

**Assessment of existing Know Your Customer (KYC) Norms in  
Telecom Sector in India and Way Forward**

**A Dissertation submitted to Punjab University, Chandigarh for the  
award of Masters Diploma in Public Administration in Partial  
Fulfilment of the requirement for Advanced Professional  
Programme in Public Administration (APPPA)**

**By**

**Prem Chand Sharma**

**(Roll No. 4624)**

**Under the Guidance of**

**Dr. Sapna Chadah**



**46<sup>th</sup> ADVANCED PROFESSIONAL PROGRAMME IN PUBLIC  
ADMINISTRATION**

**(2020-21)**

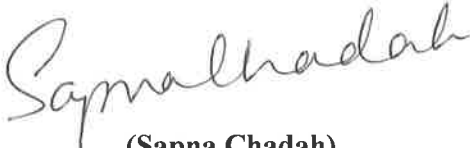
**INDIAN INSTITUTE OF PUBLIC ADMINISTRATION**

**NEW DELHI**

## CERTIFICATE

I have the pleasure to certify that Shri Prem Chand Sharma has pursued his research work and prepared the present dissertation titled “**Assessment of existing Know Your Customer (KYC) Norms in Telecom Sector in India and Way Forward**” under my guidance and supervision. The dissertation is the result of his own research and to the best of my knowledge, no part of it has earlier comprised any other monograph, dissertation or book. This is being submitted to the Panjab University, Chandigarh, for the purpose of award of Masters Diploma in Public Administration in Partial fulfilment of the requirement for the Advanced Professional Programme in Public Administration of Indian Institute of Public Administration (IIPA), New Delhi.

I recommend that the dissertation of Shri Prem Chand Sharma is worthy of consideration for the award of Masters Diploma in Public Administration of Punjab University, Chandigarh.

  
(Sapna Chadah)

Indian Institute of Public Administration  
I.P. Estate, Ring Road,

New Delhi-110002

## **Acknowledgement**

Foremost, I would like to express my sincere gratitude to my guide Dr Sapna Chadah for the continuous support, generous guidance, patience, motivation, enthusiasm, and immense knowledge for conducting this study in a very short period of time. Her guidance helped me during all the research and writing of this dissertation. I could not have imagined having a better guide and mentor for my APPPA dissertation.

I would also like to thank the IIPA as an institute for giving me this opportunity to choose a very relevant subject and providing the much needed infrastructural facilities to complete the work. I want to thank the IIPA library staff for the kind cooperation and making the required books available. I am grateful to all the experts for giving very valuable comments during the research proposal presentations which have helped me a lot in conducting this research work. I would like to thank the Course Coordinator of 46<sup>th</sup> APPPA, Dr. Charu Malhotra and Dr. Pawan Taneja for creating a very conducive and pleasant environment throughout the course, and also showing a very considerate attitude regarding timelines of various assignments especially the dissertation work. I would also to thank the APPPA officer staff Shri Manish, Shri Bisht and Shri Rajesh providing excellent support.

I would fail my duty if I do not thank the Department of Personnel & Training (DoP&T), the Government of India, for providing this wonderful opportunity to join the 46<sup>th</sup> APPPA course and thus widening vistas of my knowledge and deepening the understanding of public policy making, and meeting the wonderful and

bright officers from various streams of Indian Civil Services and Indian Armed Forces having varied and enriching experience. I shall cherish my association with all these bright minds of India.

Finally, I must thank my wife and adorable kids for showing tremendously supporting attitude and letting me have enough time to complete this work.

\*\*\*\*\*

## Table of Contents

<b>Chapter</b>	<b>Title</b>	<b>Page No</b>
<b>Chapter-1</b>	<b>Introduction</b>	<b>1-20</b>
<b>Chapter-2</b>	<b>KYC Norms in Telecom Sector – International Scenario</b>	<b>21-44</b>
<b>Chapter-3</b>	<b>KYC norms in Telecom Sector in India</b>	<b>45-75</b>
<b>Chapter-4</b>	<b>Conclusions and Suggestions</b>	<b>76-82</b>
<b>Bibliography/ References</b>		<b>83-86</b>
<b>Annexures</b>		<b>87-99</b>

## List of Tables

<b>Chapter/ Table No.</b>	<b>Title of Tables</b>	<b>Page No</b>
<b>Chapter-3</b>		
<b>Table-1</b>	<b>Developments and milestones</b>	<b>47-48</b>

## List of Figures

<b>Chapter/ Figure No.</b>	<b>Title of Figures</b>	<b>Page No</b>
<b>Chapter-2</b>		
<b>Figure-1</b>	<b>Unique Mobile Subscribers as a percentage of total population</b>	<b>22</b>
<b>Figure-2</b>	<b>Aggregate Mobile Subscribers as a percentage of total population</b>	<b>23</b>
<b>Figure-3</b>	<b>Share of Prepaid Connections as a percentage of total mobile subscriptions</b>	<b>24</b>
<b>Figure-4</b>	<b>Status of SIM Registration Policies</b>	<b>28</b>
<b>Figure-5</b>	<b>Type of Mandatory SIM Registration Policy, by Country</b>	<b>32</b>
<b>Figure-6</b>	<b>Prepaid SIM verification using DVS and VEVO</b>	<b>39</b>
<b>Figure-7</b>	<b>Information Flow for Identity Verification Using DVS</b>	<b>40</b>

## List of Annexures

<b>Chapter/ Annexure No.</b>	<b>Title of Figures</b>	<b>Page No</b>
<b>Chapter-2</b>		
<b>Annexure-1</b>	<b>SIM Registration Policy Landscape by Country</b>	<b>87-98</b>
<b>Chapter-3</b>		
<b>Annexure-2</b>	<b>Instructions dated 29<sup>th</sup> December 2004 regarding verification of identity of subscribers</b>	<b>99</b>



## **Executive Summary**

Know Your Customer known as KYC in general parlance is the process of verification of customers or clients by businesses before enrolling them for services. In Telecom Sector, KYC of the subscribers is done from the angle of security of the Nation. The purpose of KYC in Telecom Sector is for ensuring traceability of the subscribers in case services are used by them against the security of the nation.

