INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Cloud computing technology and legal challenges

Sreevidya KV
sreevidyamattur@gmail.com
School of Legal Studies CMR University, Bengaluru, Karnataka

ABSTRACT

Law influences society and society influence the law making procedure. This symbiotic relationship is unavoidable. Any change in society has an impact on the legal process. Technology is no exception to it. Technology is today's lifeline. Technology has become part and parcel of everyone's daily life. Law and technology are becoming two balances of the scale by which human behavior is controlled. It is interesting to observe how these variants, law, and technology interact with each other and what effect is caused in society by such interaction. With the latest technological development in cloud computing, an opportunity has been created for researchers to investigate the action and reaction formula of law and technology on society. Cloud computing technology is very popular in the present days. It is the new technology that is looked upon by industries. Nowadays cloud computing is gaining popularity amongst business community because of its features like low cost, easy maintenance, scalability etc. Indian business is also adapting to cloud computing very rapidly. India is outsourcing in the field of cloud computing services. This increase in the adaptation of cloud computing technology is not without risks, the advantage of cloud computing technology comes with many disadvantages. As cloud computing technology transcends boundaries it has resulted in the spreading of legal problems like violation of privacy of cloud customers, access, and safety in online handling of data, copyright issues of the data stored in cloud and questions of jurisdiction. If regulatory framework with regard to the above-stated issues is not clear, the confidence of stakeholders will not be boosted. Additionally, any breach of privacy, data loss or data theft, on cloud causes catastrophic effects. The purpose of this research is to find out the necessity of regulating cloud computing, to inquire about the available methods of cloud regulation and also to find out suitable methods of cloud regulation for India.

Keywords— *Cloud computing technology, Privacy violation, Data theft, Data misuse, Legislative measures*

1. INTRODUCTION

Cloud computing technology is the utilization of computing resources like hardware and software that are conveyed as a service over a network, typically internet.[1] Cloud computing is essentially a combination of prevailing technologies that are organized for the advantage of customers. As the available technologies and the number of ways in which it can be combined both are numerous, a rigid and uniform definition of cloud computing is difficult to formulate. Nevertheless, it is very essential to provide a definition. Presently, an effective definition of cloud computing that can be given is, that, cloud computing is, "any type of computing that can be completed remotely through the internet as an alternative of doing it locally". This kind of all-encompassing description is also inevitable; because of the fact that cloud computing is a developing knowledge.[2]

To understand in easy language, cloud computing is a system of operating software, hardware, and infrastructure of cloud, rather than in house building and maintaining it. It is the outsourcing of computer product and /or services to the cloud service provider.[3] The five main characteristics of cloud computing, according to NIST is first, need-based provisioning of service, secondly extensive network log on, thirdly, assembling of sources, fourth speedy flexibility or scalability, and fifth calculated package.[4] The designation, cloud computing was stirred by the cloud representation that is frequently employed to symbolize the internet, in flow charts and graphs.[5]

2. TYPES

According to the function performed by clouds they can be classified as, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). SaaS offers comprehensive applications on request. For example, word processors can be held distantly, sparing individuals from diverse dwellings of fixing the software on their systems. In SaaS software is provisioned. PaaS is the facility in which whole operating system or the platform is delivered to consumers through the cloud. IaaS is a complete simulated computer accessible over cloud wherein elementary computing amenities such as handling and loading of data could be done despite one's own data center or server. In a sense in this service of IaaS infrastructure is provided.

Clouds can also be categorized on the basis of their nature like the public, private and hybrid clouds. Public clouds like Amazon EC2, Google Drive etc., can be opened by the general public. Private clouds, on the other hand, are devised and custom-made to

the wants of a particular business or a person and are exclusively available to them. Hybrid clouds are essentially a combination of the attributes of public and private clouds.[6]

3. BENEFITS

One human resource related benefit of the cloud is that companies can allow people to work from home who do not want to take long hours to commute or keep young children in day-care. The technical benefits are that if any upgrade or change is required in software it is easier in the cloud as compared to one to one service model where the same has to be carried out using downloadable patches and upgrades. Financial benefit is that customers of cloud service pay as they use. Chief marketing fact for cloud computing is its less price. Management benefits include freedom from devices and locations. Consumers can contact their machines without worrying as to where they are situated or what device they are using.

