Regulatory Issues in Cloud Computing -An Indian Perspective

Mrs. Gowri Menon, Assistant Professor, Symbiosis Centre for Management Studies, Survey No. 231, Viman Nagar, Pune, Maharashtra, India

ABSTRACT
Cloud computing refers to anything that involves delivering hosted services over the internet. In other words, it refers to the activity undertaken by IT service organizations for delivering computing requirements as a service to a heterogeneous community of end-recipients. All cloud computing models depend heavily on resource and data sharing. This kind of data centre environment permits enterprises to get their applications up and running faster, with easier manageability and little maintenance, and facilitates IT to adjust more swiftly, its IT resources (namely storage, servers and networking) to meet asymmetrical and volatile business requirement. The flip side is that huge concentration of data at one centre makes it more vulnerable to cyber attacks; and the extreme power given to cloud centers to control resources, increases the risk of potential deceitful conduct. The practice seems to be in nascent stages in India. The fact, however, is that, cloud computing is distrusted in India since service providers do not take cloud computing due diligence very seriously.

In light of the above scenario, this paper seeks to understand the suitability of cloud computing in India, considering that India does not have any dedicated regulatory framework to support the same. The reasons for cautious adoption of cloud computing in India can be attributed to lack of privacy laws, absence of data protection laws, inadequate data security, inappropriate data erasing mechanism, poor watch over data handling, licensing and jurisdictional issues; to name a few. This study further seeks to suggest certain mechanisms and measures that may be adopted to pave way for more liberal adoption of cloud computing in India.

Keywords: Cloud computing, regulatory framework, data security, resource sharing, data protection laws in India

General terms
Data Protection, Privacy, legislation, data protection regulation, information security, legal issues, cloud computing in India

Definitions
‘Cloud Computing’ refers to internet based computing that allows organisations to access a pool or network of computing resources that are owned and maintained by a third party via the internet.

‘Personal information’ is any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available within a body corporate, is capable of identifying such person.

‘Sensitive Data’ is defined as personal information that relates to:
1. passwords;
2. financial information such as Bank account or credit card or debit card or other payment instrument details;
3. physical, psychological and mental health condition;
4. sexual orientation;
5. medical records and history;
6. biometric information;
7. any detail relating to (a) – (f) above received by the body corporate for provision of services; or
8. any information relating to (a) – (g) that is received, stored or processed by the body corporate under a lawful contract or otherwise.

‘Body Corporate’ is defined as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. The term ‘body corporate’ is not restricted to a ‘body corporate’ established in India.

‘Provider of Information’ is not defined in the Data Privacy Rules but it is understood to refer to an individual whose Sensitive Data is being collected.

‘Intermediary” is defined as anybody who receives, stores or transmits a particular electronic message on behalf of another person, or who provides any service with respect to that message.

1. INTRODUCTION
Cloud computing is soon becoming the most insidious delivery method for IT services across the public and private sectors in the UK. Benefits such as a wide range of tailor-made solutions and increased efficiency make cloud computing an attractive prospect. Nevertheless, there are some legal implications to consider. These aren’t
necessarily ‘new’ legal issues, and there is no specific ‘cloud computing’ law; rather, this may mean existing legal duties, regulations and considerations have to be restructured to fit the new model. As the cloud computing market stabilises, the risks will become clearer and standards set. The law may, in course of time, be updated where required, to meet the new technological needs. Cloud computing itself is not a new concept; social networking and search engines are examples wherein cloud computing is successfully applied. The salient characteristics of cloud computing are:
- Independence of location on account of the use of remote servers
- Services that are accessed by users on demand through a broadband network.
- These services can include applications, computing power and operating systems, or the general outsourcing of Information and Communications Technology (ICT) processes and services.

India’s business, data and knowledge process outsourcing industries have been growing significantly in the recent years. However, data theft and mishandling of private and personal information have been reported frequently; and these have increased apprehensions about outsourcing to India. India does not have an exclusive data protection law. In the absence of specific legislation, data protection in India is achieved through the enforcement of privacy rights (enforced under the Indian Constitution and Information Technology Act, 2000) and property rights (taken care of by Indian Contract Act, 1872, the Copyright Act, 1957, and the Indian Penal Code, 1860)

2. LITERATURE REVIEW

The concept of cloud computing is understood and applied the world over, and not without shortfalls. Cloud computing has been posing problems especially on the legal front.