In India, KYC in telecom sector is regulated through the instructions issued by Department of Telecommunications, Ministry of Communications as per provisions contained in the Indian Telegraph Act, 1885. Earlier, it was being regulated through administrative instructions only. However, in 2019, statutory provisions have been made in Indian Telegraph Act, 1885 regarding KYC.

In some cases, Telecom facilities are misused by miscreants for committing crimes from remote locations. In such cases, telecom facilities are obtained by miscreants in the name of other persons by using fake/ forged identity documents or by using someone else identity documents. As an illustration, 251 SIMs were obtained in one name from 163 different points of sale situated in 57 different cities. In another case, 218 SIMs were obtained in one name on different dates from 157 points of sale located in 59 different cities. These SIMs were obtained by forging of documents.

The main purpose / objective of the study is:

- (i) To study the existing Know Your Customer (KYC) regulatory norms in telecom sector in India and abroad e.g. Australia, USA, UK etc.
- (ii) To analyse the effectiveness of existing Know Your Customer regulatory norms (use of fake/ forged documents and identity theft) in telecom sector of the Country.
- (iii) To suggest the improvement in the existing Know Your Customer norms in telecom sector.

Quantitative Research Strategy has been employed in this study. Further, descriptive/ theoretical research design/ methodology has been employed. The study is based on

secondary method of data collection. Different aspects related to KYC norms nationally and internationally in telecom sector have been explored/ studied. A detailed study of Government guidelines on telecom sector KYC has been made. Further, detailed study of judgments and orders delivered by various legal forums has been carried out. Also, various media reports on the subject have been examined and studied. Data has been collected from different websites including International Telecommunications Union, Department of Telecommunications, Telecom Regulatory Authority of India (TRAI).

This study will present the best practices being followed internationally for KYC in telecom sector. The outcome of this study will suggest improvement in the KYC process being followed at present in the country which may help in elimination/ minimisation of the issuance of SIM cards by miscreants by using fake/ forged documents and identity theft thereby substantial reduction in crimes using telecom services.

The conclusions as under have been arrived in the study:

- (a) That SIM cards are getting issued to the subscribers by use of fake/ forged documents and also through identity theft.
- (b) That in Aadhaar based E-KYC process using biometrics, there is practically no possibility of issuance of SIM cards using forged/ fake documents.
- (c) That in Aadhaar based E-KYC process using biometrics, issuance of SIM cards through identity theft is also avoided.
- (d) That in other processes wherein no online verification of subscribers is done before activation of SIM cards, SIM cards are found to be issued by use of fake/ forged documents.
- (e) That SIM cards are found to be issued through identity theft in case of process wherein no online verification of subscribers is done before activation of SIM cards.
- (f) Thus, KYC Regulatory Norms in Telcom Sector of the Country are not effective.

Following improvements are suggested in the KYC regulatory norms in telecom sector:

- (i) Government should launch an Identity Verification Service for online verification of identity and address documents presented by the customers against the records maintained by the issuing authority of such documents.
- (ii) Identity Verification Service should be launched through a partnership between the Central Government, State Government and Local Bodies as identity and address documents to be verified are issued by them.
- (iii) Identity Verification Service should have provision for:
  - (a) Document Verification Service – checks whether the biographic information on the document matches the original record.
  - (b) Identity Data Sharing Service – For sharing information held by document issuing agency with the requesting agency as per consent of customer.
  - (c) Face Verification Service – comparing the photo against the image used on the identity documents with the consent of customers.
- (iv) Identity Verification Service should be made available for use of private organisations (Telecom, Banking, Insurance etc.) as well as Government Agencies.
- (v) Government should made provision for Identity Gateway Service Providers for having connectivity between Identity Verification Service and the users of the service.
- (vi) As Government has time and again reiterated that it has no business to be in business, Government should authorise private organisations (either through license or otherwise) to act as Identity Gateway Service Providers.
- (vii) The SIM cards should be issued to the customers only after online verification of the identity documents produced by them through Identity Verification Service.
- (viii) The identity document presented by the customers for obtaining SIM cards should be online verified using “Document Verification Service” under Identity Verification Service for avoiding use of any fake/ forged document.

- (ix) Live photograph of the customer desirous of obtaining SIM cards should be matched with the photograph maintained by the identity document issuing authority using “Face Verification Service”. It will ensure the avoidance of identity theft cases.
- (x) Once photograph is matched, the demographic data maintained by the identity issuing authority should be transferred using “Identity Data Sharing Service” to Mobile Operators similar to Aadhaar based E-KYC service.
- (xi) Presently SIM cards are being issued through about 25 types of identity and address documents. Some of these documents are issued using digital platform thereby verifiable online and some are issued without digital platform which may not be verifiable online using Identity Verification Service.

