

A decorative graphic consisting of a light olive-green square on the left and a dark maroon rounded rectangle on the right. The text "Cloud Computing" is centered in white within the maroon rectangle.

Cloud Computing

A Look at Clouds from Both Sides

September 16, 2010

This presentation was created sent by Dorsey & Whitney LLP, 50 South Sixth Street, Suite 1500, Minneapolis, MN 55402. This presentation is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created or continued by sending and/or receiving this presentation. Members of Dorsey & Whitney will be pleased to provide further information regarding the matters discussed in this presentation.

A decorative header element consisting of a light brown square on the left and a dark red rounded rectangle on the right containing the word "Panel" in white text.

Panel

- **Scott Read**, Principal, Deloitte Financial Advisory Services
- **Shari Aberle**, Partner, Dorsey & Whitney LLP
- **Melissa Krasnow**, Partner, Dorsey & Whitney LLP, and Certified Information Privacy Professional
- **Caroline Sweeney**, Director, Practice Group Technology Services, Dorsey & Whitney LLP

What is “Cloud Computing”?

- Data and software platforms and services are stored off-site “in the cloud”
- No need to install software on each employee’s desktop computer
- Services are provided over the Internet

But...it’s more than just an opportunity to outsource server and storage needs...



What is “Cloud Computing”?

Cloud computing allows a company to essentially reach into a “cloud” for resources in order to boost capacity or add capabilities on the fly, in realtime, without having to invest in:

- New infrastructure
- Training new personnel
- Purchasing more software licenses

And:

- It is a “pay-per-use” service
- Highlights Web 2.0 technologies
- It’s not new!

Five Characteristics of Cloud Computing

- On-demand self-service
- Ubiquitous network access
- Location independent
- Rapid elasticity
- Pay per use



– *source: NIST (National Institute of Standards and Technology)*

Cloud Computing: Delivery Models

- IaaS: Infrastructure as a Service
 - Company out-sources the equipment used to support operations: storage, hardware, servers, networking components
 - The provider owns the equipment and is responsible for housing, running and maintaining it
- SaaS: Software as a Service
 - Software applications are hosted by a service provider
 - Applications are available to customers over a network, typically the Internet
 - Vendor provides daily technical operation, maintenance, and support: Gmail, virtual data rooms
 - Per 2010 McKinsey Quarterly, SaaS is growing at a 17% annual rate
- PaaS: Platform as a Service
 - Offers operating systems and associated services, e.g. Salesforce.com

The Different Kinds of Clouds

- Private
 - Operated within a single organization
 - On demand, pay by the hour computing services
 - Can be known as “internal clouds”
- Public
 - Available to the general public
 - Examples include Amazon, Google, Facebook, Twitter
- Managed
- Hybrid
 - Combination of private and public clouds



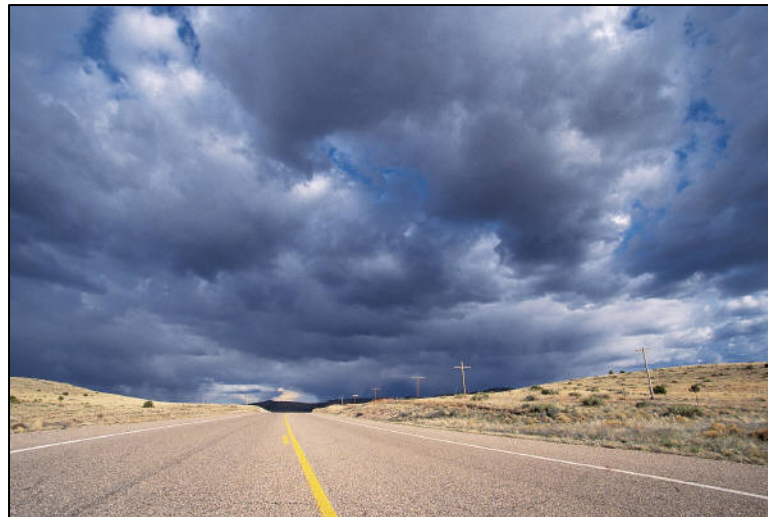
Public Cloud Candidates

- Applications used by mobile workers to manage their time and activity, e.g. sales support, email
- Software development environments
- Applications requiring hardware or software not normally used by a company's IT operations
- Distributed server and data center implementations
- Test and pre-production systems
- Marketing and any data that is already on the Internet for public consumption as the data is not sensitive and no security breach will compromise the company
- Many companies are simply too small to affordably build out their own business network. They can achieve better computing value and higher levels of security on a well-provisioned public cloud



Not so good for the Public Cloud

- Applications that involve extremely sensitive data
- Applications that contain data where there is a regulatory or legal risk involved in any disclosure
- Applications that may require intensive workloads and where performance over the Internet might be a problem.



