C L O U D C O M P U T I N G

Risks / Challenges - Legal & Tax Issues

MY CLOUD, YOUR CLOUD, WHOSE CLOUD?

Nishith Desai Associates
Legal & Tax Counseling Worldwide
Mumbai • Silicon Valley • Bangalore • Singapore • Mumbai-BKC • New Delhi

Table of Contents

EXECUTIVE SUMMARY

The evolution of the Internet coupled with the development of massively scalable IT infrastructure is revolutionizing the storage and dissemination of information and communication technologies creating epoch-changing implications on business models and processes. These technologies include development tools, software and applications, network services, etc., which organizations, in the past, would have licensed or purchased, and installed, maintained and managed all by themselves at exorbitant costs. These technologies are now being bundled and repackaged into a distinct outsourcing service model and offered on "pay as you use" basis. Thanks to *Cloud Computing*!

As the hype continues to surround cloud computing as a viable business solution, it is interesting to look at the ability and opportunity for India to exploit this technological phenomenon. In our paper, we aim to outline the concept, rationale, and various models of cloud computing as well as offer greater clarity on the legal and tax issues associated with cloud computing.

A. INTRODUCTION

In late 1990s and early 2000s, organizations spent enormous amounts of money to set up their own IT infrastructure including purchasing dedicated servers and equipments for running their business applications. Gradually, the servers became virtual and accessible through the Internet and this was the period when the 'cloud' was born. The Internet and 'cloud' have now become so intertwined, that the 'cloud' shape is frequently used to represent the Internet in flow charts and diagrams.

Although the phrase "cloud computing" is somewhat new, the elements of the concept have been around for many years. In practice, cloud computing is not a new concept nor any new technology nor any new computing paradigm nor a new phenomenon. Cloud computing encompasses several technological practices that existed long before the phrase became popular. Hence, this is perhaps the reason that many of us have already been using cloud computing in some way or the other. For example, free personal email, such as Yahoo! Mail or Gmail, (unless we download and store the same on our desktop or laptop), we access at absolutely no cost from a third party server that may be hosted anywhere in the world without us having any knowledge of where those servers are located.

To understand the concept of cloud computing in the most basic sense, let's look at a physical world example: Imagine four employees of a company availing car pooling services. The car in which they travel from their respective homes to their office can either belong to any one of them or they may avail services of a third party car pooling company. In case of the latter, the ownership of the property (car) does not belong to the employees, however, they own the articles (such as bags, laptops, documents, etc) which they carry along with them in the pooled car. They pay the car pooling company for availing the transport services as per their actual usage and the car is available to them as and when required by them. Similarly, the essential characteristics of 'cloud computing' are;

- Pay as per use;
- Use it 'as and when required';
- Services provided by a third party service provider;
- No change in the ownership of the main property.

Further, in a cloud computing environment, a cloud can either be a 'public cloud' or a 'private cloud', similar to one of the employee owning the car (or joint ownership of the car by all four employees) or the car pooling service owning the car respectively. While essentially the end result of using a public cloud or a private cloud remains the same, there is a slight difference between the two. A public cloud offers cloud computing solutions to almost anyone who has access to the internet and generally at no or low cost. On the other hand, a private cloud is typically a private data center/network that offers cloud computing solutions to a limited number of identified users at a certain or shared cost.

B. CLOUD COMPUTING: PRIMER

Although many definitions prevail with respect to cloud computing, there is no standard definition. In the simplest sense, cloud computing can be defined as:

> *An abstract computing and data storage business method where dynamic IT capabilities such as hardware (Infrastructure-as-a-Service), software (Software-as-a-Service) and tools (Platform-as-a-Service) are provided by third parties/cloud service providers which enables users to store as well as access their data and applications virtually from anywhere and through any connected device.*

It is also sometimes referred to as synonymous to server hosting. Cloud computing services are provided 'on demand' as opposed to licensed or purchased software, tools and hardware. Cloud computing resources are offered 'as a service' on 'as needed' basis and the payment for the same is also either 'subscription' based or 'pay as you use' basis.