Either the Government should restrict the issuance of SIM cards:

- (a) only through online verifiable documents

OR

- (b) in case of non-online verifiable documents, SIM cards should be restricted to be issued only through “Telecom Service Provider Operated” Point of Sale by following some special verification procedure. In such case SIM cards should not be issued through retailers.

- (xii) As in all the above-mentioned suggestions, private and sensitive data/information of the citizens shall be involved, it is also recommended that Government should enact a very strict privacy and data protection laws in order to avoid any remotest possibility of misuse of data / information of the customers.

## **Chapter-1**

### **Introduction**

#### **1.0 Introduction**

1.0.1 Know Your Customer abbreviated as “KYC” in general parlance is the process of verification of customers or clients by businesses before enrolling them for services etc. It is generally used to ensure that services provided to the customer are not misused by them. In Telecom Sector, KYC is done for ensuring security of nation. The purpose of KYC in Telecom Sector is for ensuring traceability of the user of the service.

1.0.2 Continuous advancements are continuously taking place in the society. With the technological innovations and development of society, new services are coming into existence. These services on one hand make life of the peoples easier but on the other hand they also create new problems. It is noted that every new innovation while delivers something good to the society but at the same time it also has adverse impact on the society. Every new innovation or service has both good and bad facets. The aim of Governments world over is that while good part of every innovation, advancement and service should be passed on to the society, at the same time proper mechanisms should be put in place to stop the ill effects of the same on the society.

1.0.3 For example, industrial revolution transformed economies that had been based on agriculture and handicrafts into economies based on large-scale industry, mechanized manufacturing, and the factory system. New

machines, new power sources, and new ways of organizing work made existing industries more productive and efficient. However, on the flip side, it resulted into enhancement of various types of pollution on the earth.

Similarly, with the development of society, very sophisticated and advance banking system has come into existence which has made life of the people very easy. The banking system has approached to every nook and corner in the world. Now, money can be transferred from one place to another place in the world on one click of the button. Now, there is no need of keeping cash money by people with them. However, at the same, it is creating various types of problems like money laundering etc.

1.0.4 In the telecom sector also, there has been very fast and unmatched advancements. These developments have made the life of peoples very easy. In earlier times, it was very difficult to communicate by peoples with another. Peoples have to move physically for communicating. But, now communication can be made within microseconds with each other without any distance barrier. However, it has another facet also. The telecom services are misused for doing various types of crimes including terrorism.

1.0.5 In order to avoid above-said ill effects, it has been mandated by the Governments world over to carry out the process known as Know Your Customer (KYC) by the businesses and service provider wherein information about identity and address of the customers is verified before enrolling them. This is done in order to avoid involvement of the customers in illegal

activities and crimes. KYC is generally done prior to enrolling the customers and also it is updated periodically.

1.0.6 In Telecom Sector, KYC of the customers is done for mandatory SIM registration from the angle of security of nation. In India, KYC in telecom sector is regulated through the instructions issued by Department of Telecommunications, Ministry of Communications as per provisions contained in the Indian Telegraph Act, 1885. Earlier, it was being regulated through administrative instructions only. However, in 2019, statutory provisions have been made in Indian Telegraph Act, 1885 regarding KYC.

1.0.7 **The Aadhaar And Other Laws (Amendment) Act, 2019 No. 14 of 2019<sup>1</sup>**

1.0.7.1 Indian Telegraph Act, 1885 has been amended in 2019 through ‘The Aadhaar And Other Laws (Amendment) Act, 2019 No. 14 of 2019’. Keeping in view the importance of KYC, first time provisions have been made in the Act for verification of customers. Till Now, the KYC process in telecom was being enforced through Administrative Circulars only without any backing of Act.

1.0.7.2 The relevant parts of “The Aadhaar And Other Laws (Amendment) Act, 2019 No. 14 of 2019” regarding amendment in Indian Telegraph Act, 1885 are reproduced as under:

26. In section 4 of the Indian Telegraph Act, 1885, after sub-section (2), the following sub-sections shall be inserted, namely:—

*'(3) Any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India, shall identify any person to whom it provides its services by—*

- (a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or*
- (b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or*
- (c) use of passport issued under section 4 of the Passports Act, 1967; or*
- (d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf.*

*(4) If any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India is using authentication under clause (a) of sub-section (3) to identify any person to whom it provides its services, it shall make the other modes of identification under clauses (b) to (d) of sub-section (3) also available to such person.*

*(5) The use of modes of identification under sub-section (3) shall be a voluntary choice of the person who is sought to be identified and no person shall be denied any service for not having an Aadhaar number.*



*(6) If, for identification of a person, authentication under clause (a) of sub-section (3) is used, neither his core biometric information nor the Aadhaar number of the person shall be stored.*

*(7) Nothing contained in sub-sections (3), (4) and (5) shall prevent the Central Government from specifying further safeguards and conditions for compliance by any person who is granted a license under the first proviso to sub-section (1) in respect of identification of person to whom it provides its services.*

*Explanation.—The expressions “Aadhaar number” and “core biometric information” shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.’.*

1.0.8 In accordance with the above-said provisions contained in the Indian Telegraph Act, 1885, Department of Telecommunications, Ministry of Communication has issued instructions dated 29.09.2020 for use of “Aadhaar Number/ Virtual ID” e-KYC service of Unique Identity Authority of India (UIDAI) as an alternate process for issuing mobile connections.

