Implications of Cloud Computing for Personal Data Protection and Privacy in the Era of the Cloud: An Indian Perspective

"What happens to our data happens to us, who controls our data controls our lives. It's intimate and personal, and we have basic rights to it." *Bruce Schneier*

Reeta Sony A.L

National Law University, New Delhi, India. E-mail:reeta.sony@nludelhi.ac.in

Sri Krishna Deva Rao

Professor, National Law University, New Delhi, India. E-mail: psrikrishnadevarao@gmail.com

Bhukya Devi Prasad

Council of Scientific and Industrial Research, New Delhi, India. E-mail: bdeviprasad@csir.res.in

Abstract

Cloud computing refers to anything that involves delivering hosted services over the Internet. It is fast, cheap, flexible and elastic in nature. In spite of its benefits, cloud computing raises risks for data protection and privacy. One key issue presented by cloud computing is the fact that it changes our thinking of what we consider to be "our data". Data is no longer physically stored on a specific set of computers or servers, but is rather geographically distributed. The globalised nature of cloud computing poses a challenge for personal data protection, which requires a clear location for personal data, an identification of the processor and a responsible individual for data processing. Cloud data can be misused and/or shared with third parties without prior knowledge or consent of the data owner. The direct participation of an individual in transborder data transfer, third party participation in data storage, the processing and transmission of dataand, finally, negligence of data protection due diligence from cloud service providers, makes data protection and privacy laws more relevant. The recent PRISM surveillance programme scandal at the US National Security Agency (NSA) demonstrated the privacy risks that citizens around the world take on when their personal information is stored and processed in the cloud. This situation requires awell-established techno-legal solution along international standards. India, unlike the European Union, has no dedicated regulatory framework to deal with privacy and personal data protection. Although cloud computing is still in its initial stages in India, existing laws for people who are currently using facilities offeredby cloud service providers are extremely inadequate. However, cloud computing requires legal protection in India under the country's data protection laws, privacy laws and data breach laws, which must meet "international standards". It is the right time for the Indian government to enact appropriate regulatory frameworks to protect personal data and privacy in the cloud era. The overall objective of this paper is to understand the impact of cloud computing on privacy and personal data protection and to analyse present legal frameworks governing privacy and personal data protection in India and Europe.

Keywords

Cloud computing; personal data protection; privacy; PRISM; global standards.

1. Introduction

The current trend of the continuous expansion of social networking services, the increasing economic importance of data and the adoption of new technological services, such as cloud computing, offer new technological perspectives and new data protection challenges. However, the global legal community tries to keep pace with ever-expanding Information Technology, albeit, for every step forward, technology seems to be at least two steps ahead. Technology is evolving at such a rapid rate that regulators may never catch up to the pace of technological innovation. At present, the reality is that governments scrutinize what we say, where we move to, whom we contact, what lifestyle we choose within a matter of seconds by using digital technology. Governments track our digital footprints through information we share online. We do not keep our private data with us: our e-mails are shared with Internet service providers, our web searches are shared with web companies, our mobile communications are shared with cellphone companies. The government or any other third party can access our name, address, Internet and phone records, including information relating to how we pay our bills. In the worst case scenario, they can even access our credit card and bank account information. If this is not properly regulated, governments can access everything we want to keep safe without a judicial warrant. Since privacy is an essential precondition of a functioning democracy, if the government does not allow its people to act freely, it suppresses the idea of democracy.

Many countries around the world have data protection laws in place and many of these laws "are based on a combination of the OECD Guidelines, the EU(European Union) Directive or the APEC Privacy Principles".[1] When the OECD Guidelines were first adopted, the Internet hasnot emerged yet, data was in physical form, and people used to exchange data through physical mediums. At a November 2004 meeting in Santiago, Chile, Ministers from APEC (Asia-Pacific Economic Cooperation) economies adopted the APEC Privacy Framework. The APEC privacy framework follows OECD principles, but the framework suggests that "privacy legislation should be primarily aimed at preventing harm to individuals from the wrongful collection and misuse of their information".[2] Later, Data Protection Directives 95/46/EC, known as EU Data Protection Directives 1995, set out to protect the right to privacy of individuals and to facilitate the free flow of personal data between EU member states. The EU Directives prohibit the transfer of personal data to other countries; however, the Article 29 Data Protection Working Party, a European working group on data protection, has included "adequate protections" in their European privacy rules.[3] On the other hand, the USA does not have dedicated personal data protection or privacy legislation in place. Instead, the United States has sector-specific laws: Gramm-Leach-Bliley (applicable to financial institutions), HIPAA (applicable to health care providers and others dealing with health information and related entities), COPPA (applicable to online data of children under 13), and the USA Patriot Act (may be applicable to foreign companies that work with cloud providers that allow data to reside in or flow through the US). The Computer Fraud and Abuse Act, etc. and the government allow American states to have the irown individual legislation; however, the US has made privacy legislation for the private sector distinct from public sector privacy legislation.[4] India is neither a member of the

[1] CSA 2012 (Cloud Security Alliance's opinion on Cloud computing and Privacy regulation).