Based on this understanding of the term 'cloud computing', there are three major elements or delivery mechanisms for cloud computing[1]:

- **Infrastructure as a Service (IaaS) or Hardware cloud:** Under the IaaS model, instead of purchasing large and costly infrastructure such as data center, virtual servers, network infrastructure, equipment, etc, users, generally large organizations, source the same as a service from third party service providers. The payment mechanism under this model is 'pay as you use'. The hardware cloud infrastructure allows users to expand as well as contract their requirements based on their business needs. *Example*: Amazon Web Services, EC2, Gogrid.

- **Software as a Service (SaaS) or Software cloud:** A software cloud is a specialized software that runs on the hardware cloud. Under this model the service provider hosts several software applications for users to use the software as and when required thereby eliminating the need to install and run the software application on the user's computer and also simplify maintenance and support expenses. This service is in the form of web services and is made available to users over a network which is normally through the web/Internet. Because the service provider hosts both the application and the data, the user is free to use the service from anywhere. *Example*, GoogleDocs, Salesforce.

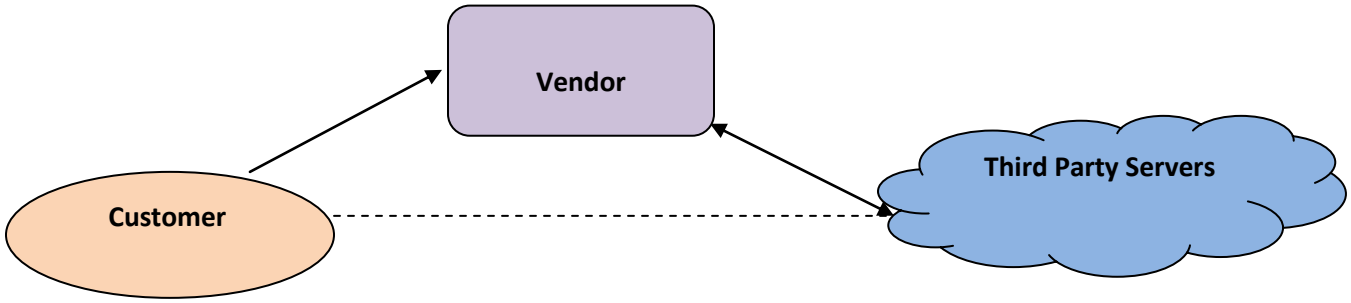
- **Platform as a Service (PaaS) or Desktop cloud:** With PaaS, software developers can avail the platform services to develop various applications without installing and maintaining any tools on their computer. PaaS tools are hosted on service provider's IaaS. Once developed, these applications can be then be tested and deployed without much trouble and effort. Example, Facebook, GoogleApps, Ning, 10gen.

[1] http://ww.accenture.com/NR/rdonlyres/321DC1B6-9A79-4F0E-8C5A-E1807444D52B/0/OutlookPDF_Edge_01.pdf

C. ILLUSTRATIVE MODELS

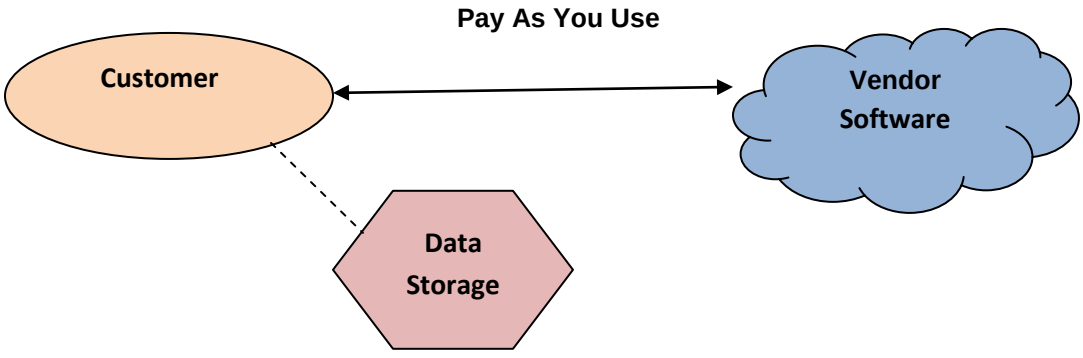
1. SERVERS USED FOR DATA STORAGE

The customer has its own software / applications and enters into a contract with a vendor to electronically store data. However, such vendor simply stores the data on third party servers. Such third party does not have any rights to tamper / modify the contents of the data. Thus as per this model, the data of the customer is stored on third party server even though the customer has entered into a contract with another vendor.



