IP and Business Issues in Cloud Computing

IP and Business Issues in Cloud Computing

1. Cloud Computing Defined

1.1. What is cloud computing?

- Numerous definitions of "cloud computing" abound, but the generally accepted key aspects of cloud computing include providing massively scalable and elastic IT-related capabilities "as a service" to external customers using Internet technologies, where the service consumers need only care about what the service does for them, not how it is implemented.
- From a practical perspective, cloud computing can be understood as an IT solution that increases existing capacity or addsfunctionalityto current IT capabilities "on the fly" and without the customer investing in new infrastructure or training new personnel. This is typically accomplished by providing those IT services across the Internet via a subscription-based or pay-per-use plan. The various types of services provided through cloud computing can generally be categorized at (a) Software-as-a Service (SaaS), (b) Application Platform-as-a-Service (APaaS), and (c) Infrastructure-as-a-Service (IaaS).
- Software-as-a Service (SaaS): Also known as "hosted applications," SaaS is a method of remotely delivering access to software and its functions to end users, usually as a Web-based service. SaaS allows organizations to access the software typically at a cost less than paying for licensed applications because SaaS pricing is subscription-based or pay-per-use. A particular feature of SaaS is that it hosts software remotely, thereby eliminating the need for end users to invest in additional hardware. Additionally, because the service is remotely maintained and delivered, SaaS also removes the need for organizations to handle the installation, set-up and routine upkeep and maintenance.
- Application Platform-as-a-Service (APaaS): Application Platform-as-a-Service (APaaS) is essentially an extended application server "in the cloud"; APaaS is an IT service that provides a development and deployment environment for cloud-based business applications. The business applications that are developed or deployed using APaaS are typically SaaS applications. For example, SaaS applications can be developed or deployed to end-users on an APaaS platform.Under this configuration, APaaSmanages multi-tenancy and scalability issues that would otherwise be left for the customer's IT department to address.In this framework, APaaS is the middle layer in the overall cloud computing structure, situated between the IaaS and the SaaS:

IaaS ↔ APaaS ↔ SaaS ↔ End Users

- Infrastructure-as-a-Service (IaaS): IaaS is typically an offering of on-demand computing capacity. This type of service replaces the need for customers to buy and maintain servers and other hardware and equipment within its own data center. By accessing the requisite servers from a service provider through the Internet or a private network as IaaS, the customer benefits from a scalable and elastic infrastructure, accessed through the cloud.

1.2. What Companies are Doing in the Cloud

- Companies are using cloud computing in a variety of ways, which can typically be categorized as described above (SaaS, APaaS, or IaaS), and there are numerous reasons for this shift towards the cloud. Although cloud computing is not the best option in all situations for all IT services, there are a number of common reasons that companies are deciding to move certain services to the cloud. One of the most pervasive reasons is cost: cloud computing can reduce IT expenditures, which is particularly important in the face of today's high-end hardware and resource hungry applications. Cloud computing also provides end users with more freedom to access software and data from multiple devices and from nearly any location with access to the Internet.Further, cloud computing frees companies of the costs and logistics involved with maintaining servers and other infrastructure that are provided and maintained by a third party. The following are examples of more specific services commonly offered via the cloud, categorized by SaaS, APaaS, and IaaS:
- Software-as-a Service (SaaS):
    a) Web access to commercial software, such as e-mail, where competitors often use the same software.
    b) Access to software that has discrete and significant spikes in demand, such as billing software that used once a month or tax services software
    c) Web access to other applications that facilitate communications between a company and its customers, such as advertisement or newsletter campaign software.
    d) Mobile applications for web or remote access, such as mobile sales management software.
    e) Pay-Per-Use Applications, such as software for a specific collaboration project that will only to be used for a short term need.
- Application Platform-as-a-Service (APaaS):
    a) Any scenario that involves multiple developers who are collaborating on a development project.

b) Any scenario where external parties need to have visibility to an internal development process.

c) Situations where developers want to automate testing and application deployment services.

d) Development of applications where the development process needs to leverage an existing data source, such as customer information or sales data fromCRM tools.

e) Facilitate iterative and incremental software development by assisting rapid application development.

f) Examples: Google App Engine, Microsoft Azure Services, and Force.com.