[2] Greenleaf, Graham. 2006."Global data privacy in a networked world." University of New South Wales, 30 March 2006.

[3] Schellekens, B.J.A. 2013."The European data protection reform in the light of Cloud Computing." Tilburg, January 2013.

[4] Simmons, Jean. "Data Protection and Privacy in the United States and Europe."*IASSIST Quarterly*.

OECD nor of APEC, and it has not signed the Budapest Convention on Cybercrime; however, it is the largest member in the Asian Association for Research Cooperation (SAARC).[5] The Indian Data Protection Bill of 2006 is still pending in Parliament and recently the Shah Committee[6] has submitted its recommendation to frame privacy laws.

It is very true that legislation is not keeping pace with technological development. With the proliferation of Internet use and the exorbitant rise in data transfer through multiple technologies, the concepts of "data protection" and "data privacy" began to receive greater attention. Because of data available at the global level, nations around the world need to understand the status and development of technology and design strong domestic privacy and personal data protection legislation to meet international standards.

2. Definitions

A list of definitions to understand the concepts discussed in this paper:

Cloud computing:"Cloud computing" refers to Internet-based computing that allows organizations to access a pool or network of computing resources that are owned and maintained by a third party via the Internet.[7]

Cloud computer user: A customer or user may be an individual, a business, a government agency or any other entity.[8]

Cloud service provider: An organization that offers a cloud computing service. A cloud provider may be an individual, a corporation or a business, a non-government agency or any other entity.

Third party: A cloud service provider is one type of third party, which maintains information about or on behalf of another entity.

Personal data: Privacy rules define the term "personal information" as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such aperson.[9]

Privacy: It means free from the interference from others. Privacy control allows the person to maintain varying degrees of intimacy. It helps in protecting love, friendshipand trust.[10]

3. Challenges and Issues of Cloud Computing: an Overview

Challenges and issues relating to cloud computing can provideus with an understanding of privacy and personal data protection issues in the cloud. The IT service known as cloud computing has been around for decades, but has not grown beyond a small fraction of total industry revenue. In the past few years however it was adopted by large, medium and small

[5] Greenleaf Graham. 2011. Promises and illusions of data protection in Indian law. *International Data Privacy Law*.Vol. 1, No. 1.

[6] A committee headed by J. A. P. Shah commissioned a 92-page report dealing comprehensively with privacy laws in the jurisdiction in 2012.

[7] Menon 2013.

[8] Gellman R. 2009. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. World Privacy Forum. USA.

[9] Dalmia Vijay. Data protection in India.

[10] Schafer Arthur. Privacy: A Philosophical Overview. Chapter 1.

industries. The availability of hardware and software services over the Internet was the concept which introduced cloud computing to individuals, consumers and business entities. Presently, cloud technology is more widely spread, used in various applications, like mature sales force management services, email, photo editing, the latest smartphone applications, and social networking.[11] Cloud computing is still in its infancy, but already it is facing several challenges.

Multi-tenancy: Multi-tenancy refers to the ability to run multiple application users on a shared infrastructure. This facilitates economies of scale by saving on the per user cost of operations. However, human error and a lack of proper understanding among users can lead to serious problems.

Virtualization: Virtualization is a key technology used in cloud services.[12] However, virtualization has some operational risks which may lead to detrimental consequences for huge data centers and information infrastructures if not properly addressed. Virtual environments have always faced system and application-based threats due to the multi-level centralized architecture with common and single points of failures.

Service Level Agreement (SLA)[13]: Cloud computing service is SLA-driven.We can discuss important issues like civil and criminal liability, data breaches, data usage, security, but SLAs for cloud-based applications and services are generally non-negotiable and are much more favorable for the provider than for the end user. Only big players can negotiate; small and medium industries do not have negotiating power.

Back up: Backup solutions play a critical role in cloud data storage. This term refers to backing up data ata remote, cloud-based server. As a form of cloud storage, cloud backup data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

Data protection and security: Data protection and security comprise one of the major challenges in cloud computing. Most organizations adopt network centric and perimeter security, which are normally based on firewalls and intrusion detection systems and which are very much the traditional security systems. This type of data and security protection does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks,[14] whereas in cloud computing services, the provider may benefit from a data centric approach with encryption, key management, strong access controls, and security intelligence to provide security for the data.

4. Privacy Issues Raised by Cloud Computing

One of the most challenging issues arising from cloud computing is protection of personal data. Various cloud aspects pose issues for privacy. Jurisdiction is one of the foremost issues affecting privacy and personal data protection in cloud computing. Within cloud computing, there are no borders. Within this environment, data can be broken up and stored in multiple data centers across multiple jurisdictions. This scenario complicates the criminal jurisdiction, and local courts struggle to determine where the data is located and which law applies to it. Security becomes the second most important issue. Personal data is processed and stored outside

[11] Young, Ernstand. 2012. Cloud Computing Issues and Impacts. Global Technology Industry Discussion Series 2012.