Cloud services are increasingly used in the healthcare sector and agriculture. Identification of patient's everyday actions is essential to deliver vigorous healthcare aids. Background facts of patients can help in improved amenities, assistance proposals, and modification in the conduct of the patient. Cloud computing can be used for health observation by screening human health and communicating the report to physicians. For example, a fever antenna can be fixed in the patient staying room to supervise temperature and an alarm will be raised when the temperature exceeds or drops lower than the normal room temperature. In case of natural calamities of fire or water, the company's data in the cloud will be more secure. Provisions for data backup will be made in the cloud.[7] Benefits of cloud computing include access from anywhere, fewer hardware costs etc. The required minimum terminal would comprise a monitor and input devices like keyboard, mouse and internet connection. A corporation can cut costs on the license for various software, their maintenance, and up-gradation etc. Need for physical space is also minimized.[8]

4. CONCERNS

Privacy protection and regulation are the two core anxieties outstretched by cloud computing. There is always a compromise between safety and price. This is intensified due to the community environment of the cloud. Cybercrime is a huge problem. In July 2013, central prosecutors in the United States charged five people responsible for a theft of 160 million credit card numbers, which they resold for $10 apiece. The victimized companies include J.C. Penny, JetBlue Airways etc. Total loss estimated in the above theft was $300 million. Though this is the highest scheme prosecuted in the United States for data theft, a thousand others have been verified in past nine years. This is despite the fact that, the majority of U.S. state notified laws to have safe harbor principle, wherein bodies that suffer a violation can opt out and not convey it thereby maintaining their reputation. In the Wall Street Journal of March 2012, Shawn Henry, a former top cyber policeman of FBI said that with the present technology and behavior of people it is very difficult to safeguard, privacy and data security in cyberspace. Cybercriminals always persist to remain one step forward than safekeeping professionals. [9]

Hacking is prevalent in many sectors like business, financial, education, government, and healthcare and also in non-profits sectors. It is both internal and external. PRCH, Verizon Business, ITRC etc. organizations have come out with high statistics of data theft and breach.[10] Before moving the business to cloud careful attention has to be given to trade secrets, which is to be placed on the cloud. Trade secrets are only protected by the fact that they are secret and protection is forever lost once it is disclosed. Whether the cloud provider has encryption facilities or will the cloud service provider submit for security audits has to be investigated.[11]

There is no accuracy as to who is accountable for safety inside the cloud. Buyers trust cloud suppliers to deliver complete safety, secrecy, admission limits and accountability. It is reasonably presumed that cloud computing corporations are the one who to take care of data confidentiality and safety. There are instances where this perception has gone wrong. For illustration, CloudFlare in recent times succeeded in discharging itself from the expected duties when a hacking group named LulzSec took up CloudFlare as their hosting. CloudFlare remained unbeaten in showing that they are unaccountable for the activities of LulzSec.[12]

Clouds particularly public clouds have issues with respect to jurisdiction. Examples of such issues with jurisdiction are; where the cloud is situated? Which country's law is applicable to it? Etc. These complications are worsened because cloud providers can manipulate the storing of the data throughout the globe according to their conveniences. They, save duplicates of documents simultaneously in diverse servers hosted in distinct places. It is common for a single data to have duplicates in quite a few territories all having different rules and guidelines.

Cloud service providers also try to escape liability by following the principle of Mare Liberum i.e. principle of high seas. Numerous cloud suppliers house their servers in uncluttered seas and air to escape government rules. Google Navy and Pirate Bay Drones use this open window. Suppliers detach the cloud servers from the territory and make it free from the control of the territory's ruling. Google Navy is exploiting hydropower for powering their servers and taking benefit of the fact that United States laws will no further effect on their servers. The Pirate Bay Drones is noteworthy because their file allocation network steadily challenges orders of numerous republics. Lodging their servers on drones and putting their actions outside of the authority of territory-founded regulations.[13]

5. PRIVACY

The term privacy originated from the Latin word Privatus, which means separate from rest. It may be defined as the competence of a person or class to seclude them or communication about themselves and thereby disclose them optionally. Privacy can be known as a right of a person to choose who can retrieve data, when they can use the information, what files they can have admission to.[14] Classical definition of privacy is attributed to United States judge Brandeis. In Olmstead *v* United States[15] then Supreme Court judge Brandeis articulated the general constitutional right "to be let alone" as the most comprehensive and valued right of civilized people. Over a period of years, a number of other definitions are formulated.[16]