- Infrastructure-as-a-Service (IaaS):

a) Where demand on infrastructure — servers, storage, and network and operating systems — is volatile and/or is prone to experience significant spikes and troughs.

b) Providing infrastructure resources to new organizations that do not have the capital necessary to invest in hardware.

c) Providing infrastructure resources to companies seeking to limit capital expenditures in favor of operating expenditures.

d) Providing infrastructure resources to rapidly growing companies where scaling hardware would otherwise be challenging.

e) Fulfilling trial or temporary needs for infrastructure hardware.

2. Intellectual Property in the Cloud

2.1. IP in the cloud

- For the most part, intellectual property laws function essentially the same "in the cloud" as they do elsewhere, and after extrapolating established laws to the Internet for over a decade, the courts and the legal community have generally been able to apply those same laws to cloud-based services. However, certain aspects of cloud computing have unique implications for intellectual property law, and some of those are addressed here.

2.2. Patents

- One interesting aspect of cloud computing is its impact on potential patent infringement by the company that is subscribing to a cloud service, particularly when that exposure is considered relative to the scenario where the company performs that same service internally. For example,

what is the impact on patent infringement liabilities for an e-commerce company when it transfers management of its customer transactions to a third party cloud service provider? In some ways, the risk of patent infringement is reduced and may be harder to establish by a patent infringement claimant. For example, the ability of patent holders to detect infringement performed "in the cloud" may become harder. Other aspects of cloud computing may reduce the likelihood patent infringement too.

- A patented method is only infringed when a single entity performs all steps of the method. See, e.g., *BMC Resources, Inc. v. Paymentech, L.P.*, 498 F.3d 1373 (Fed. Cir. 2007), and *Muniauction, Inc. v. Thomson Corp.*, 552 F.3d 1318 (Fed. Cir. 2008). In these cases the Federal Circuit held that actions by third parties only count toward infringement if those parties are acting as agents of or under the control and direction of the single direct infringer. Accordingly, while a company cannot avoid patent infringement merely by enlisting a third party to perform some of the steps necessary infringement, when key aspects of a company's functions are executed by a third party cloud provider without specific control by its customer, such as running standard applications in the cloud, there are likely more opportunities for divided infringement defenses for the customers.
- Moreover, jurisdictional issues may also minimize certain infringement exposure because United States patents generally do not cover activities outside the U.S., with some exceptions. Specifically, whereas United States patents cover infringing acts that occur entirely in the United States, they typically do not cover extraterritorial activity; under §271(a), U.S. patents are infringed by activity that occurs "within the United States". Thus, when processes performed "in the cloud" are executed on servers in another country, which is common, the cloud customer's patent liability may be reduced by providing an additional non-infringement defense.
- On the other hand, using cloud-based services does not immunize a company from patent infringement liability, and employing cloud services can actually increase patent infringement exposure for a company in some circumstances. For example, as patent enforcement campaigns become more sophisticated, a patent owner may be able to more readily identify infringing activities with more available damages by asserting the patent against a cloud services company rather than independently trying to identify every customer that uses those services. Medium and small companies that otherwise would not have been on the patent owner's radar for patent assertion may now be ensnared in a patent infringement action due to their use of a large cloud services company that is sued for patent infringement.

2.3. Trade Secrets

- Another issue with particular implications for cloud computing relates to trade secret protection. One of the indispensible elements of a trade secret is its secrecy. For example, in *Sasqua Group v. Courtney*, 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010) a New York district court found a company's customer list was not a trade secret because the information at issue had already been disclosed in the cloud. A similar question can be posed with respect to attorney-client privileged information. Delivering confidential information to a third party cloud provider for storage raises the question of whether that information is subject to reasonable efforts to maintain secrecy or whether third party access to that information destroys the legal protection of trade secret. Moreover, even when the information that is stored "in the cloud" is the subject of sufficient secrecy efforts, the information owner must consider whether storing that information in the cloud nonetheless increases the risk that the information will be accidentally or intentionally disclosed to third parties.

