pISSN: 2454-7107, eISSN: 2455-4189

Indian Journal of Law and Human Behavior
Volume 5 Number 1, January - April 2019
DOI: http://dx.doi.org/10.21088/ijlhb.2454.7107.5119.8

Original Article

Addressing Data Privacy Issues in the Indian Telecom Sector: The Way to A Healthy Competitive Environment

Rupal Marwah

Author Affiliation

Ph. D. Research Scholar, University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University, Dwarka, New Delhi 110078, India.

Corresponding Author

Rupal Marwah, Ph. D. Research Scholar, University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University, Dwarka, New Delhi 110078, India.

E-mail: rupalmarwaha@rediffmail.com

Received on 15.02.2019

Accepted on 07.03.2019

Abstract

The Indian telecom sector is growing at a very fast pace and will continue to be on this expansion path exploring new opportunities. This rapid development of telecommunications services in India has accelerated the socio-economic development of the country largely. With the expansion of telecom sector in India the use of information and communication technology (ICT) services have increased and at the same time have also facilitated sound network connectivity throughout the country. We have likewise seen an enormous growth in the quantity and quality of data that is being created by employing advanced ICT services. With the enhanced level of ICT services, the Indian telecom sector is exposed to numerous kinds of data security and information protection dangers. Taking into consideration changing dynamics of the sector and efficiency potential of data analytics the paper has discussed whether there is adequate protection of data privacy and ownership rights of users and the challenges associated with it. Another important issue that has been be addressed in the paper is to what extent individuals can dominate the manner in which data concerning them is retrieved and utilized by various entities. This paper has also discussed the recommendations given by Telecom Regulatory Authority of India (TRAI) in its consultation paper published in July 2017 concerning 'Privacy, Security and Ownership of Data in the Telecom Sector'. The paper is ended with a meaningful concluding remark.

Keywords: Data Privacy; Data Security; Telecom Regulatory Authority of India; Telecommunication; Telecom Service Providers.

How to cite this article:

Rupal Marwah. Addressing Data Privacy Issues in the Indian Telecom Sector: The Way to A Healthy Competitive Environment. Indian J Law Hum Behav. 2019;5(1):55-61.

Introduction

The issue of protection of data in India has stemmed from the substantial development of cellular market respectively in mobile cellular and mobile broadband subscriptions. Use of cell phones and online services through net access are growing at a very fast pace and therefore the cost for transfer of data between telecom users is also witnessing a considerable downfall. Telecom Service Providers (TSPs) have launched low cost data packs resulting in significant rise in cellular data consumption. India has grabbed this opportunity of taking benefit from this vast data resource which is generated through employing of modern technology. Consumer data has always been of prime importance and several studies have revealed that companies that smartly make use of this consumer data always have an edge over their competitors in gaining considerable market strength.

Technologies like the Internet of Things (IOT) and Artificial Intelligence (AI) are in a developing phase in India [1]. Consumers' now-days prefer digital platform for making payments over other modes of making payments. Online shopping, numerous applications for travel and banking, e-wallet firms like paytm, mobikwik etc. complete the digital environment [2]. This trend is emerging because of rise in cell phones use and decline in cost of data usage. This trend is further backed by Demonetization and Aadhaar exercises throughout the nation.

Large scale capturing of data and extracting valuable information out of it by plethora of entities is increasing. These entities make use of this enormous data resource to enter into or to gain dominant position in the relevant market. In most of these entities, the complete business plan is founded on data monetization. In the light of these developments telecom users suffer the most from the threat of their right to data privacy being infringed as various firms and start- ups driven by profit motive may intrude upon the consumer privacy by using their personal data without their consent. The violation of right to security and privacy of data may be internal coming from within the organization by those who may easily obtain client data and may use it to fulfill their corrupt motives as well as from third parties who are not a part of the organization engaging in data theft and stealing products by using corporate networks.

These underlined issues are a cause of concern for the sector specific regulatory bodies in the nation and therefore they are making persistent efforts to ensure data privacy and frame laws for data protection in the nation.

