**CLOUD COMPUTING AND ITS LEGALITIES IN INDIA**

Pritish Sahoo and Taruna Jaiswal*

1. **INTRODUCTION**

Cloud computing refers to mode of storage of data and information that concerns providing hosted services over the internet. Basically, it refers to the activity taken on by IT service companies for delivering storage necessities as a service to a company of end-recipients. All cloud computing modes depend greatly on resource and data sharing. This type of data centre setting authorize organizations to get their applications up and running quicker, with simpler manageability and barely any maintenance, and eases IT companies to regulate more promptly, its IT assets namely servers, storage and networking to meet irregular and unpredictable business requirement. The negative side is that vast concentration of information at single centre makes it more susceptible to cyber attacks; and the excessive power given to cloud companies to manage resources, amplifies the threat of a potential untrustworthy conduct. The system seems to be in emerging stages in India. The fact, although, is that, cloud computing is doubtful in India since cloud providers do not take cloud computing due diligence very sincerely.

*5th Year Students, KIIT School of Law, Bhubaneswar, Odisha (India).*
The technical meaning of cloud is an infrastructure that provides on demand resources or services over the Internet, which depends on the scale and reliability of a data centre. Storage cloud meaning which provides for storage services (block or file-based services); similarly a data cloud is one which provides for data management services (record-based, column-based or object-based services); also there is compute cloud which provides for computational services. Usually these are stacked together to serve as a computing platform for developing cloud-based applications.

For instance Google’s Google File System (GFS), Big Table and Map Reduce infrastructure; Amazon’s S3 storage cloud, Simple DB data cloud and EC2 compute cloud;¹ and the open source Hadoop system,² consisting of the Hadoop Distributed File System (HDFS), Hadoop’s implementation of MapReduce and HBase and implementation of BigTable. The implicit assumption with most high-performance computing system is that the processors are the scarce resource, and hence shared. When processors become available, the data are moved to the processors. To simplify, this is the supercomputing model. An alternative approach is to store the data and to co-locate the computation with the data when possible. To simplify, this is the data centre model.

Cloud computing platforms (GFS/MapReduce/BigTable and Hadoop) that have been developed thus far have been designed with two important restrictions. First, clouds have assumed that all the nodes in the cloud are co-located, i.e. within one data centre, or that there is relatively small bandwidth available between the geographically distributed clusters containing the data. Second, these clouds have assumed that individual inputs and outputs to the cloud are relatively small, although the aggregate data managed and processed is very large. This makes sense since most

clouds to data have targeted Web applications in which large numbers of relatively small Web pages are collected and processed as inputs and outputs consists of search queries that return relatively small lists of relevant pages. Although some e-Science applications have these characteristics, others must ingest relatively large datasets and process them. In addition, queries for certain e-Science applications also result in relatively large datasets being returned.3

Discussing the above issues, this article looks to comprehend the appropriateness of cloud computing in India, bearing in mind that India does not have any devoted regulatory framework to maintain the same. The basis for careful acceptance of cloud computing in India can be credited to jurisdictional issues, inadequate data security, and absence of data protection laws, erasing mechanism, lack of privacy laws poor watch over data handling, inadequate data security, licensing and jurisdictional issues. This paper broadens look for to propose certain systems and events that may be approved to overlay road for more substantial adoption of cloud computing in India.

2. PRIVACY ISSUES: WHAT CAN THE CLOUD PROVIDER DO WITH THE USER DATA

Cloud providers often manage huge amount of personal data from millions of users of cloud service, and the data from one user commingles with the data of other users.4 There was a debate on cloud computing and privacy from a settlement in Author’s Guild, Inc. v. Google Inc.5 The stipulations of the agreement permitted Google to keep on offering copies of books on their cloud-based Google Books platform in return for a stipulated amount to the authors. Although privacy was not the main concern in the settlement, many

public interest organizations were alarmed that the agreement did not acknowledge the security of the privacy of its users.

The issue raised by Consumer Watchdog in 2010 was that the settlement “still contained no restrictions on what data could be gathered, and contained only limited restrictions on how that data cloud be shared”. The settlement agreement did not address whether a user’s reading preferences could be shared with news outlets or governmental units acting without a search warrant. Consumer Watchdog was concerned that the settlement gave Google a monopoly over the book-search and book-subscription markets and at the same time gave it unrestrained authority to share private information about users with outside entities.

A group of objecting class members to the Google settlement, Privacy Authors and Publishers, asserted that the lack of privacy protection in the Google settlement agreement would deter readers from reading and purchasing their works. According to the Privacy Authors if readers were worried that information about their reading habits could be disseminated to the government, divorcing spouses, or other interested third parties, these readers would be less likely to view books on controversial topics. Not surprisingly, the Privacy Authors included several authors who had had penned books on sensitive or controversial subjects.