## **1.1 Literature Review**

### **1.1.1 Dissent on Aadhaar, Big Data Meets Big Brother<sup>2</sup>**

- (a) Dissent on Aadhaar is a book edited by Reetiak Khera, Associate Professor (Economics) at IIT Delhi. Earlier, she was Associate Professor (Economics and Public Systems group) at the Indian Institute of Management, Ahmedabad (IIM Ahmedabad) from 2018-20. This book comprises of 15 Essays by community of dissenters on various issues related to Aadhaar. These include journalists, such as Anumeha Yadav, whose reporting on Aadhaar for the website, Scroll.in, was pioneering, economists such as Khera herself and Jean Dreze, engineers, policy experts, and lawyers, including Shyam Divan, who led arguments for the petitioners in the Supreme Court, and Usha Ramanathan, who saw alleged dangers inherent in the Aadhaar project.
  
- (b) This book was put together before the Hon'ble Supreme Court rendered judgment dated 26.09.2018 in Aadhaar matter in Writ Petition No. 494 of 2012 titled as Justice K.S. Puttaswamy (Retd.) and Another Vs Union of India and Others<sup>19</sup>. However, some of the chapters have been updated in the 2019 book to incorporate the judgment's effect.

- (c) This book examines following issues in 15 chapters containing essays by various dissenters on Aadhaar:
- (i) Impact of Aadhaar in Welfare Programmes
  - (ii) On the Margins of Aadhaar : The Living Dead, and Food ‘Disruptions’.
  - (iii) A Unique Identity Dilemma
  - (iv) Aadhaar and Privacy
  - (v) Surveillance Project
  - (vi) Aadhaar – Identity or Dystopia?
  - (vii) Inside the Plumbing of Technology Projects.
  - (viii) Aadhaar’s Biometric Tsunami: Will it Seep Away Privacy, Drown Civil Liberties?
  - (ix) Aadhaar – Constitutionally Challenged
  - (x) The Privacy Judgment
  - (xi) The Relevance of Children’s Consent under a Mandatory Aadhaar Regime
  - (xii) Aadhaar – From Welfare to Profit
  - (xiii) Public Investments and Private Profits
  - (xiv) Is Aadhaar like the Social Security Number?
  - (xv) Identity and Development” Questioning Digital Credentials
- (d) This book examines various issues like was Aadhaar necessary to create because there were many Indians without a legal ID? Aadhaar data says, only 0.03 percent of Aadhaar enrollments were by people

without existing IDs, using the ‘introducer’ system. Were existing IDs compromised, necessitating an overhaul of our national ID systems? If so, how is it that those very compromised IDs were used to create the Aadhaar database? And what of the loopholes in the Aadhaar system, like cards for dogs and gods?

- (e) Does Aadhaar prevent fraud? The book points out three kinds of fraud: identity fraud, eligibility fraud, and quantity fraud; Aadhaar only provides some measure of protection against the first. The most prominent kind of fraud in India’s social schemes is quantity fraud. Even eligibility fraud, where citizens claim benefits reserved for others, cannot be checked by Aadhaar, as eligibility depends upon a separate set of documents.
  
- (f) This book also examines that in a country where basic infrastructure in terms of electricity and mobile phone connections is poor, can a digital ID system like Aadhaar really ease the process of disbursement?

This book discusses various issues related to Aadhaar but does not specifically examine the KYC norms of Telecom Sector in the country.

### 1.1.2 **Telecom KYC and mobile banking regulation: An exploratory study<sup>3</sup>**

- (a) This study deals with alignment of the ‘Know Your Customer (KYC)’ process of the telecom sector with that of banking. It explores KYC processes of both the sectors and brings out the ‘issues and challenges’ associated with subscriber acquisition and customer document management of telecom companies (telcos).
  
- (b) According to study, as telcos do not have any exposure risk from prepaid customers, they tend to treat the KYC and document management of prepaid users merely as a compliance formality. They resort to lowest-cost outsourcing and heavily depend on a large ill-equipped field-force. This leads to inadequate capture of customer details and loss of many opportunities for completion/correction of records.
  
- (c) The Banking and Telecom sectors will need to jointly address this by training the work-force and by bringing down the dependence on field-staff for verification/authentication of customer documents. It may be useful to review the penalty on defaulting telcos and enforce periodic verification of prepaid subscribers to align the KYC processes of the two sectors and achieve successful implementation of m-banking.

This study is regarding alignment of KYC in Telecom and Banking Sector. It does not address the matter of SIM issuance on fake/ forged documents and identity theft.

### 1.1.3 **Digitalisation & Data Protection – Changing Landscape of Indian Telecom Sector<sup>4</sup>**

- (a) This study paper basically deals with data protection and privacy issue in telecom sector. It also discusses biometric based E-KYC process in place of paper based process in Telecom Sector which in absence of adequate data protection regime, may have implications from privacy laws perspective.
- (b) It discusses various privacy related law and policy documents like Information Technology Act, 2000, Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules 2011, Telecom Regulatory Authority of India Act, 1997, Telegraph Act, 1885, Clause of Telecom Licenses, Department of Telecommunications (“DoT”), Ministry of Communications, Government of India instructions dated 23 March 2017, requiring the Mobile Operators to re-verify all existing mobile subscribers (prepaid & post-paid) through Aadhaar based E-KYC (Know Your Customer) process. It also discusses Judgment dated 24 August 2017 in the Putuswamy case (Privacy Judgement) wherein the

Supreme Court in a nine judges that held that privacy is a fundamental right under the Indian Constitution.