Data Privacy and its Legal Regulation in India

In the Indian legal framework data privacy, security and ownership in telecom sector and related laws finds place under the following statutes and regulations:

- Information Technology Act, 2000: Section 43A (provision for compensation for inability to execute reasonable safety efforts), Section 72A (imposing criminal obligation on the individual who reveals personal data without permission or in violation of a contract)[3].
- The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (IT Rules) established in accordance with Section 43A of the IT Act, 2000 [4].
- Unified License Agreements provisions: Clause 37 (licensee to guarantee the safety of privacy of communication and to guarantee that unlawful interference of messages does not happen), Clause 39.12 (Requirement towards maintaining appropriate monitoring tools according to the prerequisites of the licensor or assigned security organizations; prerequisites towards adopting important hardware and software for doing the legal interception and checking from a centralized location) [5].

Apart from the laws discussed above, we do not have any exhaustive law on data ownership and security issues in telecom sector. The current laws, rules and regulations framed by the government are only limited to the sector. Therefore it is the need of the hour that a data protection law be enacted at the earliest.

Current Issues Surrounding Data Privacy in Telecom Sector

Protecting and maintaining the privacy of data is the very basis for guaranteeing the security of telecom framework. Poor telecommunication framework could prompt interruption of essential services with a serious effect on people, organizations and the delivery of public services. It is thus important to make sure that each strata of telecom framework and the digital environment all together are secured through sufficient safety measures to protect the framework from any anticipated risk.

Few of the significant data security areas in the telecom industry that need to be addressed immediately are:

- Extensive data security risk evaluation encompassing the whole establishment
- Understanding and resolving the key legitimate concerns that affects the telecom sector
- Focusing on data security in a comprehensive form comprising of telecom system, equipments and IT frameworks, developing strong internal organization security foreseeing the potential risks and functioning prerequisites of business
- Third party security being an important component of the data security structure, elucidating an activities monitoring system for preserving the confidentiality of sensitive data
- Evaluation of threats at regular intervals which

emerge as a result of latest technologies being used and outlining controls to alleviate them.

Therefore, the following are the main parts of data security mentioned below;

a. *Network Security*

TSPs have a complicated networking system, which consist of networking components owned and controlled by various vendors. These networking components are mainly the functional configurations and procedural standards, proprietary applications, about which these TSPs have least knowledge. The situation is increasingly complex for TSPs that have networking components belonging to various Original Equipment Manufacturers (OEMs). Outsourcing of network management, agreements with different network merchants causes further complications in the system.

Difficulties in meeting the requirements of the telecom security are;

i. Huge spread of telecom network

- Telecom network containing of equipments from different merchants and these network spreading throughout the nation (operating circles)
- Consistently increasing network
- Absence of clear visibility on equipment's used and in this way there security
- Advanced business operations and innovative services
- Complications in the network architecture

ii. Administration of telecom network by third party

- Several TSPs in different operating circles
- Network equipment used by sellers which are owned by them
- Ignorant of all risks associated with the use of these equipments because of their distinctiveness
- Expenses incurred in inspection of security of all the network equipment's
- Heavy expenses incurred in installation of these equipments
- Expenses incurred in preserving records of all incoming and outgoing calls and data usage for a year

iii. Functional provisions for building an efficient security environment in the establishments

- Required expertise and knowledge for performing crucial operations
- Recruitment of Indian citizens only for key positions/jobs in the establishments
- From 1st April 2013 the TSPs shall get their accreditation done only from approved and certified laboratories in India.

iv. Guaranteeing Proper Implementation of Network Security Check

- Strong and centered network security checks could be accomplished by completing an exhaustive and all-inclusive data security threat evaluation to ascertain high threat zones that need attention.
- Setting up a well developed network security work with the operator association
- Team up with specialized, talented and experienced experts to guarantee strong security check
- Devising means for constant two way communication amid the operator network security work and the TSP
- Constant expansion of safety operations and employing technology resolutions in order to comply with network security provisions
- Constant supervision of the security regulatory framework to ascertain the numerous risks and measures to be taken for reducing these risks

b. *Consumer Privacy*

In the era of technological advancement consumers have become more vigilant about their right to privacy of data. Consumer privacy of data has acquired significant importance for the TSPs. On the other hand, the steps taken for ensuring the privacy of consumer's data are in emerging stage. In the Indian digital ecosystem various socio-economic and technological factor play a significant part in establishing a requirement for consumer privacy.