European Convention on Human Rights was put into force in 1953. In its preamble, signatory states reaffirmed their profound belief that peace in the world can be best maintained by the observance of effective political democracy and human rights. Privacy is known worldwide as Human Rights. It has diverse dimensions like confidentiality of individual, secrecy of private conduct, concealment of individual communication and secrecy of private information. Article 8 of European Convention on Human Rights provides that all people have right to regard, for his personal and domestic existence, his residence and his communication.[17]

5.1 The rise in Privacy violation

With introduction and developments in the latest technology, it is becoming very difficult to maintain privacy. Loss or theft of data personal or credit card related can create damage to the individual as well as to the nation as a whole. For instance, from generating an e-mail account to start an electronic finance account we document our private data, commonly in our daily life. The given material should be used for the purpose to which it is gathered. Conversely, the reality is that this data is additionally handled, conveyed then abused for unlicensed reasons with no authorization from data proprietor.[18]

One of the tools for data protection is the technology which created it. Nevertheless, technology is neither full proof nor sufficient. Legal intervention and management become essential in this situation. Cloud computing technology has also experienced the same throughout the globe. An investigation on the response of European Union and the United States in the matter of privacy and data protection reveals that the United Kingdom has a common law which governs all acts including the formation of internet contracts. However, the system in the United States is different. Each individual American State has different laws, although federal law overlay.[19]

It is the opinion held by many legislators that cyberspace is a complex area. The law regulating it must be technically complex. Basic questions like will this law persuade the cyberspace, actor? Will the actor respect the law-making authority? Help legislators, as starting points of legislation.[20] Time has ripened for regulating cloud services. Data exchange being international, protection through national regimes proves not sufficient. Time for India has arrived to lead the change.

5.2 Efforts in India

Indian Constitution under Article 21, Part III, provides for protection of life and personal liberty. No person will be divested of his life or personal liberty except under a process recognized by rule of law.[21] Under Article 21 personal liberty, includes the right to privacy. Hence privacy is measured as one among fundamental rights and constitutional remedies are available for its violation.[22] Sufficiency of this remedy is also uncertain since the case of Mr. X *v* Hospital Z.[23] Apart from Article 21of Indian Constitution, there are very few other laws which relate to the problem of privacy violations viz., Information Technology Act 2000, Information Technology (Amendment) Act 2008, Consumer Protection Act 1986, Indian Penal Code, Indian Contract Act 1872, Indian Copyright Act, Indian Telegraph Act and Specific Relief Act 1963 etc. Protection of privacy under these acts is insignificant and not suitable to a cloud environment.

For example, section 43-A of Information Technology Act, 2000, provides that, where an organization owning, trading or managing any delicate private files or records inside a computer reserve is neglectful around applying and sustaining realistic safety rehearses or procedures as a consequence of which, it instigates unjust damage or unjust advantage to any individual, such organization will be legally responsible to reimburse the costs by making payment to the individual aggrieved. According to Section 77 of Information Technology Act, 2000, not any recompense is given, fine levied or seizure below this Act will constrain the decision of any other benefit or penalty under another rule presently in force.[24] These provisions relate to a computer reserve and not to cloud.

Even though the Information Technology (Amendment) Act 2008 has made changes regarding the provisions of protecting individual data, it does not define personal information. This has paved the way to a different interpretation.[25] The other problem is to have proper protection for the data that is outsourced from Indian jurisdiction. Data, outsourced into India is protected u/43A and 72 A of Information Technology (Amendment) Act 2008, in a piece meal manner.[26] Hence, India is lacking in legal measures aimed at data shielding and confidentiality.

One noteworthy case law from Delhi State Consumer Disputes Redressal Commission is Cellular Operators Association *v* Nivedita Sharma. The commission levied a total sum of Rs.75 lakhs as penalty on Airtel, Cellular Operators Association of India, ICICI Bank, and American Express Bank, on a complaint of the customer for nuisance. This harassment was caused by unwanted marketing communications through voice calls and text messages.[27] In 1997, Supreme Court of India instructed Reserve Bank of India to appoint an organization to execute methods to lessen unsought calls for the reason that such calls violate the fundamental right of right to privacy.[28] Companies with billions and trillions of turnovers per year will be hard hit by these decisions. They continue to violate the privacy rights of individuals, for the profit at stake is very huge. The Aadhaar Bill which was also opposed in Lok Sabha on the ground of violation of privacy rights was moved and passed as a money bill.[29]