- (c) According to paper, overall approach by DoT ought to have been in a logical manner where first step should have been that only prospective acquisitions being only mandated through E-KYC in near future. Unless this is done first, 100% re-verification of existing customers through E-KYC has little meaning and sense to the customers.
- (d) There are also many operating challenges of the Re-verification process, viz. outstation customers, various Large NRI population, Person of Indian Origin (PIO) and / or Overseas Citizens of India (OCI) who may also be citizens of other country, having mobile connections with Indian MNO's, does not have Aadhaar and further those having Aadhaar may not necessarily visit India for re-verification.
- (e) Paper also discusses Justice Srikrishna Committee constituted on data protection in the country.

This study inter-alia deals with data protection in E-KYC process in Telecom Sector. It does not address the issues arising due to issuance of SIM cards on fake/ forged documents and identity theft.

1.1.4 **Unique Identification Project for 1.2 billion People in India Can it fill Institutional Voids and enable 'Inclusive' Innovation? <sup>5</sup>**

(a) India has no equivalent of a social security number and more than 400 millions of poor suffer in the hands of the existing system because they are unable to participate in the formal economy. In a nation that is struggling to meet basic challenges of poverty, hunger, poor infrastructure etc., the government of India's UID project appears to be a striking outlier as it is building the world's biggest and advanced biometric based database of identities for 1.2 billion people at a remarkable pace. Using the theoretical lens of institutional voids, this paper describes the case of UID project and explores its potential in terms of filling institutional voids and enabling inclusive innovation in India.

(b) A telephone/mobile connection in India is issued only after a stringent know-your-customer (KYC) process, which requires identity and address proof. People lacking such documents either get excluded from telecom services or resort to fake documentation to get a phone connection. UID can be used as an identity proof for obtaining mobile phone connections.

This study inter-alia deals with providing identification to all the citizens through UID project and thereby providing telecom services to all such peoples who presently do not have identity. It does not address the issues arising due to issuance of SIM cards on fake/ forged documents and identity theft.



## **1.2 Statement of Problem**

1.2.1 Security of Nation is paramount. The KYC norms of telecom subscribers are done keeping in view the security of Nation.

1.2.2 It is noted that telecom facilities are misused by miscreants for committing various types of crimes without coming into physical contact and sitting at remote locations. Miscreants find telecom services as one of the easiest mode of committing various types of crimes. In such case, telecom facilities are obtained by miscreants in the name of other persons by using fake and forged identities and identity theft etc.

1.2.3 251 SIMs were obtained in one name from 163 different points of sale situated in 57 different cities. In another case, 218 SIMs were obtained in one name on different dates from 157 points of sale located in 59 different cities. These SIMs were obtained by forging of documents<sup>6</sup>. Similarly, in Punjab, 185 pre-activated SIM cards in fake names and documents of fake addresses were recovered in Punjab by Police<sup>7</sup>.

1.2.4 Two persons were booked for selling SIM card on fake ID by Punjab Police. The SIM was used for sending objectionable and threatening messages to many peoples<sup>8</sup>. A SIM card issued on fake and forged documents was used in a ransom case in Bihar<sup>9</sup>. Similarly, a SIM card issued on fake identity was used in making ransom calls in Punjab<sup>10</sup>. SIM card issued in the name of

fake person was used for making fishing calls in Jharkhand<sup>11</sup>. Haryana police identified 685 SIM cards issued on fake and forged documents. Out of these 392 SIM cards issued on forged documents were deactivated by Haryana Police. These SIM were being used in fraudulent activities<sup>12</sup>. In Telangana, Police seized 4000 SIM cards which were procured using forged ID proofs and photographs and were used for cheating major companies through marketing campaigns<sup>13</sup>. Maharashtra Police busted racket of illegal purchase-sale of SIM cards and impounded 11,345 activated SIM cards, 49,500 photographs, 9,400 fake Aadhar card copies, 3,072 copies of fake voters ID cards<sup>14</sup>. 938 complaints covering 65,991 mobile connections have been received in the last five years with regard to sale of SIMs on fake identity proofs and disconnection was carried out in all such cases<sup>15</sup>. Department of Telecommunications (DoT), on 16.08.2016, has Aadhaar based E-KYC process for issuing new mobile connection to subscribers (individual category). This E-KYC process is an alternative process to the document based process (Proof of Identity/Proof of Address documents) to avoid any public inconvenience on account of non-availability of Aadhaar number. In this process, the customer and Point of Sale of the Licensee are authenticated biometrically from UIDAI servers and the demographic details and photograph of the customer are captured in the Customer Acquisition Form (CAF) and stored in the Telecom Service Provider's (TSP's) database. In E-KYC process no separate document for Proof of Address/ Proof of Identity are required to be submitted, therefore the possibility of forgery/misuse of documents submitted by the subscribers can be avoided<sup>15</sup>.