**JURISDICTION CONFUSION: WHICH LAWS APPLY TO THE DATA IN THE CLOUD?**

The amorphous nature of the collection of servers, applications, and data that makes up “the cloud” lends itself to potential jurisdiction conflicts. The jurisdictional question is an important one because of the display in privacy laws; if a company does not know which jurisdiction its data is subject to,

---


6 Id.
how can it know which laws apply? In the United States, for example, the Patriot Act gives the government broad latitude to intercept suspicions electronic data that comes through the country.\(^7\) “European and Asian companies have expressed concerns about having their data stored on computers in the U.S.A. which fall under the jurisdiction of the USA Patriot Act, allowing the U.S government to access that data very easily.”\(^8\) In the European Union, on the other hand the data protection directive puts stringent standards on the collection of electronic data by the government and by any other entity.\(^9\) Because of these distinctions, it is important that cloud computing or SaaS (Software as a service) agreements specify where the data is physically located and which laws apply.

Yet another statutory hurdle to cloud computing in the United States is the Health Insurance Portability and Accountability Act (“HIPAA”).\(^10\) HIPAA places substantial restrictions on the transfer and disclosure of private health information. For example, entities that are covered by the Act must enter a business associate agreement with cloud providers before the providers can store records containing health information in the cloud.\(^11\) Because of HIPAA’S requirements, it is important for foreign entities to know where their data is located.\(^12\) This knowledge ensures that they can enter the necessary agreements with the cloud provider to avoid liability under HIPAA.\(^13\)

\(^10\) Health Insurance Portability and Accountability Act of 1996.
Cloud computing agreements do not just cause jurisdiction confusion internationally. Privacy Laws also vary from state to state within the United States. For example, a law in Massachusetts requires anyone who holds personal information belonging to a Massachusetts resident to implement a detailed written security program to protect the data. Companies subject to these regulations that want to implement cloud computing must determine whether the cloud provider maintains adequate security measures to protect its electronic data. Because a Massachusetts resident’s data could be commingled with the data of many other users in the cloud, it would be difficult for cloud providers to know which state regulations applied to such providers. With the business world rapidly embracing cloud computing solutions, it is only a matter of time before litigation arises that directly addresses the jurisdictional problems with cloud computing.

3. CONTRIBUTORY LIABILITY FOR INFRINGEMENT

In addition to concerns about violations of privacy and decisions about jurisdiction, cloud providers have another burgeoning problem on their hands: contributory liability. Online auction site and cloud provider eBay recently defended itself against a claim by Tiffany Inc. (“Tiffany”) for contributory trademark infringement. Tiffany alleged that several of eBay’s users were using the site to sell counterfeit Tiffany merchandise with the Tiffany mark and that eBay should be liable for these actions by its users. In Tiffany (NJ) Inc. v. ebay Inc., the district court utilized the Inwood test to determine eBay’s contributory liability, the first time that the Inwood test was applied to an online marketplace. Under Inwood, a service provider is liable for contributory trademark infringement if one of two conditions is met: (1) the provider “intentionally induced another to infringe a

---

16 Tiffany (NJ) Inc. v. ebay Inc., 600 F.3d 93 (2d Cir 2010).
trademark,” or (2) the provider continued to supply its services to a user who it knew or had reason to know was infringing on trademarks. Tiffany asserted that eBay was liable under the second provision because Tiffany brought the infringement to eBay’s attention and eBay certainly knew or should have known that users were selling counterfeit items on the site. The district court determined that eBay’s generalized knowledge of infringement did not trigger the second provision of the Inwood test because eBay did not have knowledge as to specific incidents of infringement.

However, a recent case from the U.S. District Court for the Northern District of California resulted in an opposite decision to that of Tiffany. In August 2009, Louis Vuitton Malletier, S.A. (“Vuitton”) prevailed in an action against internet service provider Akanoc Solutions, Inc. (“Akanoc”) for contributory infringement of Vuitton’s trademarks and copyrights. Akanoc’s services included the rental of server space, IP addresses, and bandwidth to foreign resellers of the same services, who then resold the services to companies which sold counterfeit Vuitton items. Vuitton claimed that the defendants had been placed on notice of the infringing activities many times and had failed to discontinue the provision of services to the offending companies. The court in Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. applied the Inwood test, with the determinative issue being whether Akanoc knew or should have known of the infringement. Ultimately, the jury awarded Vuitton $32.4 million is statutory damages for the contributory infringement.