To understand the adequacy of data and privacy protection under Indian Copyright Act, Indian Penal Code, Indian Contract Act 1872, the following points are considered. Under the Indian copyright law, there is no specific provision for privacy and data protection in the cloud. There are many issues related to copyright in databases like ownership of copyright, placement of copyright notice etc. which needs specific answers.[30]

Contractual remedies for privacy and data protection in the cloud is also not adequate for the following reasons. Long-established contracts and licensing agreements do not offer passable legal recourse and solution for data and privacy protection in the cloud environment.[31]India also lacks market specific laws like Health Insurance Portability and Accountability Act (HIPAA).[32]

Other modes of remedy are available under the private liability of tort and Indian penal code for privacy and data protection. These remedies have very limited and specific application in cases of defamation, forgery etc. There is a need for a comprehensive and holistic approach to privacy and data protection in the cloud.

5.3 What needs to be done?

Currently, in India, there is no authorized planning, in line with European Union directive, OECD guidelines or safe harbor principles, for data defense agency, the merit of documents and files transparency etc. to appropriately tackle and cover data protection concerns.[33]

The issues of concern include:

(i) No comprehensive law on protection of personal information.
(ii) There is no sorting of information into community material, confidential data and then sensitive material.
(iii) No official structure that groups around proprietorship of personal plus sensitive knowledge.
(iv) No certified process of generating, treating, conveying and warehousing of data.
(v) Lack of recommendations on data quality, proportionality and data transparency.
(vi) No agenda on cross-country movement of data.[34]

6. JUDICIARY

India acquired its first demonstrative e-court in Ahmedabad. E-courts need to arrange for safety and confidentiality of electronic filings.

7. ADMINISTRATION

E-Governance has established a novel aspect in the direction of growth and globalization. The tasks related to e-governance have increased, due to the hefty loading of private and vulnerable data. The aim of government must include plans like

1. Creating a union chief privacy officer
2. Installing chief privacy officers in all major departments
3. Ensuring that data mining techniques are addressed by the Privacy Act
4. Strengthening and standardizing privacy notices including privacy impact assessments, complaint processing in case of breach of privacy.[35]

8. LEGAL PROFESSION

As the whole world is moving in the direction of adaptation of cloud computing technology, the legal profession is also working in the same path. Attorneys should take proper care of confidentiality risks while storing their client-related information in the cloud. Many U.S. states have rules and guidelines for attorneys to ensure security measures in the cloud. For example, Ohio rules of professional ethics, California and Arizona state bar rules, Iowa state bar regulation, the north California guidance, Pennsylvania bar association guidelines, Massachusetts rules of conduct etc. provides for standard of reasonable care, use of SaaS application in cloud and other security measures to be followed by attorneys before adopting cloud computing technology in their profession.[36]

8.1 Role of Advocacy Groups

Advocacy groups are defined as organized groups of individuals with a common social goal, for example, promoting gay rights or protecting environmental quality etc. Advocacy groups have played a pivotal role in promoting, the diffusion of technologies. There are two channels for working advocacy groups. First, they can lobby policy makers to create a proper legal environment for use of technology. Second, advocacy groups can induce end users to adopt new technologies. If governments fail to enact policies, that allow technology diffusion, then advocacy groups can create schemes that increase end users' adaptation of new technologies. One key function that advocacy groups can also perform is to provide information about people's policy preferences to the government.[37]

8.2 Role of Service Providers

Privacy protection and deceit of data are the two greatest safety concerns on the cloud. From a consumer's point of view trusting upon service provider alone for his outsourced data is not very encouraging. Data accessibility and better privacy may be attained by distributing the consumer's data block into data pieces and allocating them amongst the existing service providers in such a way that, the maximum number of service providers can participate in the effective recovery of the entire data block. For example, a consumer can split his data amongst numerous service providers present on the cloud, according to his budget. This restrains the likelihood of a service provider mistreating the customers' data or breaking through the privacy of data.[38]

To avoid risks or to mitigate loss, cloud providers may try to ensure their risks. The risk involved is huge, cyber insurers and reinsurers will not wish to take such risk. The cloud-computing client must shoulder the burden of self-protection, to escape from liability to its customers, resulting from a cloud vendor's security breach. Choosing a cloud-computing vendor carefully and engaging a broker who has special expertise in cyber insurance can be few precautions.[39]