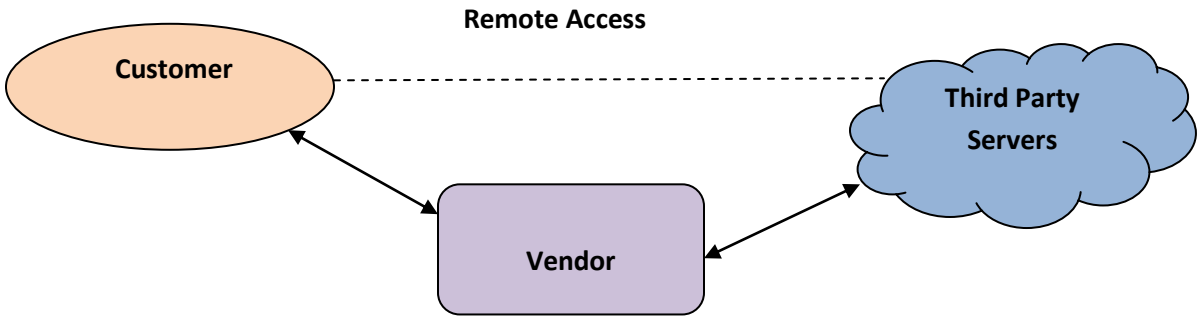
2. SOFTWARE / APPLICATION USED ON NEED BASIS

The customer receives the right to use vendor's software solely on a need basis. The software is electronically run on the customer's platform for a limited period. All data generated is stored on the internal servers belonging to the customer. Thus, the vendor's software is only used for a limited period and is based on a *pay as you use* model.



3. REMOTE USAGE

The customer enters into a contract with the vendor to use software applications which reside on servers belonging to third parties. The vendor has a contractual arrangement with such third parties for hosting such software. The customer remotely uses vendor's proprietary software which is stored on third party servers. In such model, even though there is no agreement between the customer and such third party, the customer has access to the software.



D. ADVANTAGES OF CLOUD COMPUTING

Cloud computing is essentially part of the Internet itself. While the Internet is fast enough to transmit data to a user from a remote server, it is not fast enough to handle voluminous data and applications. Cloud computing comes to the rescue. Let us now see some of the advantages of using cloud computing services.

- **Scalability, Flexibility & Mobility:** Cloud computing helps organizations to access additional computing resources as and when required especially when their business requirement amplifies. Depending on the growth and fall in the business environment, organizations can accordingly scale up or scale down its requirements. By sharing computing resources, an organization can get more flexibility than earlier computing methods by availing computing resources only as and when required. Cloud computing also offers mobility as it enables users to access information whenever and wherever, as required.

- **Automation:** Cloud .computing enables automation of an organization's existing as well as proposed data management requirements.

- **Resource sharing:** By enabling multiple sharing of computing resources, organizations can do away with creating or setting up their own infrastructure. Further there is no requirement to have a separate storage/data center.

- **Unlimited Storage:** Cloud computing offers virtually unlimited storage space for storing vast amount of voluminous data and applications.

- **Cost reduction:** Sharing common IT infrastructure allows an organization to do away with setting up its own datacenter, network infrastructure and other resources and thereby considerably reduce both capital and operational costs. Further, organization need to pay only for the services they use which is usually subscription based or as per 'pay as you use' basis.

- **Focused approach:** By sharing of resources, organizations can have better IT management in place and they can focus on more warranted activities like research and development, innovation etc which are vital for the business.

E. RISKS AND CHALLENGES IN CLOUD COMPUTING

On the flip side, cloud computing also throws up certain challenges. Unlike conventional service providers, vendors of cloud computing solutions or cloud computing service providers do not cater to a single organization but cater to hundreds and thousands of organizations and end users over a single virtual infrastructure located somewhere over the Internet. Hence organizations need to undertake assurances from such vendors and service providers that their data hosted on virtual infrastructure is safe and secured.

The other challenges in a cloud computing environment may be from a technical, business, regulatory or legal perspective. Quite often these challenges overlap with each other. We have discussed below the likely issues/risks/challenges which may be faced in a cloud computing environment and have also provided insights from an Indian law perspective.