Majmudar and Co., International Lawyers, India[1] contend that India needs a law on data protection if it is to sustain investor confidence, especially among foreign entities that send large amounts of data to India for back-office operations. The provision of the Information Technology Act 2000 (IT Act) seeks to protect only Sensitive Data. The Data Privacy Rules refer consistently to ‘sensitive personal data or information’ as the subject of protection, but it must be noted that sensitive data is only a compartment of ‘personal information’.

The Data Privacy Rules do not specify any timeframes for retention of Sensitive Data. The body corporate or Data Processor must not retain the Sensitive Data for longer than is required for the purposes for which the Sensitive Data may lawfully be used. The Central Government has yet to frame rules implementing the retention provision. Therefore, the nature of data that is to be preserved, and duration of retention, is not known.

Research conducted by Orin S. Kerr of Washington University Law School helps to identify with data protection and processing norms in the United States. The study focuses on the enactment of Stored Communications Act, which helps to ensure that no tampering is done with personal data in the hands of any Internet Service Provider (ISP) or vendor.

Previous studies on cloud computing seem to focus its attention either on the issues faced due to manhandling of data by a cloud, or on the criticality of data and the need for protection; or on the current lacunae in the India law with respect to data handling. This paper is an effort to emphasis not only the loopholes in the data protection laws but also an attempt to make constructive suggestions which will make it easier for adoption of cloud computing in India.

3. CLOUD COMPUTING

CHALLENGES

3.1 Overview

Cloud computing, still in its nascent stages in India, is facing several problems/challenges. One of the challenges encountered is that of self-healing. It demands timely back-ups of data in the event of network, application or data storage failure. Yet another major challenge is that of being highly SLA-driven; which permits instances of one application to be replicated on multiple servers. This may cause the cloud to shut down a lower level application, when a priority scheme is defined. Such a challenge when tackled successfully will help to reduce substantially, the power shutdown. The use of hardware by several users simultaneously -known as multi-tenancy - without a thorough understanding of the same, often results in a conflict of interest among users and such a scenario poses yet another major challenge. Virtualization poses another colossal challenge in the field of cloud computing. Various applications being vague on the hardware they use tend to create a conflict of interest among programs created to operate the same. Linear scalability is another tight spot of cloud computing. The cloud should ideally be capable of handling an increase in data processing in a linear proportion, but this is a dream yet to be materialised. Management of data; with the inclusion of distribution, division, and protection of the same; is still a huge challenge.

3.2 Issues in cloud computing

- Location (where is your data; what law governs?)
• Operational (including service levels and security)
• Legislation/Regulatory (including privacy)
• Third-party (contractual limitations on use of cloud)
• Security (with respect to data storage and processing)
• Investigative/Litigation (discovery)
• Risk allocation/risk mitigation/insurance (precautionary and punitive)

3.3 Legal issues
Cloud computing, due to its technical, operational and commercial characteristics, involves a relatively complex data processing relationship: it may not always be easy to distinguish the controller and it may be unclear which national data protection authorities (DPAs) are likely to assert jurisdiction over the data processing operation. To address this, the customer - normally a data controller - will carry out pre-contractual due diligence. On that basis, the parties will try to ensure that the contractual arrangements reflect the responsibilities as accurately as possible. In determining their strategic approach, suppliers and business customers should carefully consider the following key data protection legal issues.

1. Liability: Including India, in many jurisdictions, cloud providers can be held liable for the illegal data they may be hosting. Escape routes bear no liability for services that “consist of” the storage of electronic information under the condition that the provider has ‘no knowledge or awareness’ of its illegal nature and removes or blocks illegal data when it does gain knowledge or become aware of illegal nature. Liability protection does not prevent so-called injunctions, which can be costly and time consuming.

With Indian Investigation agencies, loss of location is likely to cripple cybercrime investigations at a very early stage.

The Budapest Convention on Cybercrime already features a legal principle which overrules location as a legal connecting factor, and surprisingly India is not a Signatory to Convention on Cybercrime.