**1.3 Purpose / Objective :** The main objectives of the present study are as under:

- (iv) To study the existing Know Your Customer (KYC) regulatory norms in telecom sector in India and abroad e.g. Australia, USA, UK etc.
- (v) To analyse the effectiveness of existing Know Your Customer regulatory norms (use of fake/ forged documents and identity theft) in telecom sector of the Country.
- (vi) To suggest the improvement in the existing Know Your Customer norms in telecom sector.

**1.4 Research Strategy**

Quantitative Research Strategy has been employed.

**1.5 Research Design/ Methodology**

Descriptive/ theoretical research design/ methodology has been employed. The study is based on secondary method of data collection. Different aspects related to KYC norms nationally and internationally in telecom sector have been explored/ studied. A detailed study of Government guidelines on telecom sector KYC has been made. Further, detailed study of judgments and orders delivered by various legal forums including Hon'ble Supreme Court,

different High Courts, Telecom Disputes Settlement and Appellate Tribunal (TDSAT) has been carried out. Also, various media reports on the subject have been examined and studied. Data has been collected from different websites including International Telecommunications Union, Department of Telecommunications, Telecom Regulatory Authority of India (TRAI) and other Websites.

## **1.6 Rationale or Justification**

1.6.1 At present predominantly frauds and crimes are taking place due to misuse of telecommunications facilities. In most of such cases, SIMs are obtained by miscreants in the name of someone else using fake & forged identities and by identity theft.

This study will present the best practices being followed by various government world over for KYC in telecom sector. The outcome of this study will suggest improvement in the KYC process being followed at present in the country which may help in elimination/ minimisation of the issuance of SIM cards by miscreants by using fake and forged documents thereby substantial reduction in crimes using telecom services.

## **1.7 Research Questions**

- (i) What are the prevalent KYC regulatory norms in India and abroad (e.g. Australia, USA, UK etc ) in telecom Sector?
- (ii) Are the existing KYC regulatory norms in telecom sector of the Country effective (use of fake/forged documents and identity theft) ?
- (iii) What are the possible improvements in the KYC norms of telecom sector of the Country?

## **1.8 Scope / Limitations/ Delimitations**

### 1.8.1 Scope

For the purpose of study, the secondary data available nationally and internationally has been explored.

### 1.8.2 Limitations

Not much study is available particularly on the KYC norms of telecom sector in the Country.

### 1.8.3 Delimitations

As such there are no specific delimitations being used in the study.

## **1.9 Chapterisation Scheme**

This dissertation consists of four chapters, namely Introduction, KYC Norms in Telecom Sector –International Scenario, KYC norms in Telecom Sector in India and Conclusions and Suggestions.

### **1.9.1 Introduction**

This is the first chapter of the dissertation. It provides basics understanding of the topic of dissertation. Further, it consists of Literature Review, Purpose/ Objective of the study, Research Strategy, Research Design/ Methodology employed, rationale/ Justification of the study, Research Questions, Scope/ Limitations/ Delimitations and Chapterisation Scheme.

### **1.9.2 KYC Norms in Telecom Sector –International Scenario**

The second chapter of the dissertation is regarding KYC norms being followed in different countries of the world. It consists of Global Telecom Scenario (global statistics mobile connections, internet, impact of telecom on GDP etc.), approaches being followed worldwide for addressing security concerns in Telecom Sector, details of countries with mandatory SIM registration policies, SIM registration implementation models, alternative to registration solutions (status in developed countries like USA, UK and Mexico), Data Protections and Privacy Frameworks in different countries of

the world, mandatory SIM registration solutions, Telecom KYC Process being followed in Australia and Identity Matching Services in Australia.

### 1.9.3 **KYC norms in Telecom Sector in India**

Third chapter is regarding KYC norms in Telecom Sector in India. It consists of brief background of Telecom Sector in India, Evolution of Telecom KYC Norms in the Country, Current KYC Norms in Telecom Sector, Status of Data Protection and Privacy and Effectiveness of existing KYC Regulatory Norms in the Country.

### 1.9.4 **Conclusions and Suggestions**

The fourth and final chapter contains Conclusions and Suggestions for improvement of the KYC norms in the Telecom Sector of the Country.