I. DATA SECURITY

a. **Data Privacy and Confidentiality:** Cloud computing solutions can be availed by any user – individual, business, government agency, etc. Under a cloud computing environment, privacy and confidentiality are one of the major bottlenecks. The question that often arises is that can any and all data be legally shared? Generally an individual user may not mind sharing his information with the cloud service provider whereas an organization may be apprehensive of sharing its proprietary data. In some jurisdictions and for some businesses there may be industry-specific laws and regulatory challenges which either totally prohibit or restrict the sharing of data. Example, for a healthcare company in the US, the Health Insurance Portability and Accountability Act (HIPAA)[2] lays down certain restrictions in relation to the sharing of medical records of individuals. Also, the Reserve Bank of India has issued guidelines for banks to follow a code of conduct where banks outsource their financial services to a third party[3]

   Thus, all parties involved in a cloud computing service may be required to know various applicable laws which seems highly unlikely and unpractical especially from the user's point of view.

   Also, there could be instances where a cloud service provider may be dealing with highly sensitive data for and on behalf of various organizations who may be competitors. Once an organization's data is on the public cloud or the organization's server, it should ensure all reasonable methods are used to protect such data. Thus, vendor contracts need to clearly specify control mechanisms so as to ensure the secrecy and protection of data.

[2] www.hipa.org
[3] http://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.pdf

In India, the Information Technology Act, 2000 ("**ITA**") was enacted to facilitate the development of a secure regulatory environment for the multiparty use of information technology and electronic commerce. The Government of India has recently notified the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**Rules**").

These Rules prescribed guidelines for the collection, usage and protection of *sensitive personal data or information* of natural persons (hereunder referred as **"sensitive personal information"**) by a body corporate which possesses, deals or handles such data in a computer resource which it owns, controls or operates. However, some provisions of these Rules in relation to collection / disclosure do not apply to a body corporate who is providing services under a contractual obligation with any legal entity located within or outside India.

Thus, various cloud computing models / transactions which involve any sensitive personal information along with a nexus to India would need to be closely examined to determine the various compliances under these Rules, as any breach shall be subject to penalties and or damages as prescribed under the ITA.

Additionally, the ITA also provides for punishment for disclosure of *personal information* in breach of a lawful contract which includes imprisonment for a term which may extend up to three years. Therefore, companies and service providers would not only need to adhere to the rules / regulations as prescribed under the ITA but would also need to adhere to the contractual provisions as agreed with the customer.

b. Security: Safeguard and security of software and data is perhaps one of the foremost concerns in a shared third party outsourcing arrangement as the same is beyond the organization's firewall. Especially when an organization's business involves securing client data and catering to sectors such as defense, aerospace brokerage, etc., security is becomes a very pertinent issue.

Under the ITA, a corporate entity in possession of sensitive personal information shall have the obligation to maintain a privacy policy and make available to the provider such privacy policy on its website. Also, the body corporate shall protect the sensitive personal information through *'reasonable security practices and procedures'* as specified under the Rules. In the event the parties do not contractually agree to *reasonable security practices and procedures*, then the minimum standard to be followed for protection would be IS/ ISO /IEC / 27001.

Further, the body corporate is obligated not to disclose the sensitive personal information without the prior approval of the provider of the information unless otherwise agreed under a contract. It should also be noted, while transferring the information to a third party, the body corporate needs to ensure that the transferee is maintaining the same level of 'reasonable security practices' as maintained by the body corporate.

c. Backup: Backup can be taken by an organization in two ways, internal and external. An organization can internally take a backup on its existing server or it can alternatively take a backup at the vendor's end. If an organization was to take a backup on its own end, then the very purpose of moving enterprise data over the cloud would make little or no sense. Further, if the backup is taken at vendor's end (i.e. over the cloud) existing threats would still prevail such as data privacy, security, accessibility, etc.

From an Indian law perspective, the Rules in relation to *Data Privacy and Security* as stated in the above boxes shall be applicable in the event of backups.

d. Interception / Encryption: Certain countries have laws relating to interception of data. Further, during the pendency of a law suit or during a government probe, an organization may be required to allow the investigating agency to access organization data. As data resides across the clouds, it may be difficult for investigating agencies to have easy access to data. On the security front, encryption levels may differ from country to country. For example India allows data encryption only up to 40 bit although the world is considering encryption beyond 256 bit, thus the standards of decryption would also need to be factored.