---

The obvious question becomes: why were the judgments in these two cases so different? Apparently, despite their similarities, the outcomes of these cases of contributory liability for infringement turned largely on the jurisdiction in which the case was heard. The court in Tiffany determined that the warnings that eBay got from Tiffany gave eBay only generalized knowledge of infringement, whereas the court in Louis Vuitton found that Vuitton’s letters to Akanoc were sufficient to find that Akanoc knew or should have known of specific incidents of infringement.21

4. INTEGRATION AND SERVICE LEVEL ISSUES

The data centers of cloud service provider are located in various jurisdictions and all the information of individuals and organizations are spread across the world and need to be integrated. If the integration is not made, it will be a hurdle for individuals and organizations to get full access of their files. It is so often that the infrastructure of a customer is not compatible with the applications provided by the cloud service provider and which in result will have an impact on working of cloud computing and the whole purpose of cloud computing gets defeated in the first place.

From a single service provider, multiple customers can have access to cloud services. The level of service can vary from provider to provider, the organizations have to make sure that the services given to them by a cloud service provider is right on time and the response is quick, this is done because the data centres are located in different jurisdictions and it will be hard for any organization to commit to cloud computing when the services given to them will not be guaranteed.

Cloud computing services are very easily available online and any individual or organization can take up the service by accepting a legal contract offered by the service provider. In most of the cases the contracts favour the service provider instead of securing the interest of the customer for the value he paid for the services offered to him. The scope of negotiation is restricted down to make very little or no changes on the terms and conditions on which the customer affixed his signature agreeing to the contract. The contracts barely acknowledge or give any guarantee of data protection of a customer or also any backup, security, etc. The contracts generally have a saving clause and give a clean chit to service provider for any kind of liability arising out of such situation, wherein any case the customer is at loss and the contract absolutely stays in the favour of the service provider.

5. CLOUD COMPUTING LAWS IN DIFFERENT COUNTRIES

In EU: Directive 95/46/EC of the European Parliament and of the Council of the European Union (of 24th October 1995) - on the protection of individuals with regard to the processing of personal data and on the free movement of such data; applicable to cloud computing as well. Though the directive is very comprehensive, covering as much questions like who is the controller of data, what the scope of authority of sub-processors is, and what happens when data is transferred outside the EU. Cloud computing emphasizes the reduction in the level of direct control over data; while the EU legislation talks volumes about keeping control of data.

In the United States the Act of Stored Communications (Electronic Communications Privacy Act, 1986)

Also, The Health Insurance Probability and Accountability Act, (HIPPA) of 1996 enacted in the United States contains a ‘privacy rule’ which controls, utilize and leakage of Protected Health Information (PHI) and instruct that practical steps be taken to ensure the privacy of communications with individuals. The Financial Privacy Rule of Gramm–Leach–Bliley Act of 1999, compels financial organizations to present each customer with a privacy notice which must describe the data collected about the consumer, where that data is shared, how that data is used, and how that data is protected.

6. LAWS IN INDIA RELATING TO CLOUD COMPUTING

The legal fraternity in India has been in front of a range of complexities in dealing with technological advancements, and the brisk growth of the internet and its influence all over the world. Time and again technology diminishes the necessity for physical communication in the formation of important relationships in legal terms between the parties. Hence, it is to the legal fraternity to settle the code of behavior to be followed by such parties in sustaining such legal relationships.

Until the Information Technology Act, 2000 was enacted, there was no law with respect to the usage of computers, computer systems and computer networks, as well as data and information in an electronic form in India. The primary aim of the Information Technology Act 2000 is to present legal gratitude to e-commerce, which involves the use of electronic means of communication and storage of information, and to facilitate the electronic filing of documents with government agencies. The Act has extra-territorial jurisdiction so it also covers offences committed outside India.

The IT Act deals with a range of computer related works such as digital signatures, electronic governance, electronic records, regulation of certifying authorities, duties of subscribers, cyber regulations, the appellate tribunal, etc., and also offer for legal identification of electronic documents and
transactions, the admissibility of electronic data/evidence in a court of law, penalty for cybercrimes, and the institution of an appellate tribunal and advisory committee for regulating cybercrimes and regulations regarding the maintenance of electronic records.

Nonetheless, the Act also has numerous grey areas, i.e. it does not grant for shield against copyright infringement, defense of domain names, taxation on e-transactions, stamp duty payable and the jurisdictional aspect of e-contracts. However, efforts are being made through a number of amendments to do away with the ambiguities.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules of 2011 were notified by the Government of India, for the protection of sensitive personal data or information of individuals or organisations by the entity who possesses, deals with or handles such data in a computer resource owned, controlled or operated by it. But various provisions of the Rules are not applicable to entities providing services under a contractual obligation with any other entity located extraterritorially, unless such entity ensures the same level of data protection as laid down in the Rules. So a cloud computing service company, before trading with “sensitive personal information” having a link to India, has to make sure to be in observance with the Rules as any non-compliance would invite penalties, and imprisonment in the case of any breach of contractual obligations under the Information Technology Act 2000. Hence, cloud service companies have to make sure that both the rules and terms of contract entered into with the customers are complied with.

