DATA IN THE CLOUDS, REGULATION AND PROTECTION: INDIAN SCENARIO

Gauri Shrikhande

Army Institute of Law, Mohali

INTRODUCTION

INSTITUTION OF CLOUD COMPUTING: GROSCH'S LAW

The development of cloud computing is as old as computers itself.[1] For almost two decades, this theory was endowed and enshrined with the feature of law of nature in a concept which was called "Grosch's Law." Herbert Grosch developed this "law" more than 60 years ago based on an assumption that computing increased by the square of its cost.[2] Grosch expressed his theory as follows: "I believe that there is a fundamental rule…giving added economy only as the square root of the increase in speed; that is to do a calculation ten times as cheaply you must do it one hundred times as fast."[3]

This interpretation has been made to indicate that the natural technological evolution would result in "supercomputing" as a standard and, fundamentally, that resettlement to centralized computing will take place because of the need to influence economies of scale coupled with the need to invest in massive data processing centres. As with any good thinker who is ahead of his time, Mr. Grosch was partially wrong, and partially right, his law held rein for nearly three decades.[4]The one's who felt that Grosch was wrong wanted

[1] In 1944, the first large-scale automatic digital computer began operation. Built by IBM and Harvard professor Howard Aiken, the Mark I was 55 feet long and eight feet high. The World Almanac and Book of Facts (Ken Park ed., 2002).

[2] Patrick S. Ryan, "Wireless Communications and Computing at a Crossroads: New Paradigms and Their Impact on Theories Governing the Public's Right to Spectrum Access," 240 J. on Telecomm. & High Tech. L. 3, at 247.

[3] Young M. Kang et al., "Comments on Grosch's Law Re-Visited: CPU Power and the Cost of Computation," 29 Comm. ACM 779 (1986)

[4] In the 1960s and 1970s, Grosch's law was still highly regarded by scientists and policy analysts, and respected papers continued to espouse his centralized computing "law." While some challenged his theories, the scientific community on the whole still had great faith in them. See e.g ., Martin B. Solomon, Jr., "Economies of Scale and the IBM System/360," 9 Comm. ACM 435 (1966) (concluding that larger computers offer the greatest economies of scale and indicating that "Grosch's Law, stated in the 1940s, appears to be prophetic"); A. E. Oldehoft& M. H. Halstead, "Maximum Computing Power and Cost Factors in the Centralization Problem," 15 Comm. ACM 94 (1972) ("In addition to increases in the level of technology, one can expect for any given

Grosch's Law to be repealed as some other much more precise cost models came to knowledge. Indeed, while Grosch's cost model was wrong (now replaced by Moore's Law),[5] his theory of supercomputing with dumb terminals, essentially, is the root of cloud computing. If it is said that Grosch was wrong about the cost model of cloud computing, he was right in his postulation that important economies of scale and efficiencies could be obtained by depending on enormous, centralized data centres instead of an over-dependence on storage in end units. Grosch's observations accentuate that the discourse around the theories of cloud computing have been occuring since more than 50 years. It is infact that, the world's prominent thinkers within the domain of cloud computing are just as ancient as the theories of computing themselves.

OMNIPRESENT NATURE OF CLOUD

So, while the idea of the "cloud" has been made vague with the Internet for some time, the term is still in use because it is well- established in the common of the technology. Yet, it is worth venturing the various exhibits of offerings to show how extensive the acceptance has been and elucidate area of the ecosystem, which the cloud has confined:

1. EMAIL

There are thousands of companies that supply separately identified cloud based email services. There is currently a very low barrier-to-entry for this market because web-based email is now available as an open-source platform, which means that the core software to run an enterprise-class Web-mail server can be obtained for no cost.[6] What a company really needs to do is to buy a basic Linux computer and an Internet connection to become a cloud-based provider of email. The users can check in for numerous email accounts from any email service provider so many offerings available around the globe. Therefore, rules (such as those in Europe) that need data to be stored within certain geographical limits are practically unenforceable. For example, even if a large cloud-based email provider, such as

level, a return to scale approximated by Grosch's Law"). But see Charles W. Adams, "Grosch's Law Repealed," 8 Datamation 38 (1962) (Adams suggests that Grosch's law may not be accurate. Adams' work was part of an early movement that ultimately led to the so-called "repeal" of Grosch's law.).