Under the Rules, government agencies can seek *sensitive personal information* from a body corporate without the prior consent of the provider of such information if such disclosure is necessary under law.
However, it should be noted that if a government official in possession of such information, discloses the aforementioned to a third party without the consent of the provider, he shall be liable to pay damages if there is a wrongful loss to the aggrieved person. Also, depending upon the equipment / instrument used in a cloud computing environment, there is a possibility that the provisions in relation interception under the India Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933 may be applicable.

II. LOSS OF CONTROL

a. Ownership and Control: Organizations can store their data on a private or a public cloud depending on the availability or economic viability of storing such data. However, the risks in relation to ownership / control while storing data on a public cloud are much higher as a public cloud operates on a non-exclusive basis.

When data and applications are transferred onto the cloud, some organizations fear that such transfer may tantamount to loss of ownership / control of their data or application. It must be noted that such data and applications are the organization's property and an organization via its contractual arrangements must ensure that complete ownership and control over the same is retained.

There may be questions as to who owns the cloud computing resources. The vendor's contract may not reveal the name of the real owner, as these services could also be outsourced to third parties. Also, there might be instances where the original vendor sells or assigns its business operations to another party without prior intimation to the organization and therefore the organization may have no opportunity to remove its confidential data before the transfer.

Therefore organizations should ensure that clauses such as assignment, indemnity, confidentiality, ownership, change of control etc are adequately addressed in the agreement with the cloud computing service provider so as to mitigate all risks on ownership / control.

As per Indian laws, usually an entity who originally owns the data shall continue to be the owner of the data stored in the cloud, unless otherwise agreed contractually. Currently, there is no specific Indian law governing the ownership of data on a cloud.

b. Intermediary: Intermediaries in the virtual world '*bring together or facilitate transactions between third parties on the internet*'. They provide virtual access to, host, transmit and index content, products / services originated by third parties or provide net-based services to such third parties. Under most data protection laws, there exist certain safe harbor principles when intermediaries are absolved of liabilities.

Thus, for organizations who avail cloud computing services of intermediaries, need to ensure that their rights are adequately safeguarded, subject to compliances under relevant laws.

An intermediary under the ITA would be liable for breach of security practices or a breach of contract. However, an intermediary can be exempt from liability if it can be shown that the intermediary is merely acting as a conduit and is not in a position to exercise control over any material or information and the intermediary has exercised due diligence as may be prescribed by the Government.
Further, an intermediary would not be exempt from liability where:
(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act; or
(b) the intermediary upon receiving actual knowledge, or on being notified by the appropriate Government that any information, or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

It should further be noted that where the provider of the information is affected or harmed due to the information posted/hosted on the intermediary's computer system, then the intermediary shall remove such information within thirty six hours being informed.

c. **Data Storage Location:** Conventionally, a customer could decide on the control and location of the data, including the location where the backup could be stored. Existing cloud computing solutions require data and applications to be stored in the cloud whose location is usually unknown and most likely organizations end up dealing with multiple clouds. This fragmentation may adversely affect the organization as the data transfer / privacy laws of one jurisdiction may be more onerous than the other jurisdiction.
This freedom could also result in the non-compliance of worldwide laws pertaining to storage and transfer of data. Also, it needs to be evaluated as to who can be held responsible and accountable in cases of data disaster where an organization's data is completely lost / destroyed.

As per Indian laws, usually an entity who originally owns the data shall continue to be the owner of the data stored in the cloud, unless otherwise agreed contractually.
Under the ITA, a corporate entity when transferring sensitive personal information to another entity should ensure, that the entity to whom such information is being transferred should have similar security practices to protect such information
Further, a corporate entity in possession of sensitive personal information should ensure that the provider of such information is aware of the agency collecting and retaining information, the intended recipients of the information and the purpose for which the information shall be used.

d. Audit: Certain countries require businesses to undergo a formal audit exercise. For an organization, when an external audit is undertaken, data privacy and confidentiality aspects need to be given due importance as the auditors may be viewing / accessing data which may be virtually hosted on third party servers. Also, for a cloud service provider it remains to be seen as to how an audit can be undertaken as the infrastructure is located virtually on the Internet and across various jurisdictions.

As per the ITA, data security audits need to be carried out by companies through independent auditor duly approved by the Government, at least once a year or as and when the company undertakes significant upgradation of its process.