2.4. Use of Information for Secondary Purposes

- Finally, many cloud providers do more than just store hosted customer information. In addition to accessing valuable information, such as customer lists or contact information and behavioral targeting information, cloud providers may also mine and perform regression analysis on hosted data. The results of these activities become even more valuable when they are performed not just on a single customer's data but on the aggregate data of a large number of customers. The providers may possess extremely valuable information if they are allowed under the services agreement to access the underlying customer data and use it for these purposes.

3. Risks in Agreements

3.1. Up front due diligence

- One of the best ways to have a successful cloud computing experience is to perform appropriate due diligence on your potential vendors. Ideally, multiple vendors should be able to provide your cloud computing services. A request for proposal ("RFP") should be generated outlining i) the services needed and other technical requirements, ii) your service level (or uptime) requirements, and iii) security and data handling requirements. In addition, it can be helpful to put contractual requirements in the RFP. There is no need to begin negotiations with a vendor if they refuse to accept your required contract provisions.
- You should also consider the type of data that you will be moving to the cloud. For instance, are you moving customer data? If so, does the

utilization of third-party cloud service providers comply with your company's privacy policy governing the use and sharing of that information? If licensed third-party software is being moved to the cloud, is this transition permitted under the license agreements governing this software?

- It can be very helpful to have potential vendors complete a questionnaire on their practices and procedures. A standard questionnaire has been drafted by the Cloud Security Alliance, and is available for download at https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/. This survey includes over two hundred questions, and maps the questions to the vendor's compliance with a variety of adopted standards (including HIPPA requirements).

3.2. Need to negotiate

- Almost every cloud computing provider has a "standard" contract that will apply to most of their customers. These agreements may be available as "click-through" agreements on web sites, allowing small and mid-size businesses to agree to enter into an agreement and begin receiving services without any negotiations. In most cases, these same service providers will be willing to negotiate changes to their agreement for larger customers. It is almost always beneficial to attempt to alter the standard agreements to address some or all of the issues described below.
- To the extent possible, your agreement should require transparency into the services provided by your vendor. For example, the agreement might specify the hardware that will support the service, the location where your data will be stored, and how data will be backed up and restored, and how security will be maintained. If you accept the standard Google Apps for Business agreement without negotiation, for instance, your data can be transferred, stored and processed in "any country in which Google or its agents maintain facilities. If you want to know who has your data, and where they are keeping it, you will need to negotiate that language into your agreement.

3.3. Audit after the agreement

- After the contract is executed and the services have begun, it is still necessary to audit your provider to ensure that they are complying with the terms of your agreement. Ideally, your provider will allow some level of in-person auditing of their facilities.
- Some vendors feel that direct, on-site auditing decreases the security of their customer's data. If on-site auditing cannot be agreed upon, auditing should be conducting by receiving and reviewing reports from your vendor on the status of their hardware, the location of their servers, and the security they are providing for your data. Your vendor should be

required to identify any data loss events or security breaches, even if your data was not directly affected, and any steps taken to remedy these situations.

4. Data Ownership

- One of the primary concerns expressed by companies considering the use of cloud services is the issue of data ownership. Once data leaves the confines of the company's own computer system, questions immediately arise over who owns that data. Does the cloud services vendor who owns the computer systems somehow acquire ownership in the data? If new data is created through the software running on the vendor's computers, can the vendor claim ownership of that data?

4.1. Ownership Provisions in a Contract

- Although this issue is frequently discussed, it is rare that the issue becomes a significant issue in the decision to use cloud computing services. This is because vendors realize that they cannot claim ownership over their customers' data if they expect to survive in the marketplace. Customers need to request that their service contract include specific provisions that clearly spell out that the customer owns all of the data that is placed on the system, as well as any modifications that are made to that data.
- Vendors typically include these provisions in their standard agreement. For example, the Google Apps for Business agreements states that "[a]s between the parties, Customer owns all Intellectual Property Rights in Customer Data," with Customer Data being defined as "data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users." Similarly, the standard Dropbox Terms of Service says simply "You retain full ownership to your stuff. We don't claim any ownership to any of it."