9. CONTRACTUAL REMEDY

It will naturally take time to finalize any regulation on the cloud by the government but industry cannot afford to sit idle till this happens hence a proper contract management will lead to better regulation. Industry standards in contract management in India could be as following;

Data ownership has to be precisely mentioned in the service providing contract. In case of termination of contract, ownership of data lies with whom, vendor's duty in case of a government subpoena, force majeure clause, escrow agreements, data encryption,

fixing the remedy for infringement of IPR, fixing damages for breach, warranty and indemnity etc. provisions must be specifically stated and not left for assumptions. The procedure for appointment of outside auditors and their access to data should be properly mentioned in the cloud service agreement.[40]

10. ALTERNATIVE REMEDY

10.1 Online Dispute Resolution

Online transactions are increasing greatly, along with it, online crimes and mischiefs are also on raise. It is very important to have an amicable clearance of problems so that expensive lawsuits can be minimized. Hence there is a need for institutional setup, similar to the alternative dispute resolution. In cyberspace, it can be called as online dispute resolution. There are procedures established under Cyber Regulatory Appellant Tribunal Rules, 2000 for cybercrimes in India. Online dispute resolution can boost the stakeholders' morale by providing alternative legal remedy.[41]

10.2 Standardization

As disagreements persist with respect to applicable laws in the cloud and the fact that technology has capabilities to cross-borders, at present cyber rules pertaining to clouds are employed on a case-to-case basis. This prevents one particular country's law from being appropriate in every case. One method of resolving the problem of uncertainty is to generate global standards in matters of cloud computing technology. However, this demands a positive collaboration between various nations and organizations to create uniform standards in cloud regulation.

10.3 Grotius's Mare Liberum

Suggestion for resolving jurisdictional issues in the cloud can be obtained from Grotius's Mare Liberum.[42] The problem of jurisdiction in case of cloud computing arises due to the efforts to lay down the law for a land-less technology by means of rules founded on land. It is better to accept that a superior methodology will be to utilize the concept of free seas that initially arose in the compositions of Hugo Grotius. The vital element in Grotius' Mare Liberum is that the terrestrial is collective but what is required is proprietorship since it is inadequate and depreciable. On the other hand, the marine is so massive in extent plus unfeasible to cover, that there is no necessity for proprietorship. Cloud is seamless similar to sea because it is equally inexhaustible and cannot be demarcated besides it is not exposed to devaluation. Cloud can be regulated by laws which are parallel to laws of seas.[43]

On the other hand, more, appropriate suggestion lies in legal protection for the cloud environment. In order to propose legal protection for a cloud environment, certain basic assumptions are necessary.

(i) The first assumption is that, extra territorial application of cloud regulation, of each nation. This assumption is based on the Lotus case decided by the International Court of Justice.[44] The reason for the decision is that unless such extra territorial application is forbidden by express treaty or law extra territorial application is justified.

(ii) The second assumption is that, whatever law that is supposed to be extra territorially administered, be public international law and not private international law. Cloud computing involves both private and public international laws. This assumption of public international law being applied is based on the principle that for questions relating to privacy laws such as in contract if parties do not provide in contract, as to which law will apply, the public international law in this regard would apply.

(iii) The third assumption is reasonableness of the application of such law. Only in cases where the extraterritorial application of the public international law is reasonable, it should be applied. The subjective and objective principles of territorial extension of jurisdiction are to be considered. For example, corporate nationality has different interpretations, which law to be applied? Requires clarifications at international level based on the reasonableness of the application of each law.[45]

11. CONCLUSION

Apart from internal and external sovereignty with cloud computing data sovereignty is emerging. This means that data should be subject to the laws of the nations in which it is created and stored. Any legal framework purporting to police cloud must refrain from excessive regulation and permit a space for the private sector. The private sector can be innovative in developing approaches to cloud governance and the creation of flexible norms to protect the cloud.

Regulating the cloud is one thing and regulating the rights and duties of cloud users is another thing.[46] While the former puts control on the expansion of cloud the later will not. Therefore the legal regulation of cloud in India has to aim at:

(i) Keeping direct governance and regulation of the cloud to a minimum. Otherwise, the development of technology is hampered or law will be outdated by technology very soon.

(ii) Using and strengthening existing legal frameworks as a backdrop for the policing of the cloud.