[12] Ruan, Keyun, Joe Carthy, Tahar Kechadi, Mark Crosbie. Cloud Forensics. Chapter 2.

[13] Service Level Agreement in Cloud Computing, PankeshPatel, AjithRanabahu, AmitSheth. http://knoesis.wright.edu/library/download/OOPSLA_cloud_wsla_v3.pdf

[14] CSO. 2012. Data Security in the Cloud. http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf.

the infrastructure in a data warehouse, which makes it vulnerable to hackers and other forms of data breaches. This vulnerability can result in lost, destroyed or improperly disseminated data. It is the primary responsibility of the cloud provider to reassure its clients that reasonable and appropriate security measures have been taken to safeguard consumer and individual data.The final challenge arises as a result of information security practices and international data transfers. It is the cloud computing provider's primary responsibility to comply with fair information practices and to fulfill legal requirements outlined in their privacy policy. Data which is collected from users or consumers for its intended collection purpose and onward transfer or third party use of the data must occur only when authorized by law, as stipulated by the terms of the privacy policy, or according to customer preference.[15] If cloud computing providers fail to manage these challenges, they will be unable to maintain the trust and confidence of their users or consumers.

5. Impact of Cloud Computing on Privacy and Personal Data

Innovation and tremendous development in information communication technologies have created new business models and tools, affecting individual lives and impacting virtually every business process and government activity. The Internet is a technology which introduced a generation of new users known as"digital natives".[16] Now, the Internet is a driving force in society. E-commerce, e-government, search engines, and social networks are deeply rooted in today's politics, culture, economy, and academia.[17] Cloud computing comprises a part of this technological development, with the Internet serving as the center point of the service. The use of the Internet in cloud computing, however, leads this service line to face the same legal issues as those facing the Internet. Cloud computing does not necessarily invade privacy; however, the storage, the processing and the transfer of personal data in the cloud pose risks to privacy. With data being transferred into the cloud, it is transferred outside the direct control of the data owner and, in some instances, it may be processed and stored in different countries. Different levels of indirect control over this data are possible depending on the type of cloud service selected. Data may be accessed and used without user knowledge or consent, which means that legal data protection mechanisms need to be in place. It is the responsibility of cloud service providers to be aware of their privacy and data security obligations when transferring personal information into any cloud environment. If privacy issues cannot be adequately addressed, it may not be appropriate to transfer "personal information", especially "sensitive information", into a cloud.

6. Impact of Cloud Computing on Privacy and Personal Data Protection Laws

The processing of personal data has become an issue of growing economic importance overthe past few years. The data analytics industry alone has been estimated to be worth over US$ 100 billion, and to be growing at almost 10% annually.[18] Personal data now comprise a cru-

[15] Privacy and Security Law Report reproduced with permission from the Privacy & Security Law Report, 8 PVLR 10, 03/09/2009 http://www.bna.com.

[16] Palfrey John, and Urs Gasser. 2008. Born Digital: Understanding the First Generation of Digital Natives. Basic Books, New York.

[17] Tene, Omer. "Privacy: The New Generations."

[18] Sotto Lisa J., Bridget C. Treacy, and Melinda L. McLellan. 2010. Privacy and Data Security Risks in Cloud Computing. *Electronic Commerce & Law Report.*

cial raw material of the global economy. Consequently, data protection and privacy have emerged as issues of concern for individuals, with confidence in data processing and privacy protection becoming important factors in enabling the acceptance of electronic commerce. The international transfer of increasing amounts of personal data and the growth of electronic commerce have resulted in economic growth that has had a positive impact around the world. The legal protection of privacy on a global scale began with human rights instruments, such as the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966. Article 12 of the Universal Declaration of Human Rights states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor, to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Sweden was the first country to enact a comprehensive national data privacy law in 1973 and the first country to implement a basic set of data protection principles.[19] Data protection laws have now spread across the world, and legislation has been enacted by a number of jurisdictions. At the time of writing, 89 countries have privacy or data protection laws.[20] Nowadays, everyone is connected to the Internet and is working in "the cloud". Cloud computing provides a service by collecting and storing online data from individuals, business entities and governments. Even governments have come to understand the potential of cloud computing, coming up with their own government clouds to provide services to their citizens. However, massive databases are maintained by both governments and private-sector businesses and these databases include information on individuals and their activities. This aspect of governments' digital agenda has led governments to consider cloud computing in framing data protection and privacy laws.

7. Personal Data Protection and Privacy in India

7.1. Status of Privacy in the Indian Constitution

One of the main barriers to developing and deploying cloud computing in India is the absence of dedicated data protection and privacy laws. In India, the constitution wasadopted in 1950. Prior to the adoption of the constitution, individual privacy was set out by parts of the criminal law, tort law, and libel and slander law.[21] Even after the constitution came into force, no fundamental right to privacy was explicitly guaranteed, whereas in countries like South Africa and Argentina the right to privacy asincorporated into the constitution. In India, the right to privacy had been derived from judicial decisions, from rights set out by Articles 19(1) (a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the constitution. However, Indian courts brought the right to privacy within the realm of fundamental rights. Examples of such decisions follow.