\*\*\*\*\*



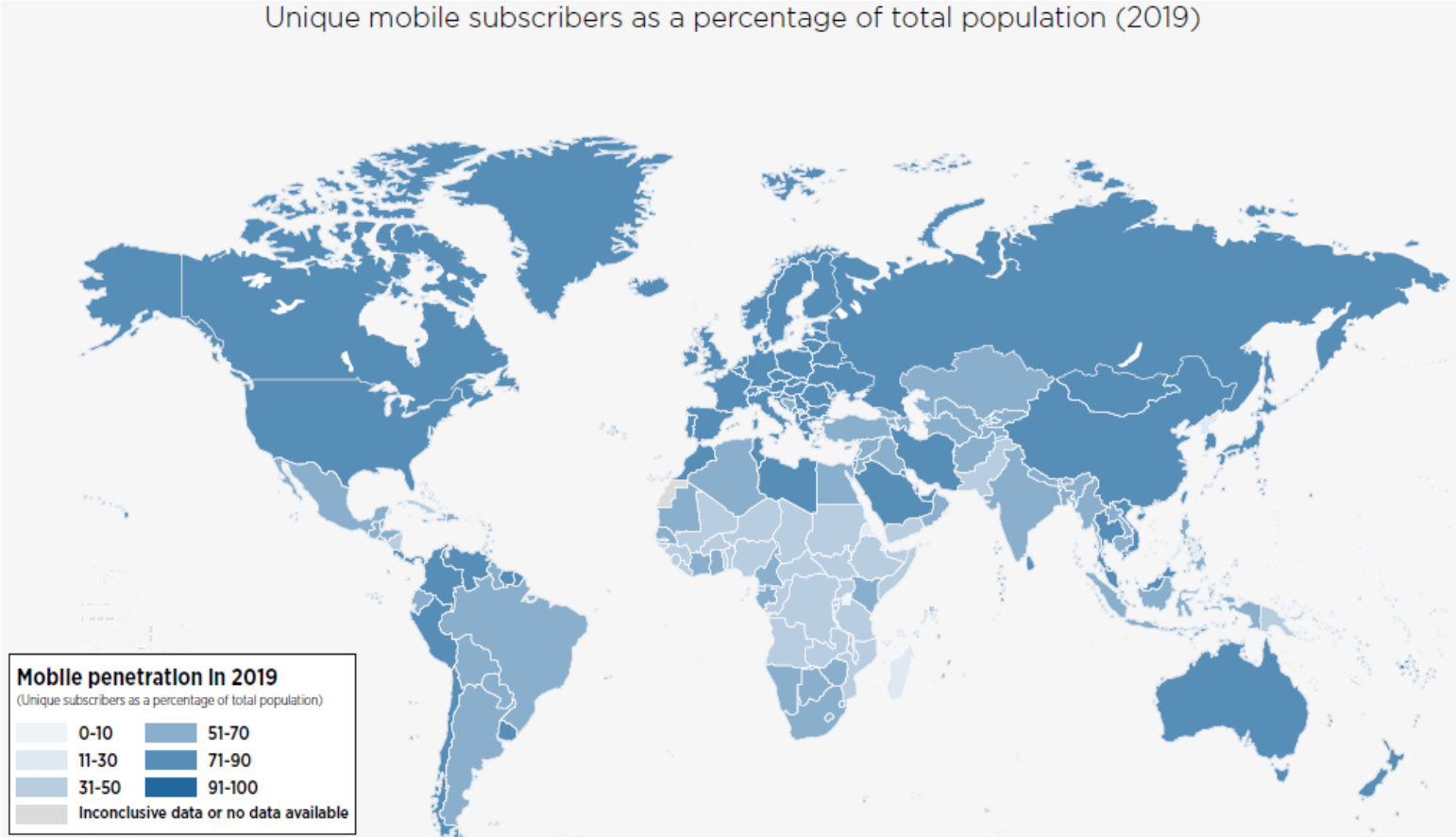
## **Chapter-2**

### **KYC Norms in Telecom Sector –International Scenario**

#### **2.0 Global Telecom Scenario**

2.0.1 By the end of 2019, 5.2 billion people subscribed to mobile connections (unique mobile subscribers) accounting for 67% global population. Adding new subscribers is becoming difficult as markets have saturated. Despite this, there will be around 600 million new subscribers by 2025 (Mostly in India, China, Pakistan and Nigeria). There were 3.8 billion mobile internet users (49% of global population) in 2019 and the same is expected to reach 5 billion by 2025 (61% penetration). SIM connections are expected to increase from 8 billion in 2019 to 8.8 billion in 2025 (excluding licensed cellular IoT). Internet of Things (IoT) connections are expected to increase from 12 billion in 2019 to 24.6 billion by 2025<sup>16</sup>.

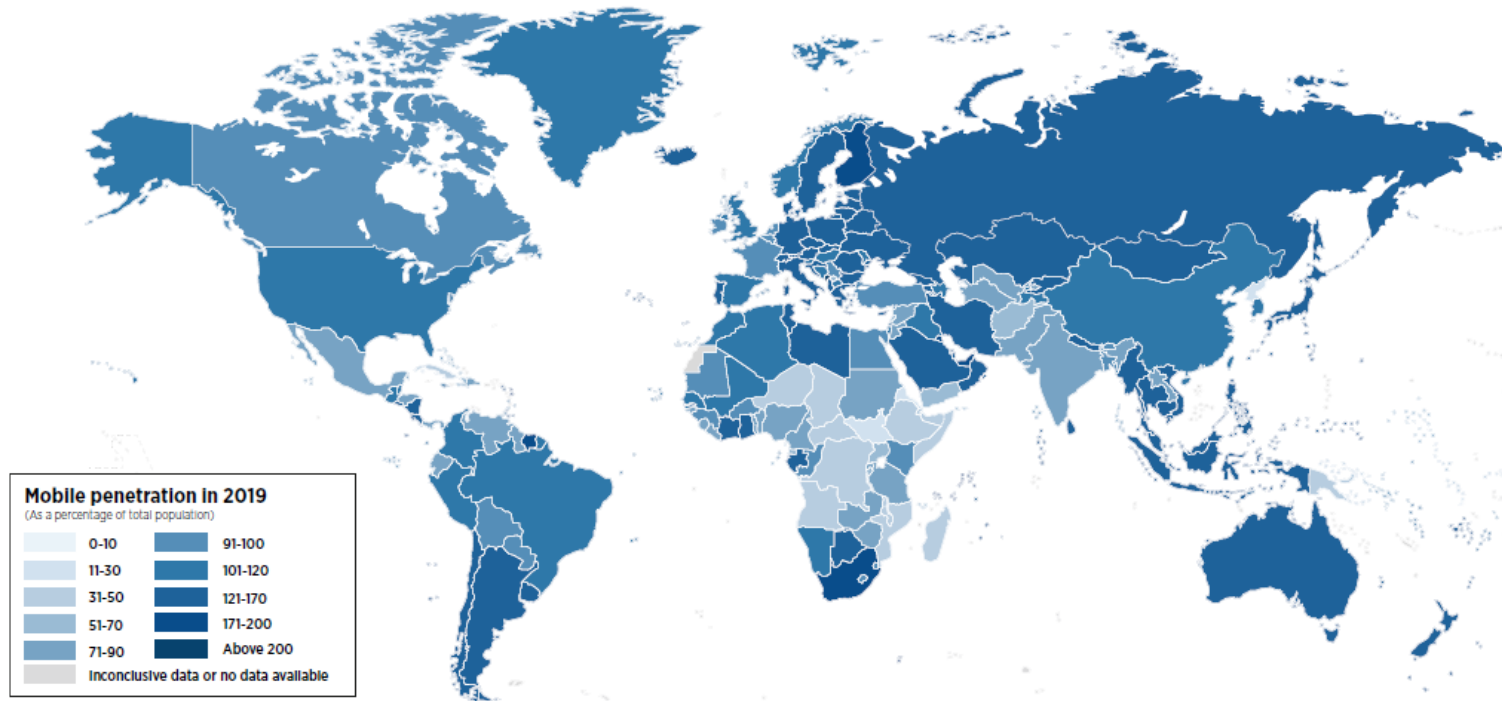
**Figure 1 : Unique Mobile Subscribers as a percentage of total population**