What are the Business Benefits?

- Delivery of services
 - Faster time to value and time to market
- Reduction of costs
 - Running application services on a cloud platform moves capital expenses to operational expenses
 - The business can develop, deploy and use more application services as it requires them, without needing huge initial capital investments (and ensuing operational costs) for dedicated infrastructure that may never be needed
- IT department transformation
 - Focus on innovation vs. maintenance and implementation
 - “Cloud computing can save customers 20 to 30 percent of their IT costs. Changes can be made quickly.”

-source *Donald Leeke, Microsoft*

And...(Business Benefits, continued)...

- Access to data from any location with an internet connection
- No need for maintaining a physical storage device
- No ongoing costs of maintaining and upgrading an on-site storage system's hardware and software
- Pay as you go model allows for reduced operating expenses
- Can add and remove capacity based on real - rather than projected - storage needs
- Dedicated security team, security auditing/testing is easier, real-time detection of system tampering

Flying to the Clouds

- Expect companies to carefully select projects that benefit from the cloud's features and cost benefits
- Expect further development of formal cloud computing strategies
- The cloud has mainly attracted smaller and medium-sized businesses seeking to lower costs
- Bigger companies, which have voiced more concerns about privacy and security, haven't embraced it
- Retailers and manufacturers are most amenable because the flexibility accommodates annual variations in their employment rolls
- Financial services and health care are slower to adopt because of privacy concerns
- Cloud computing is not regulated...yet



Who Offers Cloud Computing Services?

- There are well over 100 cloud data backup providers of one type or another. Easy to try out because of the nature of storage as a service and the lack of capital investment
- IBM - currently collaborating with corporations, universities, Internet-based enterprises and government agencies
- Yahoo - works with Carnegie Mellon University researchers to modify and evaluate software
- Google - makes processors in data center available to University of Washington, Stanford, and MIT to help students understand cloud computing technology.
- Amazon S3 - aimed at small to medium businesses, from consumers saving personal data to Web startups offering online services and larger companies wanting to back up databases or store archival data
- Nirvanix - geared toward medium and large users.

Who is in the Clouds?

- 3M
 - Launched new business - Visual Attention Services
 - Unable to predict the demand for the services
 - Did not want to commit to long-term data center use
 - Cloud computing became the inexpensive way to launch a new business for which demand is unknown

– *Source: Star Tribune: Clearer on Cloud Computing (May 11, 2010)*

Who is in the Clouds?

- The New York Times
 - Uses Amazon S3 to store and deliver articles from its historical archives.
- NASDAQ
 - Uses Amazon to store historical market data, making it available to traders through its Market Replay tool
- Genentech (bio technology company)
 - Uses Google for e-mail and document creation
- Law firms
 - Examples include law practice management systems, document management systems, secure email networks, digital dictation services, billing and timekeeping services...virtual data rooms
- Schools & Universities
 - “Cloud computing and collaboration technologies can improve educational services, giving young and adult students alike access to low-cost content, online instructors, and communities of fellow learners.” - *source: McKinsey Quarterly report, 2010*
- Automotive industry
 - Design teams spread throughout the US or internationally can log on and collaborate on engine, body, interior and other product components with little or no outside exposure, securing all aspects of the new design.

Who Offers Cloud Computing Services?

- Microsoft - in the cloud computing space for 15 years.



Hotmail®

- Hotmail (350 million users)
- Xbox live (6 million active accounts)
- Windows Update services



- 70% of MS employees who are involved in building software are working on entirely cloud-based or cloud-inspired projects

- Office 2010 and SharePoint 2010 –

- Include MS Office web applications – the cloud companion to Word, PowerPoint, and Excel
- Allows users to work from virtually anywhere
- Companies can acquire licenses based on the number of months they need applications

– *Source: In Their Own Words: Microsoft's Legal Cloud Computing Strategy: Not 'All or Nothing'*