III. VENDOR RELATION ISSUES

a. Governing Law And Jurisdiction: According to the traditional rules of private international law, the jurisdiction of a nation only extends to individuals who are within the country or to the transactions and events that occur within the natural borders of the nation[4]. However, this traditional jurisprudence on jurisdiction has evolved with the advancement of commerce and technology.

In a cloud computing environment, an organization which is a resident of one country may store data on a cloud which is located in a different country and such cloud may belong to a vendor who is located in a third country. Thus, there could be a situation whereby the laws of three jurisdictions are applicable.
Subject to the laws / dispute resolution mechanism agreed under the definitive agreement, if there is any problem faced by the organization while accessing the data from the cloud or when there is any infringement action, the question which would then arise is which is the appropriate jurisdiction for the purposes of ascertaining the cause of action for initiating a claim. Will it be the country where the server / data center is located or where the infringing act took place or where the parties reside? To add, USA and most member states of the European Union have directives / laws on data privacy which may also encompass jurisdictional forums.

Therefore, various factors would need to be considered while determining an appropriate jurisdiction along with the harmonization of domestic laws of each applicable country, to avoid conflict of laws.

As per Indian laws, the parties have the right to choose the law which would govern their contractual relationship. However, courts in India have also considered the choice of law as agreed in the contract and its nexus to the transaction.

Further, the Indian Arbitration and Conciliation Act, 1996 (the "Arbitration Act") is based on the UNCITRAL Model Law (*as recommended by the U.N. General Assembly*) and facilitates international commercial arbitration as well as domestic arbitration and conciliation.

However, a significant issue that may arise with both litigation and arbitration is in enforcing a foreign judgment or award in India. Although, India is a party to the New York Convention (1960) which has been signed by around 140 countries, under section 45 of the Arbitration Act, India has notified only about 45 of these as reciprocating territories. Therefore, awards delivered only in those 45 countries (*i.e. when seat of arbitration is in a reciprocating territory*) can be enforced in India on a reciprocal basis. Similarly, India recognizes about 12 countries for the reciprocal enforcement of judgments. Thus, a judgment or award from a jurisdiction that has reciprocity will be enforced in India as though it is a decree of the Indian courts. On the other hand, a judgment or award from a non-reciprocal jurisdiction cannot be directly enforced as a decree in India.

[4] "Private International Law", Cheshire and North, 11th Ed. pg. 188

b. **Integration and Service Levels:** Data and applications as well as the infrastructure that are stored in various scattered clouds need to be eventually integrated. Quite often organizations may be posed with an integration problem where they are unable to have complete access to its dispersed resources. Further an organization's existing network and infrastructure may be such that it may not be compatible with the applications / infrastructure of the cloud provider. Thus if the vendor's infrastructure creates any performance or integration problem then the entire purpose of cloud computing would get compromised.

Also, cloud computing adopts the availing of shared resources from various third parties. In such a scenario, service levels may differ from provider to provider and hence organizations have to ensure that service levels are not compromised and are consistently maintained. Conversely, if the data and applications are accessed from an organization's server then it is easy to control the IT environment in which the data and application are accessed. But this is not true when the data resides over the cloud. Cloud providers may not be able to guarantee response time or service/quality levels because the data and applications may be on multiple servers hosted in various jurisdictions.

Till there is a concrete solution on service/quality level guarantees, cloud computing may prevent organizations from migrating their critical and existing enterprise applications onto the cloud.

Integration, service levels and the rights / obligations subsequent to the same, would solely depend on the parties contractual arrangement, which would be governed in accordance with the Indian Contract Act, 1872, in the event the governing law of the contract is Indian law.. However, while transferring sensitive personal information to a third party, a company would need to ensure that the transferee is maintaining the same level of 'reasonable security practices' as maintained by the company itself.

c. **Vendor Contracts:** Market vendors who provide cloud computing services usually have one sided contracts or service level agreements which are not easily negotiable. For example, an online-click wrap cloud computing agreement is non-negotiable and very vendor friendly. In such agreements the vendor would not make any representations nor would it provide any warranties in relation to the data security, protection, backup etc. Also, all claims and liabilities arising from the acts of the vendor would be disclaimed.