Determining Consumer Privacy

Consumer privacy should be guaranteed all through the lifecycle of consumer data which could be carried out by having a comprehensive setup which incorporates recognizing the correct set of data to be taken and the reason for the same;

having a comprehensive and thorough inventory of the customer personal data; recognizing the correct level of approach to the data based on the classification; privacy standards identified with (collection, notice, revelation of data) being vital part of the business procedures; expanding the consumer security in interaction with the third party; increasing awareness about the consumer security prerequisites for business operations[6].

c. *Internal Organization Security*

Due to the rapid development of latest technology and their increased use by TSPs, data security has become a key concern at the internal organization level. Absence of staff sincerity in maintaining data security, immense geological spread and absence of consistency of controls are the main difficulties in guaranteeing successful internal organization security. Furthermore, there exists a requirement for building up an Information Security Organization Structure that incorporates both Information Security (IT) as well as network function.

As the establishments commence new business operations, they have a tendency to concentrate more on legal prerequisites and external threat factors. Huge spread of operations and telecom services, huge employee strength, participation of third parties and complicated infrastructure makes guaranteeing internal organization security a tough task. Though, as the organizations develop, their security operation likewise develops to the level that internal information security turns into an essential hygiene for doing business activities.

Some of the difficulties faced in the Internal Organization Security are explained hereunder:

growing business actions; inorganic business development; dissemination of information over vast geographical areas; increasing clients of information resources; poor worker awareness; poor administration commitment.

Determining Internal Organization Security

Internal information security could be accomplished through incorporating security as a component of work life and executing controls to implement data security [7]. The implementation of the said steps could encourage in achieving this change by setting up a strong system, (for example, ISO 27001) alongside Information Security Management Office for driving security across establishment; setting up a consolidated system driving concerted effort from different data security activities inside the establishment; building up a structured program of making workers/merchants mindful of their data security duties across geographical areas and business capacities; making the workers responsible for data security through having security as a feature of their employment contract or set of working responsibilities; implementing security arrangements, for example, Digital Rights Management (DRM), Information Leakage Prevention (ILP) for ensuring security at the end client level; and constant supervision and learning to be incorporated as a part of the establishment system [8].

d. Third Party Security

TSPs regard outsourcing as a vital choice for the business to flourish, to reduce expenses and to give bandwidth to concentrate on core abilities. This multiparty inclusion towards delivering services to end users includes sharing of data between the third party service provider as well as the telecom administrators, which opens them to various data security threats. Difficulties in bringing about a safe and secured third party environment, overseeing data security at third party level, for example, infrastructure supplier, framework integrator, software merchant, retailers and distributors and so on is a challenging job because of constrained supervision over the third party environment. Due to the expanding number of third parties and the threats related with outsourcing, incorporating security features as a component of the agreement has become a mandate now days. Though, securing compliance with the rules and regulations and fixing the accountability for the same may end up being a tough task in the current scenario.

The main difficulties towards building up and enhancing security at third party level are; setting up proper security administration; categorization of third parties for pertinent security controls to be applicable; recognizing of Key Performance Indicators (KPIs) for data security; coordinating the security approach of the third parties with the operators security prerequisites; implementation of security necessities through contracts/ Service Legal Agreements (SLAs) Cost for occasional evaluations of third parties; extending the business continuousness beyond organizational limits towards third parties.

Determining Third Party Security

Information Security at Third Party level could be improved by outlining thorough security procedure for selection of third party to guarantee benchmark information security efforts; designing contracts with third parties containing data security prerequisites and KPIs/SLA; implementing an organized periodic threat assessment procedure with third parties; identifying an Information Security SPOC (ideally committed) from third party service supplier and formalizing controls bearing in mind that third parties are expanded limits of organization [9].

TRAI's Role in Securing Privacy and Ownership of Data

Though Telecom Regulatory Authority of India (TRAI) is only a sector regulatory body and its opinions are not binding on the government yet the government gives significant weightage to its opinions before taking any important decision on any issue concerning the telecom sector. TRAI has made some remarkable contributions in securing the privacy of consumers' data through its persistent efforts. One of these efforts include its recent recommendations concerning 'Privacy, Security and Ownership of Data in the Telecom Sector' in its consultation paper published in July 2017.

TRAI observed that as most of the consumers these days are availing e-services for various purposes, it becomes essential to protect them from any likelihood of threat emerging as result of entities in the digital environment making use of their data for gaining maximum profit [10]. The inability to secure the privacy of consumer's data may lead to hampering the development of telecom sector and Indian economy as a whole.