[5] Miniaturization is most often associated with the growth of personal computers that took place from the 1970s through the 1980s, and it is most often expressed in terms of "Moore's law." Moore's law, developed by Intel founder Gordon Moore in the 1970s, holds that the microprocessor's performance will double every 18 months. See "Caught in the Net," The Economist, March 27, 1997, at S16 (describing Moore's law and indicating that it has so far proven to be correct).

[6] VMWare's Zimbra, for example, is an open-source product that has been widely adopted by enterprises. It also is seen as a competitor to Microsoft Office 365 and to Google Apps. See "Microsoft Office 365 Launch: Zimbra Scores Surprise PR Win," The VAR Guy, June 28, 2011.

AOL, Gmail, or Hotmail were to adhere to by holding some of its servers in a particular country, there isn't any way to impose such a condition on the thousands of other cloud-based email service providing systems.

2. SOCIAL NETWORKING, PHOTOS, AND STORAGE

Social networking is big merchandise. Recent market valuations of the well-known site Facebook have cited the value of the upcoming IPO as high as $100 Billion.[7]The basis for this estimation is not just established on users' consumption, it's the boundless amount of information carried in the Facebook cloud and the price that businesses and consumers place on it. Adding on to that, with the help of services such as Yelp, businesses and users join forces in the cloud to share and rate information on businesses.

Albums or shoe boxes are no longer used to store the most prized family photographs, these are now in the cloud, stored on Flickr, Picasa, Snapfish, Apples' iCloud and many other such locations. Along with the value-added services, there are many other services that provide "hard-drive replacement" in the cloud, for example, JungleDisk, Dropbox, Onedrive, and many others.

3. MONEY MANAGEMENT AND BANKING

Banking mostly happens in the cloud. A large number of banks offer their users the chance to complete online transactions, purchase and sell stocks, pay bills, and other activities, and in number of cases, it has completely superseded the need to keep paper-based transactions or visit a physical bank branch. In addition, there are several actions of cloud-based services that help people manage their money, in a way that has been called "Banking 2.0."

Cloud-based banking products like Mint, Quicken, Wesabe, Expensr, Geezeo, Xero, MoneyStrands, and other suites either share data or consolidate data in some manner with other cloud-based suites that can help with filing and tax preparation, such as TurboTax. In total, the banking and financial system has in its complete sense moved to the cloud, such that it's easy for individuals and businesses to maintain all of their records like everyday transactions, taxes and stock trades, financial planning, all through the cloud.

4. OFFICE TOOLS

Companies like Google offer a wide base of business production tools and office-software substitutes in the cloud. Google Apps, for example, is a venture-ready suite of applications that has Gmail, Google Docs, Google Calendar and Spreadsheets, Google Sites and Google Videos.

[7] George Simpson, "A Billion Here and a Billion There," Online Media Daily, July 1, 2011.

5. E-COMMERCE

The cloud can qualify businesses to set up a complete presence of virtual business without the requirement of any infrastructure. Ebay and Amazon provide "virtual storefronts" that allow cloud-based advertising, presentation, search, and payment processing and delivery of products. Products such as Google Apps have given power to companies like Open Entry, which offers free e-commerce catalogues to Small and Medium Enterprises (SMEs) and artisans worldwide that include catalogues maintained by Google spreadsheets, images stored on Picasa Web Albums and payments by Google Checkout.[8]

PRIVACY CONCERNS WITH RESPECT TO CLOUD COMPUTING IN INDIA

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.[9] There was a debate on cloud computing and privacy from a settlement in ***Author's Guild, Inc. v. Google Inc***.[10] The conditions of the agreement allowed Google to keep on providing copies of books on Google Books which is their cloud-based platform in reciprocation for a specified amount to the authors. Though privacy was not of main concern in the agreement, many public organizations were shocked that the agreement did not recognize the security of the user's privacy.

The issue which was raised in 2010 by Consumer Watchdog was that the agreement "still contained no restrictions on what data could be gathered, and contained only limited restrictions on how that data cloud be shared". The settlement did not acknowledge 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.