Kharak Singh vs.the State of Uttar Pradesh (UP)[22]

In this case, the appellant was being harassed by the police under Regulation 236(b) of UP-police regulations, which permits domiciliary visits at night. The Supreme Court found Regu-

[19] Greenleaf. 2011.

[20] Global Data Privacy Laws: 89 Countries and Accelerating; Social Science Research Network; 6 February 2012.

[21] "The Cloud: Data Protection and Privacy,Whose Cloud is it Anyway?"*GSR2012 Discussion Paper by ITU 2012*.

[22] AIR 1963 SC 1295.

lation 236 unconstitutional and in violation of Article 21.It is true that the Indian constitution never expressly declares the"right to privacy" as part of fundamental rights, but the court concluded that Article 21 of the constitution includes the "right to privacy" as part of the right to "protection of life and personal liberty".

R. Rajagopal vs.the State of Tamil Nadu[23]

In this judgment, the court stated that "A citizen has a right to safeguard hisprivacy, the privacy of his family, marriage, procreation, motherhood, child bearing and education among other matters. No one can publish anything concerning the above matters without his consent-whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages".

People's Union for Civil Liberties (PUCL) vs. Union of India [24]

The Supreme Court ruled that the telephone tapping by the government under Statute 5(2) of the Telegraph Act (1885) amounts to the infraction of Article 21 of the Indian Constitution. The right top rivacy is part of the right to "life" and "personal liberty" enshrined under Article 21 of the constitution. The said right cannot be curtailed "except according to procedure established by law". The court wanted the right to privacy under Article 21 to be expounded consistently with Article 17 of the International Covenant on Civil and Political Rights.

Naz Foundation vs. Govt. of NCT of Delhi[25]

The Delhi High Court judgment allows persons to develop human relations without the interference from the outside community or from the state. It states: "'The right to privacy thus has been held to protect a 'private space in which man may become and remain himself'".

However, all cases dealing with the right to privacy have been decided in the context of government actions that resulted in private citizens being denied their right to personal privacy. No privacy judgment has granted private citizens a right of action against the breach of privacy by another private citizen. To that extent, data protection and personal privacy jurisprudence in India is not yet developed.

7.2. Existing Legislation Protecting Personal Data and Privacy

7.2.1. The Indian Information Technology Act, 2000

The development of electronic information systemsin India enhanced awareness regarding the need to protect personal information. The Indian Information Technology Act (IT Act) came into force in 2000. The IT Act is based on Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on 30 January 1997 and is related to the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce. This legislation deals primarily with electronic transactions and digital signatures. The primary scope of this Act is to regulatee-commerce and promote the IT sector. The IT Act does not deal with privacy.

[23] (1997) 1 SCC 301.

[24] AIR 1995 SC 264.

[25] Naz Foundation vs. the Government of NCT of Delhi WP(C) No.7455/2001. 2 July 2009.

7.2.2. Information Technology (Amendment) Act 2008 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, Information Technology (Intermediary Guidelines) 2011.

The main laws regulating data privacy are the Information Technology (Amendment) Act 2008 (IT Act 2008) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules 2011 (IT Privacy Rules 2011).The concept of privacy was introduced in the IT Act 2008 through Section 43-A (compensation for failure to protect data) and Section 72-A (punishment for disclosure of information in breach of lawful contract). In 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules Act was introduced. It extends the scope of section 43A of the IT Act and regulates the collection, disclosure and transfer of sensitive personal data. The IT Privacy Rules 2011 requires corporate entities, which collect, process and storing personal data, including sensitive personal information, to comply with certain procedures. It distinguishes "personal information" and "sensitive personal information" as defined below. According to IT Privacy Rules 2011, enacted under section 87(2) of the IT Act, which defines"sensitive personal data or information", the following information is included:

- Passwords
- Financial information, such as bank account, credit or debit card, or other payment instrument details
- Information regarding physical, physiological and mental health
- Sexual orientation
- Medical records and history
- Biometric information (technologies that measure and analyse human body characteristics, such as "fingerprints", "eye retinas and irises", "voice patterns", "facial patterns", "hand measurements" and "DNA" for authentication purposes)
- Any details relating to the above bullet points provided to the body corporate responsible for providing a service or for processing or storing data under a lawful contract, or otherwise.

However, any information that is freely available in the public domain is not considered as sensitive personal data or information and is exempt from the above definitions, as set out by the 2005 Right to Information Act or any other law in force.

The IT Privacy Rules 2011 distinguishes "personal information" and "sensitive personal information", which were not previously included. The law requires that a corporate entity or the person on whose behalf it collects, stores and processes personal data or information need to meet the "Reasonable Security Practices and Procedures". The prescribed rules are explained below.