4.2. Licenses to Your Data

- Even though most cloud service agreements provide that customers retain complete ownership of their data, these agreements frequently include a license provision where the customer grants the service provider certain rights to the data. Some of these licenses are broader than others.
- For instance, Dropbox revised their agreement in July 2011 to include the following license language: "By submitting your stuff to the Services, you grant us (and those we work with to provide the Services) worldwide, non-exclusive, royalty-free, sublicenseable rights to use, copy, distribute, prepare derivative works (such as translations or format conversions) of, perform, or publicly display that stuff to the extent reasonably necessary for the Service." Unfortunately, it is unclear whom "those we work

with"includes, and the definition of "Service" is quite broad and does not seem limited to Services specifically requested by the user. This provision appears to be broader than necessary, and likely undermines a customer's expectation that their data remain private and confidential.

- A non-business user of Google Apps is subject to Google's standard Terms of Service Agreement, which includes "a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services." This license is limited to "the sole purpose of enabling Google to display, distribute and promote the Services." Furthermore, Google explains that this "license includes a right for Google to make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services."
- Luckily, the Google Apps for Business agreement does not have these terms. Rather, Google relies on the provision that gives Google the right to "transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities."
- Many of these licenses are overbroad, and should be altered if the customer has the negotiating power to change the agreement. While some right to access and distribute data is required, such a license should be limited to what is absolutely necessary to provide the agreed upon services as requested by the client. The license should not extend to third parties unless that third party is identified and the third party is necessary for the implementation of the services. Furthermore, it is likely that most service providers will have no need to access the actual content of data files to perform their services.
- In addition, some agreements include a license for the service provider to track your usage of their service, and to aggregate such data for commercial exploitation. Customers should consider whether such a privilege is appropriate for their situation. If a customer does not wish to allow such use, it is possible to include a prohibition against such use by making usage patterns subject to the confidentiality (and non-use) provisions of the contract.

4.3. Confidentiality / Non-Disclosure

- If your service provider must have access to the content of your data, then it is extremely important that your agreement include some type of non-disclosure provision. Google includes a confidentiality provision in its Apps for Business agreement, in which Google agrees that Customer Data is confidential, and agrees to use the same standard of care it uses for its

own data. In contrast, the Amazon Web Services agreement includes a merger clause that specifically overcomes any other agreement related to the privacy and confidentiality of your data. The agreement then states only that they will use reasonable security measures, and will abide by their Privacy Policy. This Policy is the general Amazon privacy policy that covers customer data, and does not provide the protections against non-use and non-essential dissemination that would be found in a standard non-disclosure agreement.

5. Access and Control

- While potential customers of cloud services usually express concern about data ownership issues, frequently their concerns have more to do with access and control over the data. Once a company places their data onto the computing devices of a third party, can they access it when they need it? Can they get that data back if something goes wrong? Will the provider adequately protect the privacy of this data? These issues are discussed separately below.

5.1. Data Loss and Backup

- While all potential customers of cloud services are concerned about data loss, in reality most reputable cloud service providers provide a more robust system for ensuring data against loss than almost any of their customers can provide.
- That does not mean, however, that losses don't occur. In one of the more infamous examples of data loss, Microsoft subsidiary Danger lost the data of more than 800,000 Sidekick smartphone users in an October 2009 "server failure" that destroyed both the main and backup databases. The data loss included emails, address book, and photo data. When the data loss was announced on October 10, 2009, users were told that their data was permanently lost. Within a week, Microsoft was able to recover most or all of the data, although the scare caused a severe public loss of confidence in cloud computing. Cloud computing companies have worked hard to avoid similar problems in the future.
- In most cases, the standard agreement provided by cloud service providers will not include any affirmative obligations to back up data.
- Ideally, an agreement with a cloud service provider will include minimum standards for both data backup and disaster recovery plans (i.e., "Business Continuity Procedures" or "BCPs"). Agreements can refer to existing disaster recovery plans of the cloud service providers. Customers can review those plans, and can request the ability to approve significant changes to the plan. Alternatively, the agreement can include minimum requirements that must be implemented in the service provider's BCP. It

can be helpful to include the ability to audit your service provider's implementation of their backup and BCP plans.