In the view of Privacy Authors if the readers were concerned that information about their reading habits could be circulated to the divorcing spouses, government or other involved

[8] See Dan Salcedo, "Free e-commerce catalogs managed with Google Docs," Google Docs Blog, February 3, 2010.
[9] William Jeremy Robison, Free at What Cost? Cloud Computing Privacy under the Stored Communications Act, 2010 GEO. L.J. 1195.
[10]Authors Guild, Inc. v. Google Inc., No. 058136(DC), 2009 WL 5576331(S.D.N.Y. Nov. 13, 2009).

third parties, it would lead to these readers be less likely interested in viewing books on divisive topics. Not so surprisingly enough, the Privacy Authors incorporated several authors who had had penned books on sensitive or controversial subjects.

JURISDICTIONAL UNCERTAINTY

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 let's say if a company does not know which jurisdiction its data is subject to,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.[11] "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."[12] 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.[13] 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").[14]

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.[15] Because of HIPAA'S requirements, it is important for

[11] H. R. Cong. Res. 3162 107 Cong. (2001) (enacted).
[12] Roger Smith, Computing in the Clouds, http://www.questia.com/library/journal/1P3-1864072981/computing-in-the-cloud, accessed on 03rd June 2016.
[13] European Union Privacy Directive 95/96/EC O.J. (L.281) 31. available at http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive, accessed on 05th June 2016.
[14] Health Insurance Portability and Accountability Act of 1996
[15] Lisa J. Sotto "Privacy and Data Security Risks in Cloud Computing", 15 Electronic Com & L. Rep. (BNA) 186, 187 (2010).

foreign entities to know where their data is located.[16] This knowledge ensures that they can enter the necessary agreements with the cloud provider to avoid liability under HIPAA.[17]

Agreements related to Cloud computing do not only cause confusion regarding jurisdiction internationally but these laws within United States also vary from state to state. 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.[18] Companies that are subject to such regulations and want to execute cloud computing need to determine whether the provider has adequate security procedures to keep its electronic data safe because the data of a Massachusetts' resident data could be mixed with the data of any other user in the cloud, which makes it difficult for such cloud providers to know which state regulations shall apply to these 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.[19]

PROS AND CONS OF CLOUD COMPUTING

Cloud computing carries with it certain advantages as well as disadvantages. One of the major plus points is that it can be personalized according to one's need and so any back-up data can be arranged easily as most of the cloud service providers use open sourced API (Application Programming Interface) software where portability is not a concern and it is interoperable. It is a highly cost effective method as it decreases the budget which is mostly spent on infrastructure and security, thereby, assisting any complicated transaction in a cost effective manner.

Although cloud computing is a technologically advanced and a very effective and means, there are also some disadvantages and risks that accompany it. As there is the presence of huge amount of data and computing resources which is being circulated, it has made this environment a target for hacker. It has major security issues involved as the data or

[16] Lin Grimes & Simmons "Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171, accessed on 06th June 2016.
[17] Lisa J. Sotto, Privacy and Data Security Risks in Cloud Computing, 15 Electronic Com. & L. Rep. (BNA) 186, 187 (2010).
[18] Mass. Gen. Laws Ann. Ch. 93 H & 2 (West Supp. 2010).
[19] Mark L. Austrian, International Cloud Computing Meets U.S.E-Discovery, available at http://www.kelleydrye.com/publications/client_advisories/0865, accessed on 08th June 2016.

information is usually saved on the internet which may attract unwanted misuse of the information which is saved[20].

Furthermore, the cloud computing environment has raised various privacy concerns as well because consumers believe that they have lost control on the data which they have stored in the cloud[21]. The major privacy issues in cloud computing are:

- Trust
- Uncertainty
- Compliance

In the present cloud services, the data is usually out in the open on a machine which is owned by an organization and operated by it as well, which is not the same as the data owner himself in a form which is unencrypted and thus raises the chances of misuse of such private data. Thus, it establishes the lack of control by the user in cloud computing which in turn might lead to the unauthorized use of the saved information. Hence, there is a requirement of strong regulatory method to battle such issues pertaining to privacy.

RIGHT TO INFORMATION AND RIGHT TO PRIVACY

Another major concern related to privacy is the power of the government to expropriate and supervise any person and his location, which is in contradiction to the right provided under **Article 21** of the Constitution of India. On the same lines the Government under **Section 69** of the **Information Technology Act, 2000**, has the authority to decrypt as well as monitor any information that has been shared in the cloud by a computer resource. Therefore, the government may possibly infringe upon this right of privacy as mentioned under Article 21. However, in order to assuage the possible effects on fundamental rights certain conditions and additional safeguards have to be considered in order to protect the privacy interests. In this respect, the Court in ***Secretary General, Supreme Court vs. Subhash Chandra Agarwal***[22] noted that as regards to right to information vis-à-vis right to protect privacy, fine balancing requirements are required between the government entities and individuals. Thus, there is a requirement to carefully look into the problems related to data chain authentication, privacy and security procedures needs to be checked and altered if necessary in a way that it runs parallel with the changes required as per the particular situation.