Reasonable security practices: According to IT Privacy Rules 2011, "Reasonable Security Practices and Procedures" are considered satisfied if a body corporate has implemented security practices and standards and has comprehensively documented information security programmes and policies that are commensurate with the information assets being protected. The IT Privacy Rules 2011 also sets out that International standards (IS / ISO / IEC 27001) is one such standard (Standards) which could be implemented by a body corporate. If any industry association follows standards other than IS / ISO / IEC 27001 for data protection, they need to get their codes (Codes) approved by the Indian central government.

The Rules state that bodies corporate which have implemented relevant Standards or Codes need to get certified or audited by independent auditors approved by the central government.

The audit must be carried out by an auditor at least once a year, or as and when there is a significant upgrade of processes and computer resources. A body corporate or any person operating on behalf of the body corporate must have a privacy policy. Such a privacy policy must contain prescribed details, such as the type of information collected, the purpose for collection of this information, disclosure policy, security practices and procedures followed, etc. The privacy policy is required to be made available to information providers and is required to be clearly published on the website of the body corporate.

Consent: The IT Privacy Rules 2011 states that any corporate entity or any person acting on its behalf, which collects sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information.

Collection and processing: Section 43-A of the IT Act defines "reasonable security practices and procedures" which states: "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such a body corporate shall be liable to pay damages by way of compensation to the person so affected". On the other hand, according to the privacy laws, it is very important for the corporate entity or any person acting on its behalf to obtain written consent from the provider of information. The corporate entity must use the information for lawful purposes and must not keep data for more than the required period of time. The information provider can request to correct the data if it is inaccurate.

Data protection officer: IT Privacy Rules 2011 mandates that every corporate entity collecting sensitive personal information must appoint a grievance officer to address complaints relating to the processing of such information. The contact details of the grievance officer must be published on the corporate entity's website.

Data transfer: There are no specific rules regulating the transfer of data outside of India, but the data collector must obtain the consent of the provider of information to transfer the data to any other entity in India or to an entity abroad, providing the other country ensures the same level of protection. However data can also be transferred by means of a data transfer agreement between two parties. This agreement should contain adequate indemnity provisions for third party breaches, clearly specify the end purpose of data processing (including a list of those with access to such data) and specify a mode of data transfer that is adequately secure and safe.[26] Finally, it is the responsibility of the corporate entity to not transfer any sensitive personal information to another person or entity which does not maintain the same level of data protection as stipulated by the Act.

Data breach notification law. Data breach notification plays a very important role in the context of cloud computing services. Data may be processed or handled by third parties (subcontractors). In some instances, data may be misused by such third parties, causing the person providing the information harm, be it social harm, physical harm, significant humiliation or damage to reputation. Therefore, it is very important to notify the individual concerned in a timely manner. In the USA such notification is part of the federal law, though it is limited to some sectors, such as health care and finance. The US prevents "identity theft" by protecting the "personal information of a person".[27] In Europe, European legislators adopted a pan-Euro-

[26] Christe, Alec. Data Protection Laws of the World Handbook. Second Edition. http://www.mondaq.com/india/x/231376/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+India.

[27] Lovells, Hogan A. A Global Reality: Governmental Access to Data in the Cloud: A Comparative Analysis of Ten International Jurisdictions. White paper.

pean data breach notification policy under the e-privacy directive 2002/58/EC amendment; however, it only applies to telecom operators and ISPs. Recently, the European Data Protection Commission proposed a regulation which, if adopted, would introduce a general obligation for all data controllers across all business sectors to notify the regulator in case of a breach without undue delay, and not later than 24 hours after having become aware of it. Companies would also have to report data breaches that could adversely affect individuals without undue delay. This regulation would apply not only to organizations established within EU territory, but also to organizations outside the EU, but which target EU citizens either by offering them goods and services or by monitoring their behavior.[28]At present, India does not have a data breach notification law in place despite significant rules and requirements being in place for general security, including mandatory compensation for security breaches that cause loss.

Table No 1

Details of Legislation in India, Which Provides Some Safeguards in the Absence of Dedicated Legislation

No	Legislation	What it regulates
1	Telegraph Act, 1885	The Act recognizes privacy as a right, but the government has the power to intercept communication for national security. Resolves disputes between ISPs or between an ISP and a customer.
2	Credit Information Companies (Regulation) Act, 2005	Credit information pertaining to individuals in India has to be collected as per privacy norms outlined in the applicable regulations.
3	Indian Contract Act, 1872	The Act offers an alternative solution to protecting data, as Indian companies acting as "data importers" may enter into contracts with "data exporters" to adhere to a high standard of data protection.
4	Specific Relief Act, 1963	The Act provides preventive relief in the form of temporary and perpetual injunctions, with a view to prevent a breach of an existent obligation, whether expressly or by implication.
5	Indian Copyright Act, 1957	The Act protects intellectual property rights in literary, dramatic, musical, artistic and cinematographic works. It protects creativity.
6	Indian Penal Code, 1860	The Actcan be used as an effective means to prevent data theft, including offences such as misappropriation of property, theft, or criminal breach of trust. Sanctions include imprisonment and fines under the IPC.
7	The National Consumer Disputes Redressal Commission (NCDRC) was established under The Consumer Protection Act, 1986	The Act deals with "unfair trade practice case" issues. "Unfair trade practice" includes misuse of personal data within its ambit.e.g., Niveditha Sharma's case.[1]

The above table demonstrates that India does not have an overarching privacy law. Nonetheless, the IT Amendment Act 2008 and the Information Technology (Reasonable security

[28] Prous, Oliver. 2013. "Data Security Breach Notification: It's Coming Your Way."http://privacylawblog.ffw.com/2013/data-security-breach-notification-its-coming-your-way.

