Cloud Computing: Managing Legal Risks and Ethical Issues

Kathryn L. Ossian
Miller, Canfield, Paddock and Stone P.L.C.

I. Introduction: The Cloud Is Calling

A. What is Cloud Computing?

Cloud computing has gained increasing credibility as an efficient and viable means of doing business. The term itself is somewhat misleading, as it can refer to a wide array of applications and functions. In touting the cloud to consumers, Microsoft portrays it as a magical place where stranded airline passengers can ease their pain by catching up on episodes of their favorite reality shows in the middle of a crowded airport and mothers trying to capture a perfect family portrait can simply cut the distracted faces of her children and replace them accordingly.\(^1\) Microsoft’s corresponding pitch to businesses starts out with the phrase: “I can own way less and do way more.”\(^2\)

Information Technology research firm Gartner, Inc. defines cloud computing as “a style of computing where scalable and elastic IT enabled capabilities are delivered as a service to customers using Internet technologies.”\(^3\)

The United States District Court for the Southern District of New York recently decided a non-compete case brought against a former IBM employee who moved to HP. The court described cloud computing as “allow[ing] businesses and individuals to use the Internet to access software programs, applications, and data from computer data centers managed by providers such as IBM and HP. Cloud computing services are not a unitary product but rather a continuum of services which businesses are able to access on an as-needed basis.”\(^4\)

B. Is It Time to Jump on the Cloud?

Cloud Computing takes place on application servers over the Internet. Cloud computing can be used for network storage, application infrastructure and even general computing resources. It is also referred to as “software as a service” or SaaS, “infrastructure as a service” or IaaS or “platform as a service” or PaaS. Two well-known examples of


\(^3\) [http://blogs.gartner.com/thomas_bittman/2010/05/18/clarifying-private-cloudcomputing/](http://blogs.gartner.com/thomas_bittman/2010/05/18/clarifying-private-cloud-computing/)

\(^4\) International Business Machines Corporation vs. Visentin, 11 Civ. 399 (LAP), U.S.D.C. (S.D.N.Y. 2011); also found at 2011WL 672025.
software as a service applications utilizing cloud computing are Salesforce.com and Google Mail.

In February, 2011, the Federal Government announced a plan to begin moving its agency’s IT resources to the cloud for an estimated savings of $60 billion dollars. The intent of the “Cloud First” policy is to “accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.”

So, if it’s good for the government, is it good for you and your business needs?

II. The Business Case for Cloud Computing

The business benefits of cloud computing are readily identifiable. Using a shared infrastructure reduces the need for hardware and software investment by individual customers, resulting in substantial cost savings and efficiency on many levels. Given that an ever increasing number of well-known and respected companies are offering cloud computing applications increases the likelihood that your organization will become, or already is, one of many users of the cloud.

A. Efficiencies

Replacing the traditional client-server model with a cloud application that is accessible over the Internet by any device with a web browser means many users can share in the efficiencies of this streamlined delivery method. From the cloud provider’s perspective, rolling out new features to its customer base or fixing a bug in the application becomes much easier, as it is done on the provider’s server, rather than separately on each individual customer’s network.

Additionally, there is no lag time, as features and fixes are also enjoyed by all customers simultaneously on a real-time basis in update distribution. According to Cloud ERP Provider, Plex Systems, “since custom feature requests are folded into the base application, Plex Online is never obsoleted with the next upgrade. Typically, new features are enabled when configured.”

---


6 http://www.plex.com/ondemand/cloud-erp.asp
B. Cost Savings

The global cloud computing market is predicted to grow from $40.7 billion in 2011 to over $241 billion in 2020, according to recent Forrester Research forecast data.\(^7\) Individual savings are apparent as the cost of buying access to the cloud is a small percentage of the cost of purchasing or leasing hardware, licensing software and incurring installation, customization and ongoing maintenance expense.

C. Infinite Possibilities

Cloud computing applications are available for virtually every business need. Data storage is a popular use for the cloud. Other basic examples of cloud application uses include email, word processing, calendar, address book, chat, video, blogs, presentations and training.\(^8\) Given the diversity of cloud activity, the specific function and purpose must be examined in assessing the level of accompanying risk.

III. What are the Legal Risks and Ethical Issues?

A. Layers of Clouds

Cloud computing also comes with a variety of risks, many of which are attributable to the fact that clouds may have several layers – e.g., the provider of the cloud application may be using another provider for the platform, a different provider for infrastructure and any of these may outsource various functions to other third parties, such as a credit card processor.