(iii) Permitting private actors to create norms and customs to police the cloud, especially through the use of tort and contract theories of liability and

(iv) Avoidance of enacting legislation that would have the effect of mandating that data centres be located in specific geographic locations.

(v) Bring a new legislation for cloud governance in the above context.

International cooperation becomes all more important in the enforcement of cloud regulations. This cooperation may manifest itself in many forms in international organizations such as UN, WTO etc. or a whole new organization may be formed to give minimum standards for cloud computing and to keep a constant check on the changing technology and division of cloud jurisdiction.[47] Any regulation set forth to govern the cloud must be visionary, recognizing its unique features and making all efforts to construct governance frameworks that will not unduly constrain the cloud. For better or for worse, regulations enacted now will set the tone for the cloud's future development.[48]

Finally, it is suggested that changes are required in laws of India to meet the requirements of cloud technology. A hacker of cloud can no more be treated the same as a hacker of a personal computer. Hence there is an immediate need for legislation to regulate the cloud. Care is essential to see that such regulation will not choke the technology, but boosts the confidence of all stakeholders and will be strict on mischief-doers and indifferent vendors. A proper synthesis of the European Union and the United States laws is what India needs at present. Further research can be done as to how this synthesis can be achieved.

12. REFERENCES

[1] Rani Srivastava & Shekhar Gupta, Cloud Computing: A Revolution in Communication, 2(5) IJCSMC 180– 83 (2013) available at http://www.ijcsmc.com (last visited Dec. 5, 2013).
[2] Xath Cruz, Cloud Computing, and its Legal Implications, CT, Dec 3, 2012, available at http://cloudtimes.org/2012/12/03/cloud-computing-and-its-legal-implications/ (last visited Jan. 16, 2014).
[3] Bhayal, S., A Study of Security in Cloud Computing, Pro Quest Dissertations and Theses, 67 (2011), available at http://search.proquest.com/docview/904586862?accountid=38885. (904586862) (last visited Aug. 07, 2013).
[4] Milligan, R. B., & Salinas, D. J., Keeping Trade Secrets in Social Media and Cloud Computing, 19(4) The IP Litigator 9, 9-17 (2013) available at http://search.proquest.com/docview/1416187998?accountid=38885 (last visited Aug. 07, 2013).
[5] Sagar B.Jadhav et al., Review of Cloud Computing and its Application, 2(1) IJARCET 1323, 1323-2278 (2013) available at http://www.doaj.org/ (last visited Dec. 5, 2013).
[6] Xath Cruz, supra note 2.
[7] Sagar B.Jadhav et al., supra note 5.
[8] Working Group on Information Security, Electronic Banking, Technology Risk management and Cyber Frauds, Report and Recommendations, Reserve Bank of India, Mumbai (2011) available at http://www.manupatrafast.in/pers/Personalized.aspx (last visited Dec.06, 2013).
[9] Xath Cruz, supra note 2.
[10] Robert. E. Holtfreter, Will Hackers Win the Battle? Strategic Finance, Jan. 2014 at 28 available at www.strategicfinancemag.com and www.imanet.org.
[11] Deciding between Patent or Trade Secret Protection, available at http://download.springer.com/static/pdf/110/chp%253A10.1007%252F978-1-4614-7912 (last visited Oct. 03, 2013).
[12] Xath Cruz, supra note 2.
[13] http://www.legalserviceindia.com/articles/art222.htm. 277 U.S. 438, 48S. ct.564, 72 L.Ed.944 (1928).
[14] http://www.encyclopedia.com/ (last visited Jun. 7, 2015).
[15] www.echr.coe.int/Documents/Convention_ENG.pdf.
[16] Shrikant Ardhapurkar, et. al., Privacy and Data Protection in Cyberspace in Indian Environment, 2(5) IJEST 942, 942-51 (2010) available at http://www.ijest.info/docs/IJEST10-02-05-136.pdf (last visited Oct. 03, 2013).
[17] Rachel Burnett & Paul Klinger, Drafting & Negotiating Computer Contracts 30-52 (Tottel Publishing).
[18] Chris Reed, Making Laws for Cyberspace 221 &229 (Oxford University Press 2012).
[19] Maneka Gandhi v UOI AIR 1978 SC 597
[20] http://lawmin.nic.in/coi/coiason29july08.pdf.
[21] (1998) 8 SCC 296
[22] Nayan Joshi, Electronic Evidence, 65 (Kamal Publishers 2011).
[23] R Ananthapur, India's New Data Protection Legislation, 8 (2) SCRIPT (ed. 192 2011) available at http://www.law.ed.ac.uk/ahrc/script-ed/vol8-2/ananthapur.asp (last visited Jul. 07, 2013).
[24] Sharad Vadehra Kan & Krishme, Data Protection and the IT Act India, Global Advertising Lawyers Alliance (2013) available at http://www.gala- marketlaw.com (last visited Jul. 27, 2013).
[25] (2011) 14 SCC 337 also available at http://www indiakanoon.org/doc/125045408 (last visited April. 13, 2016).
[26] Shrikant Ardhapurkar, et. al. supra note 18.
[27] Venkitesh Ramakrishna and T.K. Rajalakshmi, Dubious tactics, FRONTLINE, April. 15, 2016 at 16-22
[28] John T. Soma & Jay Batson, The Legal Environment of Commercial Database Administration, 27(3) Jurimetrics, 297, 297-315 (1987) available at http://www.jstor.org/stable/29762021 (last visited Aug. 20, 2013).
[29] Kerr, J., & Teng, K, Cloud computing: Legal and privacy issues, JLICB 1, 1-11 (2012) available at
[30] http://search.proquest.com/docview/1017672586?accountid=38885 (last visited Aug. 07, 2013).
[31] Vic (J.R.) Winkler, Cloud Computing: Legal and Regulatory Issues available at http://technet.microsoft.com/en-us/magazine/hh994647.aspx (last visited Jan. 16, 2014).
[32] EU Directives, available at http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm and OECD Guidelines, available at http://www.oecd.org/dataoecd/56/36/1922428.pdf.
[33] Shrikant Ardhapurkar, et. al., supra note 17.
[34] Vir Singh, Under Pressure, India Mulls Steps to Protect Privacy, available at http://spectrum.ieee.org/telecom/security/under-pressure-indiamulls-steps-to-protect-privacy.
[35] Meghan C. Lewallen, Cloud Computing: A Lawyer's Ethical Duty to Act With Reasonable Care When Storing Client Confidences in the Cloud, 60 Clev. St. L. Rev.1133 2012, 2012-13 available at http://heinonline.org (last visited Dec. 04, 2013).
[36] Sung Eun Kim & Johannes Urpelainen, When and how can Advocacy Groups Promote New Technologies? Conditions and Strategies for Effectiveness, 33 PPJ, 259, 259-87(2013) (discussing the relationship between advocacy groups and promotion of new technology based on game-theory analysis).
[37] Thota Reshma Kishore, et. al., Client and Data Confidentiality in Cloud Computing Using Fragmentation Method, 3(2) IJSCE 2231, 2231-2307 (2013) available at http://www.ijsce.org/attachments/File/v3i2/B1537053213.pdf (last visited Oct. 03, 2013).
[38] David E. Wood, The Unthinkable Risks of the Cloud, CFO.com Aug. 27, 2013, 08:00 PM GMT at 1&2 available at http://www3.cfo.com/Image, (last visited Dec.06, 2013).