[20] *http://sbinfocanada.about.com/od/itmanagement/a/Cloud-Computing-Disadvantages.html accessed on 09th June 2016.*
[21] *Ishan Rastogi, International Journal of Advanced Research in Computer Science (Vol 4 No. 4 March – April 2013),* http://www.academia.edu/3893183, accessed on 10th June 2016.
[22] Secretary General, Supreme Court v. Subhash Chandra Agarwal AIR 2010 Del 159.

THE LEGAL FRAMEWORK IN INDIA

In the present scenario, there is no written legislation that deals with privacy and data security. Various laws relating to intellectual property, information technology, crimes and contractual relations can help in securing the data and privacy. Although in the Indian situation, there is no specific statutory enactment expressly providing a general right of privacy to individuals in India, essentials of this right, as originally carried in the common law and in criminal law is accepted by Indian courts. These comprise the principles of trespass, nuisance, harassment, malicious falsehood, defamation and breach of confidence.

Adding on to this, a number of pieces of distinct legislation also identify this right: for example, the **Juvenile Justice Act 2000**, in which publication of names and other particulars of children involved in proceedings under the Act is prohibited; the **Hindu Marriage Act 1955**, which has similar regulations on the publication of reports relating to proceedings of matrimonial disputes; and the **Copyright Act 1957**, which strictly prohibits the unauthorised publication of photographs and certain other documents, etc. The **Code of Criminal Procedure, 1973**, also allows limitations to be forced on the publication of reports related to certain legal proceedings, eg. Rape trials.

Although there is no specific right that focuses on protection of personal data in India, there are a number of other primary sources of Indian legislation that talk about this right for Indian citizens. The sources are:

1. **Article 21**: Article 21 of the Indian Constitution is about the general Right to Privacy. This right covers the first generation of rights for Indian Citizens. The Information Technology Act of 2000 is based on a resolution that was adopted by the United Nations on January 30, 1997. This act is focused on e-commerce and cybercrime in general.

2. **Indian Contract Act**: The Indian Contract Act basically deals with requiring Indian importers to pay a duty if they are unable to protect data coming in from other countries. The **Credit Information Act of 2005**, on the other hand, imposes duties on credit information companies and credit institutions for any unauthorized sharing of an individual's credit information with external sources.

3. **Information Technology Act of 2000**: The Information Technology Act of 2000 has explicitly stated penalties for the breach of data and privacy, at least in the domain of computers and cybercrime. For instance, a person gaining access to or downloading/changing information from a computer system without prior permission from the owner is subject to civil liability. Intentional tampering with a computer system's source code is punishable by up to **three years imprisonment** or a fine of up to

two lakh rupees. The same penalty is applicable to anyone who is involved with hacking a computer system to cause wrongful loss of property.

Four sections of the **Information Technology Act** specifically deal with penalties against breach and misuse of data in India. These are Sections 43, 65, 66, and 72.

- **Section 43** protects the consumer from damages to the computer or the computer system. It foresees civil liability for actions including but not limited to unauthorized copying, extraction, database theft, and digital profiling.
- **Section 65** protects consumers against the tampering of computer source documents. It is applicable to intentional actions such as concealing, destroying, or altering of computer source code and is punishable by either or combination of a fine of up to two lakh rupees and imprisonment of up to three years.
- **Section 66**, quoted in India as a data protection provision, deals with computer hacking and protects data users from intentional alteration/misuse of data on their computers diminishing the value of the data in the process. The penalty is the same as that for Section 65.
- **Section 72** imposes a fine of one lakh rupees and an imprisonment term of up to two years for any breach of confidentiality and privacy of a person's material.

To be precise, the regulatory framework which exists at the moment does not provide complete security from breach of data; nevertheless, it is ample enough to solve a majority of the issues in the Indian situation. The coming in of new policies does not show any distinctive benefits. Whereas, new regulations that have come into existence could also pose definite and serious issues for cloud computing and the functioning of the Internet itself. In addition to slowing down the adoption rate and increasing the time to obtain benefits, it will give rise to confusion and lead to panic in our economy.