With many potentially different parties involved within the cloud come a variety of potential legal risks and ethical issues.

B. Security and Privacy

The security associated with software and hardware set up at a physical location is within the control of the using entity. The security and privacy of any data housed on a traditional network can be managed with firewalls, other technical security and physical security methods. Security and privacy are not so clear in the cloud.

The security of data stored or accessible via the cloud is within the control of the various providers of cloud services. Some providers try to shift the entire risk of security and privacy to the user in contractual terms of use, offering services on an “as is” basis, without any representations regarding security or privacy and with terms that limit the

\(^7\) As reported in *Sizing The Cloud* by Stefan Ried, Ph.D. and Holger Kisker, Ph.D.

provider’s exposure to liability and damages claims. If you are using the cloud for an application that doesn’t involve any sensitive data, such risk shifting may be acceptable.

C. Ethics of Client Data in the Cloud

On the other hand, trusting a risk-averting public cloud provider with sensitive data (perhaps even client confidential data) may raise ethical implications. Over the past two years, several state bar associations have addressed this issue.

The Arizona State Bar’s Committee on the Rules of Professional Conduct held that an Arizona law firm may use an online file storage and retrieval system allowing clients to access their files over the Internet, provided the firm takes “reasonable precautions” to protect the security and confidentiality of client documents and information.9

In answer to the question: “What are the ethical considerations relating to electronic files?” the Alabama Ethics Commission opined that “[t]he lawyer must have reasonable measures in place to protect the integrity and security of the electronic file . . . [and] take reasonable steps to ensure that the files are secure from outside intrusion.” The Commission noted that, when a lawyer chooses to place client data in the cloud, “there is always the possibility that a third party could illegally gain access to the server and client confidential data through the internet, [but] a lawyer may use ‘cloud computing’ or third-party providers to store client data provided that the attorney exercises reasonable care in doing so.”10

The State Bar of California Standing Committee on Professional Responsibility and Conduct issued a formal opinion in response to the following question:

“Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?”11

The Standing Committee concluded that before using any particular technology, the lawyer must take appropriate steps to evaluate: “(1) the level of security attendant to the use of that technology . . . (2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; (3) the degree of sensitivity of the information; (4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; (5) the urgency of the situation; and (6) the

9 State Bar of Arizona Ethics Opinion 09-04, Confidentiality: Maintaining Client Files; Electronic Storage; Internet (December, 2009); http://www.myazbar.org/Ethics/opinionview.cfm?id=704


11 The State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179; http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqEClHp7h4%3D&tabid=837
client’s instructions and circumstances, such as access by others to the client’s devices and communications.

The North Carolina Bar Association also has proposed a formal ethics opinion on lawyers utilizing cloud computing (or SaaS) services while still fulfilling the duties of client confidentiality. In response to the question “[m]ay a law firm use SaaS?” the Ethics Committee opined “Yes, provided steps are taken effectively to minimize the inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client’s file, from risk of loss.”12

Finally, consider this recent opinion by the New York State Bar Association: “A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer’s obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client’s information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.”13

So, it is clear that state bar associations that have considered the issue unanimously recognize a lawyer’s ability to utilize cloud computing, but caution against a lawyer not exercising due diligence before actually engaging a particular technology.

D. Is a Private Cloud the Answer?

Some cloud providers have obtained a SAS-70 Type II audit, which provides a ‘snapshot’ of security controls by that provider along with a service auditor’s opinion on the effective operation of those controls.14 As cloud computing is used for more diverse purposes, including the storage of sensitive data, such as customer and employee personal information, the security and privacy challenges become greater. How are cloud providers complying with HIPAA, PCI credit card standards and other applicable privacy standards? The answer may lie in the type of cloud being utilized.

A public cloud, while the least expensive, may offer little or no guarantees regarding security and privacy. A private cloud, according to Gartner, Inc. is “a form of cloud computing where service access is limited or the customer has some control/ownership of


13 Ethics Option 842 (September 10, 2010); http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&template=/CM/ContentDisplay.cfm&ContentID=49629

14 The SAS-70 auditing standard was developed by the America Institute of Certified Public Accountants (AICPA). For more information, go to: http://www.aicpa.org/InterestAreas/EmployeeBenefitPlanAuditQuality/Resources/GeneralAccountingandAuditing/SASNo.70andServiceOrganizations/Pages/default.aspx
the service implementation.\footnote{http://blogs.gartner.com/thomas_bittman/2010/05/18/clarifying-private-cloud-computing/} As a private cloud consumer, you are, essentially, buying more control and minimizing some of the risks associated with the public cloud. Presumably, the private cloud provider will be more receptive to contractually agreeing to assume some security and privacy risks and to comply with applicable privacy laws.