2. Law: Laws or regulations typically specify who within an enterprise should be held responsible and accountable for data accuracy and security. If you’re collecting and holding HIPAA data, then you must have a security position designated to ensure compliance. The Sarbanes–Oxley Act designates the CFO and CEO to have joint responsibility for the financial data. The Gramm–Leach–Bliley Act is broader, specifying the responsibility for security with the entire board of directors. Less specific is the Federal Trade Commission (FTC), which just requires a specific individual to be accountable for the information security program within a company.

3. Compliance: The intermediary shall observe following due diligence while discharging his duties, namely: —

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary’s computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that, if such hosting reported, then action to be taken in 36 hours

Many contracts impose auditing possibilities that include physical inspection while in reality clouds are geographically decentralized. Where litigation is to be addressed outside one’s own country, it could become prohibitively expensive. Further, the issue of consequences of bankruptcy of the cloud service provider is not addressed adequately.

4. Data Portability: Data Portability can be loosely described as the free flow of people’s personal information across the Internet, within their control. It has now become a standard term in the Internet industry in the context of cloud computing, open standards and privacy. Examples could include, Being able to import all your social network connections, ability to reuse your health records while visiting different doctors, etc.

5. Indemnity: The ISP and other intermediaries disown responsibility for service interruptions or for any damages caused to the data subject (information provider). In such a case, the customer is stranded and cannot look up to the cloud for any sort of indemnification. There are absolutely no measures taken for risk mitigation. Vendor form contracts rarely include any form of indemnification benefitting the provider, but such protection is critical in at least two areas: infringement of third-party intellectual property rights and inappropriate disclosure or data breach, both of which are largely, if not entirely, in the vendor’s sole control, and both of which can be extremely costly to defend and cure.

4. FINDINGS, SUGGESTIONS AND CONCLUSIONS

4.1 Current status – data protection laws in India vis-à-vis other countries

1. 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; is applicable to cloud computing as well. Though the directive is very comprehensive, covering as much as 72 provisions; it fails to answer few important
questions like who is the controller of data, what is the scope of authority of sub-processors, 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.

2. UK: Data Protection Act, 1984 was introduced to provide protection and privacy to personal data of individuals; and Regulation of Investigatory Powers Act, 2000 was introduced to take account of technological change such as the growth of the Internet and strong encryption of data for national security and personal and economic wellbeing.

3. US: Stored Electronic Communications Privacy Act, 1986 - a law that addresses voluntary and compelled disclosure of “stored wire and electronic communications and transactional records” held by third-party internet service providers (ISPs). The Health Insurance Probability and Accountability Act, (HIPPA) of 1996 also enacted in the United States of America includes a ‘privacy rule’ which regulates the use and disclosure of Protected Health Information (PHI) and mandates that reasonable steps be taken to ensure the confidentiality of communications with individuals. The Financial Privacy Rule of Gramm–Leach–Bliley Act of 1999, enacted in the US, requires financial institutions to provide each consumer with a privacy notice which must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected.

4. India: Under the IT Act, 2000, a network service provider or an intermediary is liable for any known misuse of third party information or data; or for not exercising due diligence to prevent the offence. The IT Act covers offences and contraventions committed outside India as well, irrespective of the offender’s nationality, as long as the computer system or network is located in India. Confidentiality obligations are limited to officers or persons having powers under the Act and do not extend to private persons. Further, the officer is not liable to compensate the person damaged by the disclosure. Moreover, most of the penalties are in the range of Rs.200,000 to Rs.500,000, which are very insignificant amounts when compared to the gains that a person may make from the crime.

While the UK Act and the EU Data Protection Directive appear to require that the transferee country provide adequate protection for processing of personal data through domestic legislation, the Data Privacy Rules appear to achieve protection in cases of transfer of Sensitive Data outside India, through a contract at the organisational level.

4.2 Suggestions for better regulation

1. Customised agreements for data - In the short term, cloud services customers and suppliers could seek to legitimise international transfers on the basis of an adapted version of the new model clauses. Compared to the new model clauses, the tailored data processing agreement should not reduce the contractual safeguards, should incorporate the same descriptions of transfers and detailed security measures. This would give room to customers and suppliers to carefully incorporate various clauses, which are contract specific and help them understand implications of breach by either party. However, where there are clauses in such agreement that contradict with those mentioned in the Data Privacy Rules, the latter should prevail.