In the above context it becomes important to study the proposed recommendations in an in-depth manner [11]. These recommendations are explained hereunder:

a. Each client owns their personal data/ information that entities gather/preserve in the digital environment. These entities are just the repositories of the information they control and handle. They do not have essential rights over this information.

b. A research must be conducted to lay down the principles for de-identifying the individual information created/gathered in the digital environment.

c. Every entity in the digital environment, which monitors or processes the information, must be refrained from utilizing Meta-data to know about the individual clients.

d. The existing structure for safeguarding the individual data of users availing telecom services is inadequate. All entities in the digital environment, which controls or processes the confidential and sensitive data of the telecom users must be brought within the purview of information security system so that the telecom users are safeguarded against any inappropriate use of their confidential information by these entities namely the data controllers and processors in the digital environment,

e. The current permit conditions/rules applicable over TSPs for security of clients' privacy should also be applicable in relation to every unit in the high-tech environment till the legislature makes a law for data protection. For the same the Government should issue notification to inform all the entities about the policy regime for control of Devices, Operating Systems, Browsers, and Applications.

f. The government must adopt data minimization and privacy by design principle to regulate each and every body in the high-tech environment.

g. TSPs must build an effective consent framework to guarantee ample options to the users of the digital services.

h. Government must notify a framework similar to one developed by Ministry of Electronics and Information Technology (Meity) i.e. the electronic consent framework and the Reserve Bank of India's (RBI) directives for data fiduciary (account aggregator). The framework should also incorporate terms for withdrawing the assent given by the telecom user at any time. This is essential to protect the interest of the users.

i. The right to be forgotten and the right to data portability are limited rights. These rights must be subject to reasonable restrictions under the law applicable.

j. Each and every unit forming a part of digital ecosystem should comply with all multilingual, easily understandable, impartial, comprehensive and reasonable provisions in the agreement to serve users.

k. Awareness programs to be initiated for the consumers in order to impart knowledge with regard to data privacy and security concerns.

l. Entities controlling and handling data must be barred from employing 'pre-ticked boxes' to take users assent. Provisions for gathering of information and limitations attached with it must be included in the contract.

m. The stipulations about usage of devices should be notified before hand, before sale of the devices.

n. It must be made compulsory for the devices to include clauses with the goal that telecom users can erase pre-installed applications in case they choose so. Downloading of the certified applications must also be made easy for the users and the devices must in no way limit such activities by the clients.

o. Department of Telecommunication must evaluate the encryption norms again, incorporated in the licensing terms for the entities providing telecom services, to strike balance with the necessities of other sector regulatory authorities.

p. To protect the privacy of information of telecommunication users, the government must inform the users about the National Policy for encryption of user's data, produced and gathered in the digital environment.

q. In order to protect the confidential information of telecom users, personal information of users must be encrypted during the storage in the digital environment. Decryption must be allowed on a need basis by approved entities in agreement to consent of the user or according to necessity of the law.

r. Every entity in the digital ecosystem must be urged to share the data regarding vulnerabilities, risks, and so forth, in the digital environment to minimize the damage caused and avert the happening of such events.

s. Every entity in the digital ecosystem must share the data regarding the privacy violations on their e-platform and the measures taken for alleviation, and prevention of such violations in future.

t. There should be a common platform for sharing of data with respect to information security violations occurrences by all entities in the digital environment, comprising also TSPs. All entities in the digital environment must be compelled to be a part of this platform.

u. Data security violations might happen regardless of implementation of best practices/ essential actions taken by those entities who control and process data. Therefore all entities in the digital environment must be urged to share data relating to information security violations. They must also be incentivized to prevent such events in future.

The issues raised by TRAI in its Consultation Paper are relevant, yet many of these do not lie within its jurisdictional limits. Although TRAI's endeavors to start policy discussions are praiseworthy, it is similarly critical to hold up under jurisdictional confinements as an important concern. The telecom watchdog has the authority to recommend data protection principles applicable over TSPs, but its intent to control the whole digital environment might cause more perplexity than precision. The rights based method to ensure security of data is the correct approach to be followed. The legislation must contain effective provisions for ensuring that each and every individual enjoys the fundamental right to security of their sensitive and confidential data, and identify the threats associated with it. Service providers gathering data (Data Controllers) in order to provide their services shall be held liable for violation of individual's right to data privacy in case there is sufficient evidence to prove that their activities have caused injury to the common public [12]. The law must also provide that data procedures be reviewed at regular intervals to correct any errors in processing.