[29] Nivedita Sharma vs. Bharti Tele Ventures, ICICI Bank Ltd, American Express Bank.

practices and procedures and sensitive personal data or information) Rules 2011 can protect personal data and regulate privacy issues of cloud computing or any other technology. Other legislation is also quite effective inproviding solutions in related areas. However, India is still managing the protection of personal data with many pieces of legislation, which can lead to confusion for its citizens, corporate sectors, the government, as well as outsiders. Even Indian courts have not created any precedents relating to technology related privacy issues.

8. The Need for a Privacy Law in India

At present India's privacy-related jurisprudence is judicially derived from the fundamental rights set out in the Indian Constitution. All judgments have been delivered within the context of individuals' rights to"physical privacy" against harassment by government authorities, although not against harassment by any private person. With increasing adoption of digitization in India, public and private sectors collect vast amount of personal data of an individual. Currently, there is no proper dedicated legal framework to protect personal data and privacy from misuse in either the public or the private sector. The Indian Unique Identification Number (UID)[30] project, which deals with large amounts of biometric data and personal information and stores this information on a decentralized database, has no legal protection in India. On the other hand, India is an IT hub, managing Vibrant ITES, BPO and KPO projects outsourced from abroad. Therefore, through these projects, India engages with personal information of foreign nationals and, in order to comply with international standards, India requires comprehensive legislation covering privacy and personal data protection, instead of the existing patchwork law structure.

9. Personal Data Protection and Privacy in the European Union

The Organization for Economic Co-operation and Development (OECD) adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, but the fundamental principle of privacy in the European Union (EU) is set out in Article 8 of the European Convention on Human Rights, which states that "everyone has the right to respect for his private and family life, his home and his correspondence." This right to privacy is not absolute, however, and can be restricted under certain circumstances.[31]The original EU Data Protection Directive 95/46/EC (European Directive) was enacted in 1995.[32] The European Directive and the e-privacy and electronic communications Directive 2002/58/EC, which covers data retention, are the main legal instruments covering privacy and the processing of personal data in Europe.

9.1. What is Personal Data and Who is Responsible?

The foundation of privacy laws in Europe sets out that individuals must be able to control their personal data at any time and that personal data must not be processed without either the

[30] «Parliament panel axes UIDAI; project in crisis of identity,» http://www.dnaindia.com/india/report-parliament-panel-axes-uidai-project-in-crisis-of-identity-1625536.

[31] "The Cloud: Data Protection and Privacy, Whose Cloud is it Anyway?" GSR2012 Discussion Paper by ITU 2012.

[32] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281).

consent of the individual or an explicit statutory permission. At the same time, the government must not intrude on the privacy of individuals and it should act to protect individual personal data against intrusions by other private parties.

The European Union data protection directives define "personal data", the role of the"data controller" and "data processors". According to these directives, personal data is: "any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Under European Union data protection laws, responsibility for personal data is imposed on the "controller", who may employ "processors" to process the data on its behalf. From a cloud perspective, the "controller" generally remains the institution which makes use of the cloud service, and the cloud provider is regarded as the "processor". To stay within the guidelines of the directives, cloud vendors must ensure all adequate measures are in place to ensure the protection of personal data.

The transfer of data to third countries is an important subject for cloud computing operators. Article 25 of the European Directive regulates the transfer of personal data from EU member states to "third countries" outside the EU (and the EEA).[33] However, according to Article 25(1), the transfer of personal data "may take place only if the third country ensures an 'adequate level of protection'". In absence of an "adequate level of protection" for EU data in a third country, transfer of personal data is still possible under article 42(2), in which case the controller or processor "has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument". The instruments are: (a) Binding Corporate Rules, (b) standard data protection clauses adopted by the Commission, (c) standard data protection clauses adopted by a supervisory authority, and (d) contractual clauses between the controller or processor and the recipient of the data authorized by a supervisory body. The presence of "data breach notifications", the defined role of the data protection commissioner and the defined roles of "data controller" and"data processor"result in EU data protection laws beingone of the best established, updated, and well-framed legislations around the world.[34] Finally, EU data protection laws attempt to balance the privacy of the individual on the one hand and the interests of commercial parties, such as cloud computing businesses, on the other.