2. Binding Safe Processor Rules (BSPR) - In the medium to longer term, suppliers can address their customers’ concerns on the basis of BSPR which are a self-regulatory solution for data processors. BSPR are a global code of practice for the data processors’ organisation based on EU adequacy standards and can be tailored to the data protection practices of the cloud supplier. The standards are applied by the cloud supplier/processor to the customer/controller’s data and are uniformly applied across the supplier’s customers and suppliers to carefully incorporate the same descriptions of transfers and detailed security measures. This would give room to customers and suppliers to carefully incorporate the same descriptions of transfers and detailed security measures. This would give room to customers and suppliers to carefully incorporate the same descriptions of transfers and detailed security measures. This would give room to customers and suppliers to carefully incorporate the same descriptions of transfers and detailed security measures.

- process the customer data only in accordance with instructions from the customer, which may be specific instructions or instructions of a general nature.
- unless otherwise requested by the customer, process the customer data only to the extent, and in such manner, as is necessary for the provision of the services.
- implement appropriate technical and organisational measures. The cloud services contract should also include additional data protection and security clauses which deal with all or some of the following matters: reliability and training of supplier personnel, management of security downtime and breach issues backed up by SLAs, breach notifications, audit rights, secure management and transfer of data on termination, data protection indemnities, regular reviews of the data processing operations, mitigation and management of reputational and brand damage, mitigating risk from mandatory disclosure requests, notification of and assistance with Subject Access Requests.

www.borjournals.com  Blue Ocean Research Journals  21
3. Adequate Penal Measures - Where the law of stipulates certain precautions to be taken by the ISP, vendor and intermediary with respect to data storage, transfer and processing, it fails to enumerate any stringent penal action against those who violate. The punitive measures and especially the fines, defined are too meager to ensure proper protection of data. Personal and sensitive data have to be maintained with utmost confidentiality; and the trust of the information provider must be safeguarded. Where highly sensitive data is being handled, the law may also suggest an imprisonment term (depending on the gravity of the crime) in addition to the fine prescribed. For repeated contravention, the licenses of service providers may be suspended or cancelled.

4.3 Conclusion
Cloud industry is immature and growing rapidly. New players will rapidly emerge to fill new market niches. Consolidation of the industry at some point will become inevitable. Big players will create standards for security and governance. The new models proposed will become disruptive to the existing models and IT practices prevalent.

In this background we have to analyse the use of cloud computing in India. Cloud computing in India cannot succeed till we have trust in the service provider. We cannot trust a service provider who can be forced to disclose even the most sensitive information and data without a court order. In India a mere order from the Indian government or its agencies is enough for the service provider to share sensitive information. There is no judicial scrutiny of a warrant that is absolutely required in these circumstances. So one never make sure of what government agencies are looking at and what information they are taking from the service provider. Any business model must essentially balance profit motives and risks associated with the business.

Till now the legal opinion is vehemently against the use of cloud computing in governmental departments and for governmental projects. Without a conducive legal framework, user’s data in India is not safe.

On 11 April 2011, the Indian Ministry of Communications and Technology published rules implementing certain provisions of the Information Technology (Amendment) Act 2008 dealing with: (a) protection of sensitive personal data: security practices and procedures that must be followed by organisations dealing with sensitive personal data (Data Privacy Rules); (b) due diligence to be observed by intermediaries; and (c) guidelines for cybercafes. The last data protection bill, The Personal Data Protection Bill 2006, introduced in Parliament on 8 December 2006, has now lapsed. On 18 October 2010, the Department of Personnel and Training, Government of India, published an approach paper for legislation on privacy. More recently, there have been news reports suggesting that a ‘Right to Privacy’ Bill will be introduced in Parliament in the upcoming monsoon session. From the extracts of the Bill reproduced in the newspapers, it appears that it will be a data protection and privacy law. In the wake of all these developments, India will have data protection legislation dealing with protection of sensitive personal data. This development could, to some extent work in favour of India, especially when the British banks appear to be moving their call centres back to the UK.

Cloud computing, through its applications, platforms, and services, is already affecting the ways that people and businesses interact with and use computers and the Internet. The viability of the technology and its growing acceptance by consumers and service providers offer powerful evidence that a lasting technological and societal shift is underway. As a result, courts will need to determine how existing laws may or may not protect electronic communications and content in this new computing model.

5. REFERENCES