- Finally, you may wish to include the ability to periodically archive data that is normally stored on your cloud computing provider's facilities onto a storage system that you control, or on the facilities of a software escrow service.

5.2. Accessibility & Service Levels

- Customers of cloud service providers need a guaranteed level of service. Google Apps for Business includes a Service Level Agreement that guarantees 99.9% availability to customers. Under the terms of their standard agreements, anywhere from 3 days (between 99.0 and 99.9% availability) and 15 days (below 95% availability) credit is given for failure to meet the SLA percentage. These percentages are for the total month, not traditional work hours, and do not include any outages that last for less than ten minutes. In addition, the customer must specifically request the credit or it will not be granted. Furthermore, the promise is subject to the Force Majeure provision, which includes both natural disasters and Internet "disturbances."
- Customers should ensure that an adequate service level guarantee is in their agreement. Furthermore, one should consider whether the credit offered is adequate (for instance, Microsoft's standard SLA provides a 100% credit for less than 95% uptime), or whether other penalties need to be included. For example, a customer may require the ability to terminate the agreement, or to seek specific corrections if the accessibility percentages do not meet the needs of the customer.
- Finally, recognize that general Internet failures will likely be excluded from all SLAs.

5.3. Transition Services, getting your data back

- Every cloud services agreement should include some provision covering the ability of the customer to extract its data back out of the cloud. Vendors must be able to locate, extract, and provide the data in a specified mannerwhenever the relationship between the customer and vendor ends. The agreement should set forth a promise to retain the data even after termination of the agreement to ensure the customer's ability to recover the data and move it to a new provider. In addition, the agreement should explicitly set forth the format in which the data can be recovered, such as XML or SQL. The agreement should also specifically require that the vendor delete all copies of the data at the end of the agreement once the customer has successfully extracted the data.
- Frequently, standard cloud service agreements include some promise to return the data. For example, the Google Apps for Business agreement

states that "Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates for the applicable Services." This agreement also provides that, "after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active and replication servers and overwriting it over time." Although the agreement does not specify the format of the data, Google at least confirms that it will maintain the data even after termination to allow extraction by their customer.

- In contrast, the Amazon Web Services standard customer agreement requires Amazon to retain the data upon termination only if Amazon did not terminate the agreement for cause. Furthermore, the ability to retrieve the content is provided "only if you have paid any charges for any post-termination use of the Service Offerings and all other amounts due."

5.4. Service Provider's End of Business

- In addition to concerns about the end of an agreement, customers of cloud service providers must consider the potential that their provider will cease doing business completely. An agreement that requires that the service provider maintain data and allow data export after contract termination will not be helpful when their servers go dark.
- To avoid this possibility, it is important to perform some due diligence on the stability of the potential provider before entering into the agreement. For some providers, it may be necessary to have access to their financials before the provider can be trusted with your data.
- In addition, cloud computing escrow services are now available. Iron Mountain provides a Software-as-a-Service Escrow service for customers of cloud computing providers. Under this service, Iron Mountain will store executable code on their servers as well as the source code for that software. By frequently copying data from the Cloud Service Provider to the Iron Mountain servers, Iron Mountain can step up and provide access to both the data and the provider's software if the provider goes out of business.

5.5. Litigation Holds and E-Discovery

- Another area in which a customer loses control over its data in a cloud computing context is the ability to implement litigation holds and e-discovery procedures. Digital evidence issues should be considered when negotiating cloud computing agreements. For instance, care must be taken that data can be preserved when a legal proceeding is reasonably anticipated. A customer must ensure that preservation is possible, and should understand how the preservation will be implemented. Technologically, when two "holds" apply to the same document, can the

provider's technology release the first hold for some documents while recognizing that a second hold will prevent alteration or deletion of other documents?