Further, as per the traditional software licensing models, organizations are granted perpetual licenses to use the software/application on customer's own premises whereas under the cloud computing model, generally a limited license right is granted for a limited period for using the application which is stored on vendor's premises. Also, the fee is paid on 'pay as per use' basis unlike the customary model where either a fixed or recurring fee is paid. This paves the way for certain contractual implications in the area of payments, warranty, termination, liability, protection of confidential, etc. Organizations therefore need to negotiate

contracts with vendors in such a way that it leads to a win-win situation for both, vendors and organizations.

Under Indian laws, e-contracts are governed by the basic principles governing contracts in accordance with the Indian Contract Act, 1872. The ITA Amendment has introduced Section 10A which fortifies the validity of e-contracts such as click wrap agreements. This section provides that communication, revocation and acceptance of proposals shall not be deemed to be unenforceable solely on the ground that electronic form or means were used for expressing such offer, acceptance or revocation. Therefore, unless expressly specified under a specific statute, e-contracts like click-wrap agreements would be enforceable and valid. However, there still exists ambiguity on the issue of whether e-contracts are required to be stamped. The ITA and the stamp laws are silent on this aspect. The manner of paying stamp duty as contemplated under the stamp laws is not feasible in cases of e-contracts unless the same are printed. In India, this issue is still at the nascent stage and there is no real jurisprudence on the same.

d. **Willingness to Cloud:** Many organizations may not be willing to move their private and proprietary data over the public cloud as this paradigm shift may not yet be culturally acceptable to the organizations. Cloud computing is not viable for users having low/weak or poor internet connectivity. Even on a fast Internet connection, web based applications can sometimes be slower than accessing a similar software program on your desktop PC / laptop / notepad.

e. **Standardization:** Many organizations may have their own procedures, standard templates, policies and guidelines which they may want to follow even when dealing in a cloud computing environment. Further, these organizations may also want the vendors to follow these procedures, standard templates, policies, etc. Certain vendors may be unwilling to accommodate and this may result in a conflicting situation for both the parties and thereby may create a deadlock.

As per the ITA, where parties do not contractually agree to security practices and procedures, the corporate entity in receipt of sensitive personal information would need to follow a minimum standard of IS/ ISO /IEC / 27001 for protection of sensitive personal information.

IV. TAXATION

E-commerce taxation in India has been rapidly evolving in recent years with a number of judicial pronouncements examining the tax implications of various cross-border service models. However, cloud computing, being a relatively new phenomenon, has neither been tested by the Courts nor scrutinized by the Indian tax authorities. Keeping in view some of the popular cloud computing models in vogue today, certain specific issues may be identified from an Indian tax perspective. The issues broadly relate to those of income characterization and permanent establishments (PE).

The income characterization controversy in e-commerce transactions has assumed immense significance in the Indian context with the tax authorities adopting a counter-OECD position that the income received by foreign service providers in most service models are in the nature of royalties and hence would attract a withholding tax in India at the rate of around 10%. However, if it is characterized as business profits, such income would be taxed in India only if the foreign entity has a PE or a business connection (in the absence of a tax treaty) in India. Under the Income Tax Act, 1961 (ITA), the definition of royalty covers both consideration paid for the right to use certain IP rights (such as copyrights, patents, secret formulae, etc.) and the right to use scientific equipment. A similar definition appears in several tax treaties signed by India. From a broad analysis of the definition, it may be possible to interpret it in a manner that would cover a number of cloud computing models. For example, if the client is entitled to exercise sufficient control over the cloud server or any part of its functionality, it may be viewed as the use of scientific equipment and the consideration would be treated as royalty income. This would also be the case if the service contemplates a transfer of the right to use certain IP rights such as the copyrights in a certain software stored on the cloud server which may be commercially exploited by the client.

In the case of *Re: IMT Labs (India) (P) Ltd*., AAR No. 676 of 2005, a license agreement was entered into between an American and an Indian company for the use of the 'Smarter Child' software on the former's server platform for the purpose of producing, hosting and distributing 'Interactive Agent' applications. The Authority for Advance Rulings held that periodic receipts received in consideration for the service was in the nature of royalties since it constituted payment for the usage of scientific equipment. Similarly, in the case of *Re: Cargo Community Network Pte. Ltd*, AR-2007-7, the payment made by an Indian subscriber to a Singapore service provider for providing access to a portal hosted from Singapore was held to be royalty income. The reasoning used was that since the portal allowed access to a number of value added data processing and information services rendered by the Singapore based server, the client in a way secured the right to use this scientific equipment.