24 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, part II section 3(1), R.7 (Apr. 11, 2011).
25 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, part II section 3(1), R. 3 (Apr. 11, 2011).
The IT Act of 2000 enforces a compulsion on a corporate body to provide for a privacy policy and disclosure of information. The entities dealing with any “sensitive personal data or information”, or any other personal information, shall provide for a privacy policy published on its website. The corporate body has to make certain that such personal data is available at all time to its clients.

When it arrives to the security of the information stored, the companies are supposed to make sure that they protect such information by implementing the “Reasonable Security Practices and Procedures”. This states that the International Standard on “Information Technology - Security Techniques - Information Security Management System -Requirements” has been adopted by the government of India. Any corporate body implementing such standards is said to have obeyed with the said act with regard to practical security practices and procedures. The law also requires a complete information security programme, standard information security plans including the managerial, technical, and operational charge of security, and physical actions which are proportionate with the secluded information possessions and which obey with reasonable security exercise and standards.

Rule 6 of the said act sets down the mode in which the data can be revealed to a third party. It asserts that no leakage of any sensitive personal data shall be made without the former approval which has been contractually agreed between companies by the corporate.\textsuperscript{26} No data shall be passed on by the corporate to any third party, unless such third party has acted in accordance with the minimum security criteria’s as specified under the rules. It specifies that government outfits can collect any sensitive information, for the purpose of authentication of identity, or for prevention, detection, investigation, prosecution and punishment of offences.\textsuperscript{27} Nonetheless, any individual who in pursuance of his powers conferred by the Act gains access

\textsuperscript{26} Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, part II section 3(1), R. 6 (Apr. 11, 2011).
to any data and reveals such information without the approval of the person concerned, triggering a wrongful damage to such a person, shall be likely to be proceeded for imprisonment, which may extend to two years, or to a fine, or to both.

One of the foremost loopholes of cloud computing services in India is that there is no precise law prevailing over the possession of data on a cloud. Generally the service providing companies possess the data unless it has been contractually agreed between the parties. This depicts the customer’s information to various perils as the rights of such data are vested with the cloud provider. Under the Information Technology Act of 2000, a cloud service provider is not accountable for any third-party data made available by him, if he shows that such infringement or offence was committed without his awareness or that he has exercised due diligence as may be prescribed by the Government for the prevention of such offence.28

In the Information Technology Act, 2000, amended section 10A has been placed which says that a contract which has been made electronically shall not be regarded to be unenforceable. Yet, there is still elusiveness as to if an electronic contract is to be stamped, as the process of payment of stamp duty as envisaged under the Stamp Act is not possible in cases of electronic contracts unless they are printed.

In particular situations the parties entering into a contract have a choice to prefer the law which shall preside over them in the case of any difference of opinion arising in the future. But this is not the same in all matters. As a result the applicable law and the authority of the court remains a loophole as the contract entered into between the parties lacks clarity on such matters.

28 The Information Technology Act, No. 21 of 2000, INDIA CODE.
7. CONCLUSION

The chief rationale why companies choose cloud computing over any other course of storage is because the information is being stored online, eliminating the risk of data being lost or destroyed. Cloud computing also has many shortcomings which need to be taken care of, for example there are a number of privacy and security issues associated with the storage of data on the internet. Additionally, there is always a danger of losing internet connectivity which could cause interruption in the workflow of a company.

Experts in the field maintain that cloud computing is more safe than the many traditional means of data storage such as hard disks, servers etc., though companies still take the menace of data being stolen by any outsider hacking into the security scheme of the cloud. The foremost ground why companies are not selecting cloud services is the lack of protection or security. Then again, the traditional storage means also present dangers like the servers can also be hacked into by outsiders and hard disks could crash and destroy the stored data.

Coming to the Indian aspect, cloud computing is a new notion and there is no law which exclusively governing it and the law currently lacks clearness. Queries as to the applicable law and jurisdiction still remain unanswered. Nonetheless, companies are substituting from traditional methods of storage to cloud computing because of the cost effectiveness.

The suggestion the authors offer is that cloud computing may not be idyllic for all companies because of the various issues brought about in the article, but it is cost-effective and suitable for global companies to use in order to store data which can be retrieved at any time from any part of the world.