NEED FOR PRIVACY LAWS

In India there is an imminent need to build a model statute that would safeguard the Right to Privacy of individuals, especially due to the surfacing of customer-service corporate bodies which collect wide-ranging personal information about its customers. It's quite apparent that in spite of the presence of sufficient non-mandatory, ethical arguments and precedents that have been established by the Supreme Court of India; in the absence of an unambiguous privacy statute, this right of privacy still remains a de facto right, enforced through a meandering way of thinking and derived from an magnanimous interpretation of both Constitutional law and law of torts. The urgency for such a statute is amplified by the absence of any regulation in existence which manages the customer information

databases, or protects the Right to Privacy of individuals who have disclosed their personal information under specific customer contracts such as insurance contracts, contracts of credit card companies, etc.

The requirement of a globally companionable Indian privacy law should not be undermined, given that trans-national businesses in the service sectors, who strategise their establishments at their advantage in India and across Asia. For example, India is set to come up as a hub at the global level for the establishment and operation of call centres, which shall serve clients all around the world. Comprehensive databases have already been accumulated by such corporates, and the results of their unregulated operations might lead to a no-win situation for customers who are not safeguarded by any privacy statute in India, which sufficiently protects their interests. Even now in the present situation where there is liberal global regulatory paradigm, most systems of governance might not be comfortable with a legal regime, which promotes commercial interests at the cost of domestic issues.

NEW PRIVACY LAW IN INDIA

The latest development by the Government of India in relation to data privacy came in June, 2011, when it passed the **Information Technology Rules (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)** in 2011. A key component of these rules was that any organization processing personal information in India requires written consent before undertaking certain activities and must implement reasonable security policies and procedures.[23]These rules are applicable to establishments operating in India irrespective of whether the data has its origin in India or if it relates to Indian citizens. It also imposes a disclosure obligation for privacy rules wherein an organization must very clearly mention the purposes of processing the personal information involved. These laws make Internet Intermediaries responsible for harmful content on the Internet.[24]

The aim of the Indian Government is to promote offshoring in the country and for that it feels that an important step is enhancing the data privacy and security .However, the actual nature of these rules does not completely solve the original purpose.[25]The wide requirements of the new rules are more likely to increase the overhead of money, energy and time to be spent by companies when offshoring to India. The new privacy law is very new, and ultimately, it will be important for its interpretation and enforcement to be

[23]"First Analysis of the Data Protection Law in India," CRID, University of Namur, (hereinafter, "CRID India Privacy Paper").
[24]Russell Smith, "India's New Data Privacy Rules: Will They Help or Hurt Legal Outsourcing?" Law without Borders, May 23 2011.
[25] Mani Malarvannan, "New Privacy Laws To Impact Outsourcing to India," Outsource Portfolio, June 10 2011.

measured so as to allay the fears that have already been expressed by many multinational businesses.[26]

CONCLUSION

The main reason why companies prefer cloud computing over any other source of storage is because the information being stored online, eliminates the risk of losing the data or its destruction. Cloud computing also has many drawbacks which need to be considered, for example there are numerous security and privacy issues connected with data storage on the net. In addition, there is always a possibility of losing connectivity over the net which might cause interference in the flow of work of a company.

Experts in this arena say that cloud computing is safer than many of the traditional means of storing data such as servers, hard disks, etc., though companies still take the risk of data being stolen by an outsider trying to hack into the security plan of the cloud. The prime ground why companies are hesitant in choosing cloud services is due to the lack of security or protection. Traditional storage also means current risks such as hard disks which could crash that in turn will lead to destruction of stored data and hacking of servers by outsiders.

In terms of the Indian context, cloud computing is very new and there is no specific law which entirely governs it and the law is ambiguous. There is still a confusion as to which law is applicable and what is the jurisdiction. However, companies are substituting the traditional methods with cloud computing as it is cost effective.

Therefore, in our opinion, cloud computing may not be suitable for all companies due to the various problems brought forth in this article, but it is ideal and cost effective for global companies to use storing data which can be recovered at any time from any part of this whole wide world.

[26]Rama Lakshmi, "India data privacy rules may be too strict for some U.S. companies," WashingtonPost, May 21, 2011.