- If business data is to be transferred to the cloud, litigation hold requirements should be analyzed and specifically set forth in the agreement. The agreement should specify a specific mechanism for how the provider will implement litigation holds, and how metadata that may be essential for e-discover will be created and stored in the cloud environment. In some cases, additional services may need to be purchased from outside vendors to be able to properly manage e-discover and litigation holds.

6. Data Privacy

- When data or applications are moved to the cloud, you lose the ability to implement your own physical and information security procedures. Even outsourcing situations usually gave the outsourcing company the ability to require specific procedures to be in place to protect their data. In cloud service arrangements, however, companies must effectively accept the same security procedures that the provider grants to all of their other customers.

6.1. Privacy Loss Examples

- Entities who are first moving their data and applications to the cloud are extremely concerned about the security being implemented by their service provider. As with issues of data loss and backup, usually the move to a cloud computing provider will actually increase the security of a customer's data. Cloud computer providers are extremely concerned with both the physical and data security of their services, and therefore tend to provide some of the most secure locations in the industry.
- However, in spite of this high level of concern over security, some surprising breaches of security have been publicized in the recent past. For four hours on June 19, 2011 anyone could log into any of Dropbox's 25 million users' accounts using any password. In effect, there was no authentication security on any of the data maintained by Dropbox. The bug was caused by a software update, and was corrected within five minutes of being recognized by Dropbox.
- In 2009, Google sent messages to Google Apps users stating that their documents may have been inadvertently shared with other users. Apparently, some documents were shared with any other user with whom the document creator had ever shared any other document, even if the creator never shared the document in question. This privacy bug was discovered by a user, and fixed within two weeks of the first notification to Google.

6.2. U.S. Privacy Regulations

- Before moving any data to the cloud, potential customers should carefully consider all of the regulatory and legal regimes that impose privacy obligations on that data. For instance, HIPPA and the HITECH Act impose substantive requirements on security measures that must be taken to protect healthcare related data that is stored or transmitted on computer systems. Similarly, the Gramm–Leach–Bliley Act is designed to impose certain security procedures on financial data.
- State laws will also impose security requirements, such as an obligation to encrypt social security numbers of customers, either in storage or when transmitted outside the "secure systems" of the business. Such legislation has been enacted in Massachusetts and Nevada.
- If a company is relying upon their cloud service provider to meet their obligations under these Acts, the services agreement should specifically assign appropriate responsibility to the service provider and provide for remedies (and even indemnification) if these obligations are not fulfilled.
- Many times these requirements will directly conflict with the standard agreement of major cloud service providers. If data that is protected by these acts will be migrated to a cloud service provider, the agreements must be modified to require compliance with the particular procedures required by these acts.

6.3. Government Intrusion

- Another area of concern is how your cloud computing service provider will handle government requests for data. While you may not be able to prohibit government ordered disclosures, you want to ensure that you receive notification of such orders in time to challenge the disclosure request. For example, the standard Google Apps for Business agreement provides: "Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure." Dropbox merely states that they will share your data "when we have a good faith belief that disclosure is reasonably necessary to comply with a law, regulation or compulsory legal request" without any notice requirement.
- Under the USA Patriot Act, the government can request access to data from cloud service providers. The CIA, FBI, the Pentagon, and the Homeland Security agency has the right to issue a national security letter (NSL) requesting information from your cloud service provider. The information requested can include non-content information, such as electronic communication transactional records (e-mail headers other than message content or subject fields). The NSL can contain a gag order, preventing the recipient of the letter from informing you that the letter

was received or the communication shared. There is no judicial oversight on the issuance of NSLs, although your service provider may contest the gag order (based on a recent Second Circuit interpretation of the Act). Obviously, there would be no risk of disclosure to the federal government without notice if the data was never placed on the cloud and remained under the control of the originating company.

- Even outside of Patriot Act, the Fourth Amendment protection against unreasonable searches and seizures will provide less protection to data existing on the cloud versus data inside a corporate or personal system. A recent article in the Minnesota Law Journal discussed the risk that the "reasonable expectation of privacy" that limits government searches without a warrant may provide significantly less protection to data in the cloud compared to data maintained by the corporation.