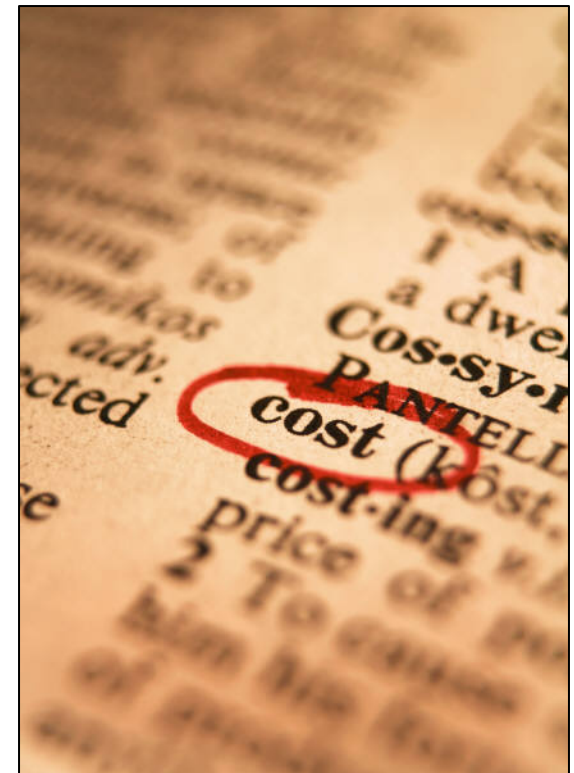
The Cloud: Sunshine or Rain? ...Challenges and Risks

- Where is my data?
- How does my data securely enter and exit the cloud?
- How is my data protected?
- Who has access to my data?
- Who is accountable if something goes wrong?
- What's the disaster recovery plan, including response to pandemic?
- How do we comply with export and privacy laws?
- What is the viability of my cloud vendor? What happens if my cloud provider disappears?
- How is the environment monitored?
- How is the data protected and secured from theft and damage?
- How is encryption managed?
- How easy to integrate with existing IT solutions?
- Customization capabilities to suit my needs?
- Will on-demand cost more?
- Are there any regulatory requirements on my business that can prevent me from using the cloud?

– Source: *An Essential Guide to Possibilities and Risks of Cloud Computing*, Maria Spinola

The Cloud: Sunshine or Rain? ...Challenges and Risks

- Be aware of hidden costs
 - cost per gigabyte of cloud storage may only be part of the picture
 - Potential fees for data transfers, metadata functions, or copying and deleting files
 - Internal costs for connecting to the cloud (T1 line, for example)



Considerations: Data Security & Data Privacy

- Fall 2009 survey by Mimecast:
 - 46% of all business respondents cited security as a concern in adopting cloud computing as an IT strategy
 - The most reluctant sectors included financial services (76%), energy (75%), and government (67%)
 - 70% of companies that have launched cloud computing initiatives plan to move additional applications and data to the cloud
- Cloud security threats from three fronts:
 - from outside, over the internet
 - from other cloud applications on the network
 - from personnel
 - threats are no different than security fault potentials on any in-house corporate network
- Data access governance concerns
 - danger of data falling into the wrong hands – either as a result of people having more privileges than required or by accidental or intentional misuse of the privileges assigned to their job
- Data segregation
 - data is typically in a shared environment alongside data from other customers

Considerations: Data Security & Data Privacy

- Control over and knowledge/information about data
- Data
 - What kind?
 - What will be done with data?
 - Where?
- Data subjects
 - Where?



Considerations: Records Retention

Records retention refers to the length of time a record must be retained to satisfy the purpose for which it was created and to fulfill applicable legal requirements. While there is no general law governing document retention, there are statutory and regulatory requirements that govern the retention of certain documents in certain industries. There is also a common law duty to preserve records that arises with respect to litigation.



Considerations: Records Management

- A records retention policy is typically comprised of a schedule setting forth the length of time documents must be retained, a framework for implementing that schedule, and a statement of the company's policy on retention.
- To begin developing a document retention policy it is necessary to understand:
 - what types of records the corporation has;
 - who controls those records;
 - where the records are located;
 - the types of litigation or enforcement action the company can expect; and
 - when the records become obsolete so they can be destroyed.

Considerations: Records Retention

While it may seem obvious, the first thing that must be done to develop a sound policy is identify the records that are regularly created and/or received by the company. A complete records inventory – which identifies the records, their location, and the format in which they are maintained – is the basis from which the records retention schedule is created.

The failure to account for changing technology in records retention policies represents a significant risk.



Considerations: Records Management

- 2009 Electronic Records Management Survey, Cohasset Associates & ARMA
 - 78% of respondents reported they do not have retention practices in place for emerging sources of records (voice mail, IM, blogs, Web pages)
- Cloud solutions must consider records management requirements, for example:
 - Can the solution implement records disposition schedules, including the ability to transfer and permanently delete records?
 - Cloud providers or managers may not be able to ensure complete deletion of records
- If particular cloud deployments present insurmountable obstacles to records management, there will be a negative impact on the company's records program.

