potential major search cost issue, as well as spoliation issue
5. Data integrity and metadata	🟨	As the law of e-evidence develops, will reliance be placed on encryption, audit trails or hash algorithms?
6. Legal privileges	🟨	Issue now being addressed by NC Bar
D. E-Commerce		
7. Enforceability of electronic signatures and contracts	🟨	Adequate process controls to satisfy UETA, ESIGN and international laws?
E. Intellectual Property		
Risk of Loss/Theft	🟧	Large target for theft
Legal Risk of Inadequate Control	🟨	Potentially undermining IP rights

Cloud Contracts:

A customer-side view of cloud-computing agreements

Cooley LLP

Robin J. Lee

ABA Annual Meeting

Aug. 9, 2010

What we’ll cover…

- The business case
  - Pros: What’s attractive to a customer about a cloud computing solution?
  - Cons: What’s the customer downside
- Selected customer issues
- Ways to address these issues in the customer agreement

Customer Benefits

- Reduced up-front investment cost
- Increased flexibility – provision-to-fit
- Service-oriented offering = more Customer-oriented focus by provider
- Freedom to walk away (well, maybe)

Customer Disadvantages

- Loss of control
- Data security and privacy
- Compliance issues
- E-discovery issues
- Risks associated with Service Provider
- Hidden costs

The Contract: Selected Issues

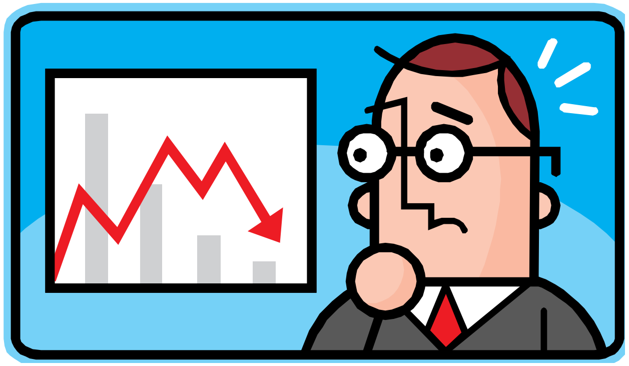
1. Data security and privacy
2. Service levels
3. Indemnification
4. Warranty/liability issues
5. Termination issues
6. Worst-case scenario: what if the service provider disappears?

Data Security and Privacy

- Customer owns its data.
- Provider will implement "appropriate" measures to ensure security of Customer data – exactly what does this mean?
- How do we deal with data-related compliance issues – data privacy, responding to security breaches, e-discovery and document preservation, etc.?
- To what extent will Provider accept responsibility for loss of Customer data?
- To what extent should Customer be responsible for "client-side" confidentiality, use of user passwords, etc.
- Who bears the risk of a "no-fault" breach?

Service Levels

- Appropriate performance measurements (uptime guarantees, throughput, mean-time-to-restore), and exclusions
- Remedies (are service credits enough?)
- Customer duties and responsibilities
- Disaster recovery provisions



Indemnification

- Quick review: what does an indemnity do?
- What should a provider indemnify the customer for?
  - Third-party intellectual property infringement?
  - Breach of privacy or security?
  - Third-party customer issues (i.e., the Customer’s customers)?
- Are there ever circumstances where it’s reasonable for the Customer to indemnify the service provider?

Warranties and Limitations of Liability

- Performance Warranty
  - Do you get one at all?
  - Duration?
- Caps on liability
- Exclusions from liability limitations

Termination Issues

- Customer can just walk away, right?
- If no termination for convenience, what constitutes “cause” for termination purposes?
- Transition, migration, and other assorted ugliness
  - Wind-down periods
  - Return of Customer data
  - Post-termination services/migration assistance

What about the worst-case scenario?

- What happens if Provider disappears?
- Early warning
- Source code/technology escrow
- Business continuity/exit plans

Final thoughts

- Understand what the Customer wants out of the cloud offering
- Understand the practical allocation of responsibility among the Service Provider and Customer—this is not always simple
- Pay attention to the ugly little details

Questions?