These decisions do not seem to be in sync with the principles of e-commerce taxation endorsed by the OECD. At the same time, it is true that it may be difficult to arrive at any concrete conclusion on the appropriate tax treatment of new business models like cloud computing involving multiple (and intricately connected) features or transactions. For instance, in certain situations, an argument may be raised that payments for certain forms of cloud computing

services may be classified as fees for technical services, the tax implications of which are similar to that of royalty. However, in standard structures where the client does not exercise any control over the cloud server and merely procures certain platform, infrastructure or support services, the consideration paid to a foreign service provider should normally be treated as business profits. Such consideration would be taxable in India only if the service provider has a PE in India.

Cloud computing also raises certain PE related issues. Depending on the type of control that the client may exercise over the cloud server, an issue arises regarding whether such a server would be viewed as a PE of the client in which case any profits earned by the client that is attributable to the services may end up being taxed in the country where the server is located. It may be noted that there is a degree of international consensus that a server carrying out stand-alone intelligent processes may be treated as a PE.

As the Indian tax authorities and Courts grapple with the tax implications of emerging e-commerce models, it is necessary to arrive at solutions that further the principle of neutrality in the tax treatment of e-commerce and ordinary commerce. The impact of the new Direct Taxes Code, proposed to replace the ITA from the finance year 2012, on new age technologies such as cloud computing would also have to be carefully examined. For instance the draft Direct Taxes Code seeks to tax technical services rendered to an Indian resident even if the services are not rendered in India. From a policy perspective, it is necessary for law makers to ensure that tax and other regulatory factors do not act as an impediment to the growth of innovation and technology. While this Direct Taxes Code is still in the draft form it would be useful for the government to provide clarity on the above issues.

F. CONCLUSION

As has been seen from the aforesaid sections, cloud computing is both a business delivery model and an infrastructure management methodology. Cloud computing, which facilitates convergence of several IT mechanisms, represents a new paradigm that will significantly impact the way organizations deal with their proprietary data, IT infrastructure, applications and business processes and the way in which these are procured, delivered, accessed and supported. The wider adoption of cloud computing systems will promote competition thus thriving innovation and bringing down prices for the end consumer. However, various challenges/issues as mentioned in this paper need to be addressed before widespread adoption of cloud computing is undertaken.

Over the years we have seen that technology and business are interdependent. It is becoming practically impossible to separate technology and business. Cloud computing is nothing but a business methodology and only time will tell as to how beneficial it is for undertaking business functions.

The cloud computing trend is likely to lead to new business models along with the evolution of contractual arrangements between service providers and their customers. Corporate customers may obtain significant benefits from this movement but they must also understand and be prepared for the implications and potential risks involved in these new arrangements.

Many organizations may not be forthcoming to put their data and applications over the cloud instantaneously. In such a scenario, organizations can take a tactical experimental approach of moving its non-core and non-strategic applications onto the cloud and internally concentrate on more core, strategic and important business areas. In this way organizations, without undertaking any significant risks, can better understand the cloud computing concept and simultaneously also determine whether cloud computing is really beneficial to them.

Further, it has been seen that business and technology is interdependent to a large extent. As business expands, organizations will have to keep themselves updated with changes in computing and technology. Cloud computing is sure to benefit these organizations in the long term and seems to have the potential of going much beyond that.

As technology such as virtualization and corresponding management services like automation, monitoring and capacity planning services become more mature, cloud computing will become more widely used for increasingly diverse and mission-critical workloads.

G. REFERENCES

- www.opencloudmanifesto.org
- What Cloud Computing Means to You: Efficiency, Flexibility, Cost Savings – 2009 Executive Report – IT Business Edge as available at http://www.hostmysite.com/cloudhosting/WhatCloudComputingMeanstoYou.pdf
- http://www.appistry.com/cloud-info-center
- http://rbidocs.rbi.org.in/rdocs/notification/PDFs/73713.pdf
- Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, Feb 23, 2009 by World Privacy Forum available at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf
- http://ww.accenture.com/NR/rdonlyres/321DC1B6-9A79-4F0E-8C5A-E1807444D52B/0/OutlookPDF_Edge_01.pdf
- Private International Law", Cheshire and North, 11th Ed
- http://www.mit.gov.in