Considerations: E-Discovery

- Gartner study: Data increasingly lives in the cloud.
 - Companies are increasingly using cloud-based services for e-mail, word processing, and spreadsheets.
 - These are the three most important targets of discovery and regulatory investigations
- Spoliation occurs where evidence is destroyed or significantly altered when litigation or investigation is pending or reasonably foreseeable.
 - consequences of spoliation can be severe and may include criminal charges, monetary sanctions, dismissal, suppression or exclusion of evidence, or an adverse inference jury instruction.
- Consider:
 - How are document holds enforced and how is data preserved?
 - How is metadata protected?
 - How is Information searched for and retrieved pursuant to e-discovery requirements?
 - How is attorney/client privilege maintained?
- Subpoenas:
 - You may not even know about them if the cloud vendor gets the subpoena
- Cooperation:
 - With the other party...and with your cloud provider

Considerations: E-Discovery

- F.R.C.P. 34(a)(1):
 - “...produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control.”
 - Typically, cloud customer is the party in control and cloud service is the party in possession
 - Requesting cloud provider to perform discovery on behalf of customer could present issues regarding attorney/client privilege
 - Without customer consent, potential to impinge upon Stored Communications Act (18 U.S.C. §§ 2701 to 2712)

The Cloud & The Law

- The Stored Communications Act (SCA)
 - Law that was enacted by the [United States Congress](#) in 1986.
 - It is not a stand-alone law but forms part of the [Electronic Communications Privacy Act](#);
 - It is codified as 18 U.S.C. §§ 2701 to 2712.
 - The SCA addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party [internet service providers](#) (ISPs).
- The [Fourth Amendment to the U.S. Constitution](#) protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures...."However, when applied to information stored online, the Fourth Amendment's protections are potentially far weaker. In part, this is because the Fourth Amendment defines the "right to be secure" in spatial terms that do not directly apply to the "reasonable expectation of privacy" in an online context. In addition, society has not reached clear consensus over expectations of privacy in terms of more modern (and developing, future) forms of recorded and/or transmitted information.
- Furthermore, users generally entrust the security of online information to a third party - an ISP. In many cases, Fourth Amendment doctrine has held that, in so doing, users relinquish any expectation of privacy. The "third party doctrine" holds"...that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information. "While a [search warrant](#) and [probable cause](#) are required to search one's home, under the third party doctrine only a subpoena and prior notice (a much lower hurdle than probable cause) are needed to compel an ISP to disclose the contents of an email or of files stored on a server. The SCA creates Fourth Amendment-like privacy protection for email and other digital communications stored on the internet. It limits the ability of the government to compel an ISP to turn over content information and non-content information (such as logs and "envelope" information from email). In addition, it limits the ability of commercial ISPs to reveal content information to non-government entities.

Source: Wikipedia

The Cloud and the Law

- Application of domestic and international laws
 - Cross-border data transfer compliance (e.g., EU Data Protection Directive)
 - Geography / jurisdictions / export law compliance
 - Regulated industries (e.g., financial, health, etc.)
 - Regulatory / legal compliance by provider



The Cloud & The Law

Flagg v. City of Detroit 2008 WL 787061 (E.D. Mich. 2008)

- Most significant test for cloud-based deployments is control
- Party in control over the data is the one that determines discoverability of data in the cloud
- The third party in possession of data is not required to produce responsive electronically stored information (ESI), given the provisions of the SCA
- No need to subpoena cloud provider, as required evidence was more easily acquired by an e-discovery request to the cloud customer

The Cloud & The Law

Crispin v. Audigier (C.D. Cal.) (May 26, 2010)

- Involved postings on Facebook and MySpace
- Judge went to great lengths to explain why the provider is NOT required to produce documents based on the protections offered by the SCA



The Cloud & The Law

- Whether an employee has a reasonable expectation of privacy in electronic communications is fact-based and will likely depend on the employer's policy.
- On June 17, 2010, the United States Supreme Court decided *City of Ontario v. Quon*, a case involving a SWAT-team member who had used his city-issued, text-messaging pager for personal communications. The City's general technology usage policy stated that e-mail and Internet usage would be monitored; however, there was an informal policy that supervisors would not audit employees' text messages as long as the employees paid any overage fees. Quon brought suit after a supervisor requested transcripts of his messages after noting Quon regularly had overages, even though Quon paid the overage fees. Quon claimed the City violated the Stored Communications Act and Fourth Amendment, among other claims, and the district court agreed.
- The Ninth Circuit, however, reversed and held that users of text messages have a reasonable expectation of privacy in the content of their text messages and that the "operational realities" of the employer created a reasonable expectation of privacy for the employee. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 907 (9th Cir. 2008).