There is also a “hybrid” cloud option, incorporating some characteristics of both the public and private cloud, offering dedicated space for sensitive data and using shared resources for those functions and features where extra protection is not required.

E. Other Legal Considerations

**Warranties and Indemnification:** What warranties, if any, come with cloud computing? Will the cloud provider indemnify you if your data is compromised and you are sued as a result?

Providers will seek to limit any warranties on the services offered while users will expect some level of protection. This dynamic is not unique to the cloud, however, the struggle takes on greater importance given the nature of cloud computing – a greater desire for assurance in a setting that may not justify the reliance on any. Again, the private cloud provider may be more willing to give warranties and indemnification than a public cloud provider.

**Tax issues.** One of the unresolved legal issues is whether cloud services are subject to tax. A handful of states, including Michigan, are grappling with whether tax can be levied on cloud computing transactions. Depending on the type of tax being contemplated, factors to be considered in determining taxability include whether a license of software is granted by the agreement, the location, or nexus, of the server and whether the service or software is being delivered to individuals or businesses resident in a state.

Michigan's General Sales Tax Act and Use Tax Act include within their scope "pre-written computer software." A group of eight Michigan state senators have recently introduced bills (Senate Bills 335 and 336\footnote{To review a summary of the bills, go to http://www.legislature.mi.gov/documents/2011-2012/billanalysis/Senate/htm/2011-SFA-0335-S.htm}) that would amend these acts to clarify that software as a service, or cloud computing, falls outside the definition of pre-written computer software and is, therefore, not subject to Michigan's 6% sales or use taxes.

The bills were passed by the Senate on June 16, 2011, and are currently pending before the Committee on Tax Policy in the Michigan House of Representatives. The bills would operate retroactively and specify that the right to use pre-written software installed on another person's server is not a taxable transaction. It is too early to know whether these bills will become law, however, anyone engaged in providing cloud computing services as well as consumers of those services should remain interested in what develops.
**Jurisdiction:** Which court will have jurisdiction to hear and decide a dispute with a cloud provider? The traditional notions of physical presence that often guide courts to determine appropriate jurisdiction and venue can be more complex in the cloud. Jurisdiction may depend on where the cloud provider is headquartered, which may not be the same place that the cloud is located. If you are dealing with a public cloud provider offering boilerplate terms of use, you may have to agree to that provider’s choice of jurisdiction and venue. In a more negotiated setting, you may have the opportunity to contractually agree upon a location that is more palatable.

**Control and Retrieval:** Who is controlling data in the cloud? Data control and retrieval can often be a critical issue. You certainly want the ability to potentially switch providers and, thus, move your data from one to another without undue burden. How long will your data be retained after you have terminated your arrangement with the cloud provider? In what manner will your data be returned to you? Each of these topics can and should be covered in your negotiated contract, if you have the opportunity to negotiate at all.

Furthermore, if you receive a subpoena or document request for data stored in the cloud, you’ll need to be able to retrieve your information or face possible sanction for the inability to do so. The cloud provider may not be interested in your dilemma or, even if interested in assisting, may not be able to oblige. Before storing critical data in the cloud, make sure you either retain copies or have an agreed upon method of retrieval. Again, the potential to negotiate these points will depend on the type of cloud services you are purchasing and the relevant leverage between you and the cloud provider.

**IV. Minimize the Risks of the Cloud**

You cannot control or eliminate the risks associated with cloud computing, but you can minimize those risks by following some important steps:

- Carefully consider the type of data to trust to the cloud
- If client data or information is involved, make sure you have exercised reasonable diligence in assessing the security and privacy risks of your chosen cloud provider(s)
- Consider public, private or hybrid cloud options
- Think about obtaining insurance coverage to help protect against the risks
- When possible negotiate key contractual terms with the cloud provider, including:
  - responsibility for employees and subcontractors
  - compliance with applicable laws and regulations
  - minimum security standards, including authentication methods

---

The cloud is an exciting new technology frontier. In light of the forecast for potential risks, braving cloud computing without seeking protection from the legal and ethical risks is ill advised.