10. Government Access to Cloud Computing Data and Implication for Privacy

One obstacle for the growth of cloud computing is government access to data in the cloud. Both cloud users and cloud service providers are struggling to understand when and how the government can access users' data, which is processed and stored in the cloud. Governments need some degree of access to data for criminal (including cybercrime) investigations and for purposes of national security. But privacy and confidentiality are also important issues, so the burdento provide legal justification falls on the government. However, at present, the world's Internet traffic is routed through the United States, and most online data is held there. In the USA, government access to online data was outlined in the Patriot Act 2001. The Electronic

[33] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law." In Past, Present and Future.

[34] Tana, Laura Vivet. 2013. "EU Data breach Notification Rule: The Key Elements" https://www.privacyassociation.org/publications/eu_data_breach_notification_rule_the_key_elements.

Communications Privacy Act ("ECPA") regulates cloud data which is stored by cloud providers in most cases. However, data can be accessed by the government by means of a search warrant, an ECPA court order or a subpoena issued by the government to the cloud provider. In 2007, the US government enacted the "Protect America Act" which allows the government to access electronic data without awarrant. In 2008 the FISA amendment Act made the Prism Internet Surveillance Program (PRISM) technically legal by obliging private companies to enable the US intelligence agencies to access their data.[35] Through NSA'sPRISM, the USA has accessed vast amounts of individuals' private communications, photographs, emails, voice traffic, file transfers, as well as social networking data from both domestic and foreign providers. This has raised major privacy and confidentiality concerns for customers of cloud-based services.

Table No 2 provides information regarding European and Indian laws concerning issues of privacy and personal data.

Table No 2

Indian and European laws dealing with issues of privacy and personal data

No	Privacy and personal data protection under cloud computing concerns	Issues	Existing laws to regulate issues in Europe	Existing laws to regulate issues in India	Remarks
1	Protection of personal data and privacy	Who protects personal data in the cloud and how?	EU Directive 95/46/EC on the protection of individuals with regard to processing personal data. 1)Directive 2002/58/EC on privacy and electronic communications data. 2)Directive 2006/24/EC on retention of telecommunication data.	The right to privacy is part of the right to «life» and «personal liberty», enshrined in Article 21 of the constitution. However, this right to privacy is only guaranteed against state action and not against private persons. Information Technology Rules 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules. Information Technology (Intermediary Guidelines)Rules, 2011. Section 43A on "compensation for failure to protect the data", Section 72A on "punishment for disclosure information in breach of lawful contract".	There are no dedicated privacy laws or data protection laws in India. The Data Protection bill 2006 is still pending. The Shah Committee has submitted its recommendation for the privacy bill.

[35] "PRISMand our Privacy by Encryption Administrator." July 2013.http://www.galaxkey.com/article-prism-and-our-privacy.

No	Privacy and personal data protection under cloud computing concerns	Issues	Existing laws to regulate issues in Europe	Existing laws to regulate issues in India	Remarks
2	Location of the server and jurisdiction	The data center's geographical location will determine which law applies and under which jurisdiction. If something goes wrong with personal data	Article 4 of Directive 95/46/EC.EU directives are applicable in these scenarios: 1) The data controller established within the EU. 2)The data controller established outside the EU, but using IT infrastructure within EU. 3) If personal data is transferred from the EU to other third countries. (The EU requires service providers to have partial servers within the EU).	Section 75 of the information Technology Act 2000 provides that the Act will apply to an offence (under the Act) or contravention of the Act committed outside India if the act or conduct involves a computer, computer system or computer network located in India. Privacy Rules 2011.	India is not a signatory of the Budapest Convention, so the provisions of the convention for international cooperation on the subject of cybercrime are absent in India.
3	Data access, transfer and responsibility	Who will access, transfer and be responsible for personal data protection in the cloud?	Article 2 d) and e) of Directive 95/46/EC defines "controller" and "processor". Under the EU Data Protection law, personal data protection responsibility is imposed on the "controller" and the "processor".	Data may be accessed under the Right to Information Act 2005. Under Privacy Rules 2011, a body corporate or person who is acting on behalf of the body corporate, which holds personal data, can access data for lawful purposes and be held responsible for maintaining reasonable security policies and procedures to protect personal data.	Under Indian laws "controller" and "processor" are not defined. In cloud computing it is very difficult to apply the concepts of "controller" and "processor" due to complex structures, shared resources, and combined services of cloud computing. Under the IT Act 2000, a network service provider or an intermediary is liable for any known

No	Privacy and personal data protection under cloud computing concerns	Issues	Existing laws to regulate issues in Europe	Existing laws to regulate issues in India	Remarks
					misuses of third party information or data or for not exercising due diligence to prevent the offence.
4	Data breach notifications	Is there a requirement to notify consumers of data breaches when cloud security is breached?	E-privacy Directive 2002/58/EC, but it is only applicable for telecom operators and ISPs. A new proposal by the European Data Protection Commission. If it is adopted, the data controller or business entities should notify of the breach within 24 hours after becoming aware of a breach.	India does not have data breach notifications but the Information Technology Act 2000 contains a mandatory compensation requirement for security breaches.	
5	Compulsory disclosure to the government	If a cloud provider stores data on third country servers, can the government require the cloud provider to access and disclose the data?		Under section 69 of the IT Act 2000, the Controller of Certifying Authorities can request the decryption of data under circumstances as outlined in the section.	In India, Europe or any other country, it is compulsory to disclose data for the following purposes: tax, criminal investigation, terrorism, vehicle registration, etc.