[39] Patrick Gray, Legal Issues to Consider with Cloud Computing, Tec Republic Blog (Mar. 5, 2013 12:15 am PST) available at http://www.techrepublic.com/blog/tech-decision-maker/legal-issues-to-consider-with-cloud-computing/8161/# (last visited Jan. 16, 2014).
[40] S.K. Verma & Raman Mittal, Legal Dimension of Cyberspace 309 & 367 (The Indian Law Institute 2004).
[41] Dmitry Belyavsky, Russian translation, The International Law of sea, 8&9 (Progress Publisher Moscow 1988)
[42] Xath Cruz, supra note 2.
[43] (1927) P.C.I.J. Series A. No.10
[44] Vineeth Narayanan, Harnessing the Cloud: International Law Implications of Cloud-Computing, 12 Chi. J. Int'l L. 783 2011, 2011-12, available at http://heinonline.org (last visited Dec. 04, 2013).
[45] Private Regulatory Scheme for Policing Cloud Computing 2013 U. Ill J.L.Tech.&Pol'y141 (2013) available at http://heinonline.org (last visited Dec. 04,
[46] 2013).
[47] Vineeth Narayanan, supra note 45.
[48] Carol M Celestine, supra note 46.

BIOGRAPHY

Sreevidya KV
Assistant Professor
School of Legal Studies CMR University, Bengaluru, Karnataka