Conclusion

In India telecom sector is at a nascent stage regulated by strong market forces and fierce competition, progressively strict regulatory prerequisites and emerging latest technologies. Therefore, to remain competitive inside the business, telecom administrators are developing their service delivery model and service offerings to give new and groundbreaking services to consumers in a cost effective manner. This has led to a complicated security framework for the TSPs. TSPs are therefore endeavoring to build an efficient security network for the organizations which is flexible, sustainable and self developing for complying with the latest security requisites.

Our lawmaking body has likewise stepped forward in this regard and framed the Personal Data Protection Bill, 2018 which was published in the official gazette on July 27th July, 2018 [13]. This bill has been framed on the basis of the report of the Committee of Experts headed by Justice B. N. Srikrishna as its chairman. The Report gives an insight into the Committee discussions and explains the clauses of the Bill. The Bill was framed with an objective to fill in the void that was present in the current data security system, as well as expand user's rights by giving them absolute command over their sensitive and private information. It also guarantees a high degree of information security. The bill has given a broad definition of 'Sensitive Personal Data'. The bill has also discussed the issue of data localization and the duties of data fiduciary [14]. The Bill will supersede Section 43A of the Information Technology Act, 2000 (IT Act, 2000) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which was framed under Section 43A of the IT Act, 2000 [15]. This is the bedrock on which data protection law has evolved in India.

As India advances towards becoming one of the world's biggest digital economy, a stringent and effective data security legislation is the need of the hour. Thus the bill should be adopted as law as soon as possible.

Source(s) of support: Nil

Presentation at a meeting: Nil

Conflicting Interest: Nil

References

1. Rise of the Machines: Artificial intelligence scares people excessively so, The Economist, May 9, 2015. Available at https://www.economist.com/briefing/2015/05/09/rise-of-the-machines, last visited on 21.12.2018.
2. R. Larose and N.J. Rifone. Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. Journal of Consumer Behaviour. 2007;41(1): 127-49.
3. Vakul Sharma, Information Technology Law & Practice – Cyber Laws and Laws Relating to E-commerce, 5th edn. Universal Law Publishing Co. 2017.
4. Information Technology Act, 2000 Along with Rules & Regulations, Universal Law Publishing Co. 2017.
5. License Agreement for Unified License Available at http://dot.gov.in/sites/default/files/Unified%20 Licence_0.pdf, Last visited on 23.12.2018.
6. T. Peltier "How to build a comprehensive security awareness program" Computer Security Journal. 2002;6(2):23-32.
7. E.C. Chang and C.B. Ho "Organizational factors to the effectiveness of implementing information security management" Industrial Management and Data Systems. 2006;106(3):345-61.
8. Supra note 7 at 8.
9. H.A. Kruger and W.D. Kearney "A prototype for assessing information security awareness" Computer and Security. 2006;25(4):289-96.
10. Pankaj Doval, Ownership of telecom data must rest with users: Trai, The Times of India, Updated: July 17, 2018. Available at https://timesofindia.indiatimes.com/business/india-business/ownership-of-telecom-data-must-rest-with-users-trai/articleshow/65016421.cms, Last visited on 6.01.2019.
11. Consultation Paper on Privacy, Security and Ownership of Data in the Telecom Sector, Consultation No. 09/2017 Available at https://main.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf , Last visited on 8.01.2019.
12. Rahul Matthan, Manasa Venkataraman and Ajay Patri, Privacy, Security and Ownership of Data in the Telecom Sector, Policy Advisory, October 2017. Available at https://main.trai.gov.in/sites/default/files/Takshashila_07_11_2017.pdf, Last Visited on 10.01.2019.
13. Suneeth Katarki, Namita Viswamath, Ivana Chatterjee, The Personal Data Protection Bill-2018 – Key Features and Implications, The Mondaq, Updated: August 15, 2018. Available athttp://www.mondaq.com/india/x/727550/data+protection/The+Personal+Data+Protection+Bill+2018+Key+Features+And+Implications, last visited on 15.01.2019.
14. The Personal Data Protection Bill, 2018 Available at https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf, last visited on 11.01.2019.
15. Ibid.