Conclusion

The status of "data" is gradually changing, and the Internet and cloud computing are making data the subject of "property, privacy and economic rights" for all individuals. There are many differences between traditional IT infrastructure and cloud computing. The benefits of

cloud computing have led to many stakeholders moving their data and infrastructure into the virtual world, where one cannot find any rules and regulations to regulate their virtual assets. Technology has the same uniform implications for privacy and personal data protection, whereas the concept of privacy jurisprudence may differ from country to country. Privacy may be viewed from different angles: in the United States,data privacy is a matter of consumer law; in Europe, it is a fundamental right; in India there is no concept called "data privacy", but the right to privacy is a part of the right to "life" and "personal liberty" enshrined in Article 21 of the Constitution. Technology, however, has the same implications for privacy around the world. Data moves around the globe within fractions of a second with the same security and privacy risks, but countries around the world still create legal environments to regulate it. Most countries have attempted to patch available legislation, with India among them, while the rest of struggle in the absence of legal frameworks to protect personal data and privacy. This is the right time to set a"global standard" on data privacy. In the EU, data protection directives guide legislation relating to the protection of privacy and personal data, with the EU constantly trying to set a "global standard" law on data privacy. India does not have any guiding legislation, but it is moving toward a set of data protection and privacy laws. India requires a proper environment develop technology awareness, technology enablers, institutions to ensure standardization, expertise to set up cooperation between the government and corporate sectors, to establish a comprehensive legal system for future technologies.

References

Greenleaf G. (2006) *Global data privacy in a networked world*. University of New South Wales.

Schellekens B.J.A. (2013).*The European data protection reform in the light of Cloud Computing*, Tilburg.

Simmons J. Data Protection and Privacy in the United States and Europe. *IASSIST Quarterly*.

Greenleaf G. (2011) Promises and illusions of data protection in Indian law. *International Data Privacy Law*, vol. 1, no. 1.

Gellman R. (2009) Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. *World Privacy Forum*, USA.

Young E. (2012) Cloud Computing Issues and Impacts. *Global Technology Industry Discussion Series*.

Patel P., Ranabahu A., Sheth A. *Service Level Agreement in Cloud Computing*. Available at: http://knoesis.wright.edu/library/download/OOPSLA_cloud_wsla_v3.pdf

CSO. 2012. Data Security in the Cloud. Available at: http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf.

(2009) Privacy and Security Law. The Privacy & Security Law Report, 8 PVLR Available at: http://www.bna.com.

Palfrey J., Gasser U. (2008) *Born Digital: Understanding the First Generation of Digital Natives*. New York: Basic Books.

Tene Omer *Privacy: The New Generations*.

Sotto L. J., Bridget C., Melinda L. McLellan (2010). Privacy and Data Security Risks in Cloud Computing. *Electronic Commerce & Law Report.*

Global Data Privacy Laws: 89 Countries and Accelerating; Social Science Research Network; 6 February 2012.

The Cloud: Data Protection and Privacy, Whose Cloud is it Anyway? *GSR2012 Discussion Paper by ITU 2012*.

AIR 1963 SC 1295.

(1997) 1 SCC 301.

Christe A. Data Protection Laws of the World Handbook. Available at: http://www.mondaq.com/india/x/231376/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+India.

Lovells, Hogan A. *A Global Reality: Governmental Access to Data in the Cloud: A Comparative Analysis of Ten International Jurisdictions*. White paper.

Prous O. (2013). *Data Security Breach Notification: It's Coming Your Way*. Available at: http://privacylawblog.ffw.com/2013/data-security-breach-notification-its-coming-your-way

Nivedita Sharma vs. Bharti Tele Ventures, ICICI Bank Ltd, American Express Bank.

Parliament panel axes UIDAI; project in crisis of identity. Available at: http://www.dnaindia.com/india/report-parliament-panel-axes-uidai-project-in-crisis-of-identity-1625536.

The Cloud: Data Protection and Privacy, Whose Cloud is it Anyway? GSR2012 Discussion Paper by ITU 2012.

Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281).

Kuner C. Regulation of Transborder Data Flows under Data Protection and Privacy Law. P*ast, present and future*.

Tana L. V. (2013). *EU Data breach Notification Rule: The Key Elements*. Available at:

https://www.privacyassociation.org/publications/eu_data_breach_notification_rule_the_key_elements.

PRISM and our Privacy by Encryption Administrator. (2013). Available at: http://www.galaxkey.com/article-prism-and-our-privacy.