The Cloud & The Law

- The Supreme Court reversed on narrow grounds, holding that the City's search of the text messages on the facts of this case was reasonable.
- The Court, however, declined to address employee privacy expectations with respect to employer-provided communications devices, cautioning the judiciary against "elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." As the Court explained, "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve."
- While *Quon* does not offer guidance on best practices for technology use and related records management, it does highlight the importance of the employer's policies around technology use.

The Cloud & The Law

- *EEOC v. Simply Storage Mgmt, LLC*, (S.D. Ind. May 11, 2010) (observing that “[i]t is reasonable to expect severe emotional or mental injury to manifest itself in some [social networking] content,” and therefore allowing discovery of the plaintiffs’ Facebook and MySpace accounts where “emotional health” was at issue. The parties disagreed on the scope of discovery, with plaintiffs fearing that the information discovered could embarrass them; however, the Court discounted this concern because the information had already been shared “with at least one other person through private messages or a larger number of people through postings.”).
- *Barnes v. CUS Nashville, LLC*, 2010 WL 2265668 (M.D. Tenn. June 3, 2010) (magistrate judge offered to create a Facebook account for himself “[i]f [the parties] will accept the Magistrate Judge as a ‘friend’ on Facebook for the sole purpose of reviewing photographs and related comments *in camera*” in a case where plaintiff raised privacy concerns about the public dissemination of photographs posted to her Facebook account).

Cloud Contracts: Due Diligence

- Consider more than one provider
 - Financial strength of provider
 - Insurance coverage of provider
 - What happens if merger or acquisition or bankruptcy involving provider?
 - Has provider had a security breach?
 - Who is data processor? subcontractor?
 - Provider's privacy and related policies, procedures and requirements
 - Customer's privacy and related policies, procedures and requirements



Cloud Contracts: Approach

- IT, legal/compliance, privacy and business / management and other functional areas should work together
- Determine position on issues and develop contract language for this



Cloud Contracts: Provisions

- Protection of data
- Control by customer over data
- Provider control over data
- Responsibilities of provider and customer
- Indemnification, limitation of liability/exceptions and consequential damage disclaimers
- Pricing, business continuity, termination, service level, compliance, litigation/e-discovery, and auditing/security
- Relationships
 - Incident response/contingency plans
 - Data breach
 - Controls to prevent data breach, security and controls
- Data preservation and electronic discovery
 - Service level agreements
 - Handling of failures

Best Practices: Records Management

- Define a Cloud Governance Program and train your staff regarding its contents
- Have Records Management staff review the cloud provider contract around a security model for preservation of data that includes communication, collaboration, infrastructure, and the application platform
 - Ensure your cloud provider agreement guarantees data recovery and assured destruction of data
 - State explicitly in the contract information ownership and control amongst parties
- Solid records management policies and data governance practices set instructions to capture, manage, and retain records; address how data will migrate to new formats and operating systems; address how to transfer permanent records in the cloud to the records authority; and create a framework for portability and accessibility issues.
- Determine which copies of records will be declared as the record copy and manage these in accordance with judicial records management content. Remember, the value of records in the cloud may be greater than the value of the other set because of indexing or other reasons.

Best Practices & E-Discovery

- Data can be stored in any country
 - know where the data center is located, as the physical question raises the question of legal governance over the data.
 - Address which country's court system will settle a dispute in event of a conflict between the cloud vendor and customer
 - Be aware of the prevailing law in that particular nation.
 - For example, German law will not allow documents to leave Germany if your client is the government. How would you adhere to these requirements in a cloud scenario?
 - The European Network and Information Security Agency - November 2009 report on cloud computing - warns companies remain responsible under UK law for safeguarding their customers' information even if that data is stored by a service provider in the cloud.
 - Intellectual property protection



Best Practices & E-Discovery

- Ensure process regarding third-party access to stored data
- The agreement with the provider must contemplate everything involved with e-discovery: notices upon service of process, procedures for receiving discovery requests, protocols for communication and data transfer between litigating attorneys and service provider personnel, pricing, etc.





Questions