6.4. EU Privacy Directive

- In addition, the European Union privacy directive requires that certain procedures be maintained for the collection and movement of personal data obtained in the EU. This directive has been interpreted to prevent the transfer of personal information to other countries that do not provide an adequate level of protection to the data. The laws of the United States do not meet this requirement, so transfer of information to the U.S. is generally prohibited unless the companies transferring the data agree to certain Safe Harbor provisions.
- In response, most cloud computing service providers abide by the Safe Harbor provisions. In an attempt to further assuage the fears of their European customers, many U.S. providers have agreed to the creation of EU only clouds, in which data in the cloud is not transferred or shared with servers outside the EU.
- Nonetheless, in July 2011, Microsoft admitted that a government order to share European originated personal data under the Patriot Act would likely require Microsoft to share that data. This is true not only for data within the United States pursuant to the Safe Harbor provisions, but also for data that is maintained only on servers within the European Union. This admission caused great concern in the European Parliament, as politicians considered revamping the privacy provisions to further enhance the privacy of European data.

6.5. Example Security Provisions

- Vendors will typically agree to take reasonable steps to secure your data. For instance, the standard Amazon Web Services agreement provides that "we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure." Google's standard agreement goes further, promising that

Google will use security standards "no less protective" than the standard that Google uses to protect its own data, and further that Google has implemented "at least industry standard systems and procedures."

- Ideally, minimum physical and data security provisions will be drafted into your agreement with service providers. Standards are being established for cloud computing security. Private consulting firms have created some of these standards. These firms work with customers to establish appropriate standards, develop specific agreement language relating to security, and create auditing practices to ensure appropriate security. Other public standards are also being proposed and defined.

6.6. Breach Notification

- Various state and federal statutes including HIPPA and HITECH require public notification of security breaches to computer systems. Even when public notification is not required, customers of cloud service providers need to know if the security that is protecting their data has been breached. Therefore, your contract with your cloud service provider should include specific obligations that you be notified as soon as possible after a security breach has been identified.

7. Vendor Liability

7.1. As Is

- Most agreements will not include any warranties on the service. The Amazon Web Services agreement provides the services "AS IS" and disclaims liability for direct and indirect damages, including any liability for an inability to use the service, loss of data, or unauthorized data access. The Dropbox agreement is similar in that the services are provided "AS IS." Google does not provide that the services are rendered "AS IS," but they do disclaim all warranties other than that it will provide the Services in accordance with their Service Level Agreement.
- Ideally, the agreement should include a promise that your vendor will keep your data secure and live up to the other provisions of their agreement (such as service level promises), and provide for penalties if they fail to do so.

7.2. Indemnification

- In many circumstances, the failure of your service provider to live up to its obligations, such as required security or notice procedures, can leave you open to litigation from third parties. To the extent possible, indemnification provisions should provide for the service provider to indemnify the customer for these failures.

7.3. Limits on Liabilities

- If you are successful in negotiating provisions where your vendor takes on some financial risk for failing to live up to their obligations, you should carefully examine the limits on liability in the agreement. In most cases, standard agreements limit liability to the amount paid for the services in the previous twelve months (three months for Dropbox). Removing the limits of liability, at least in part, will greatly strengthen the value of the contract. For example, breaches of confidentiality should be excluded from the liability limitations, as should any indemnification obligations assumed by the service provider.

8. Successful Negotiations

- A good example of what can be obtained by negotiating your agreement is the publicly available agreement between the City of Los Angeles and Google for their Google Docs services. It had been reported that this agreement included the following elements
  - unlimited damages for a data breach
  - audit rights
  - guarantee that the data will stay within the United States
  - penalties if services are unavailable for more than five minutes
  - a non-disclosure agreement with an unlimited damages provision and an agreement that Google will not examine the data
  - a promise to encrypt the data
- Unfortunately, a review of the agreement indicates that the actual agreement achieved less than all of these results. For example, the contract may be read to provide for unlimited damages only if data is disclosed by act of the contractor, not through third party breach.