Source: GSMA Report March 2020<sup>17</sup>

**Figure 2: Aggregate Mobile Subscribers as a percentage of total population**

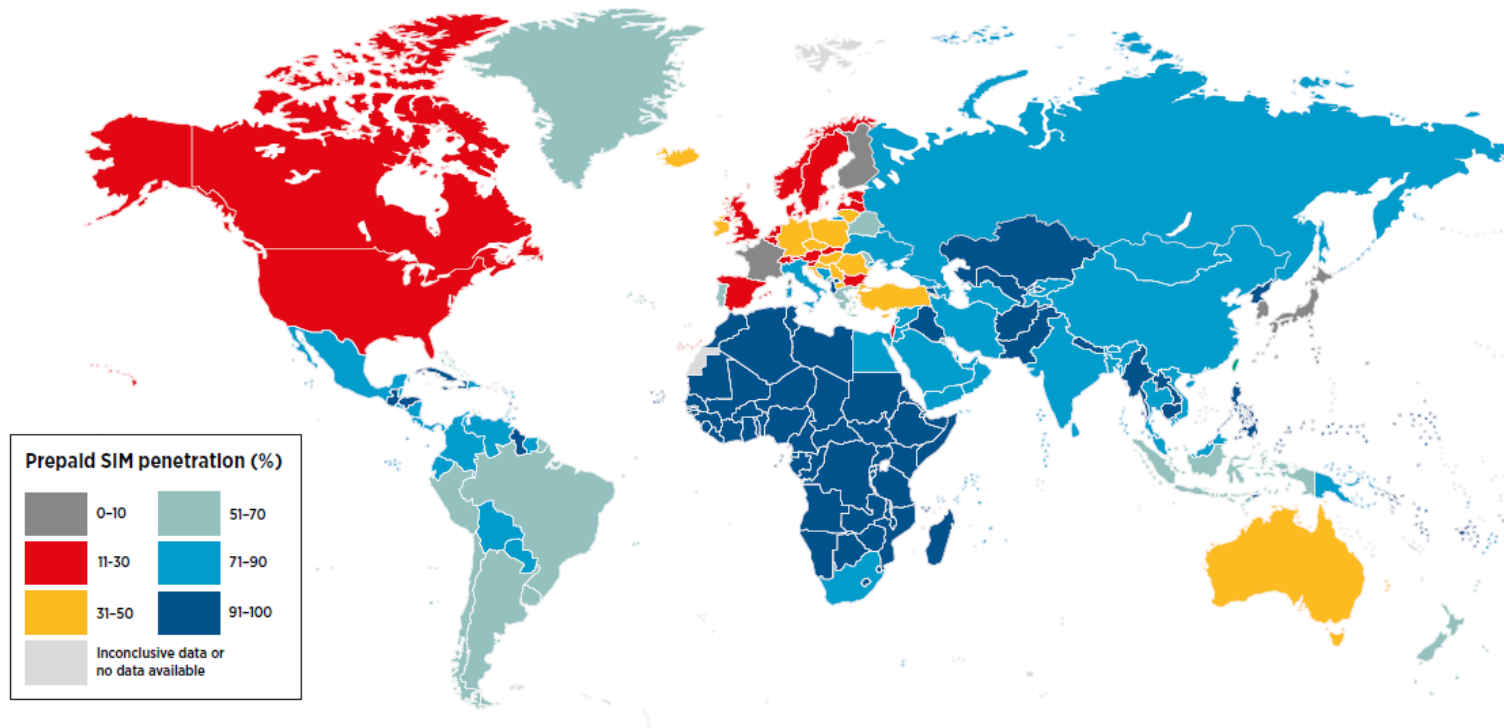
Aggregate mobile connections as a proportion of total population (2019)



Source: GSMA Report March 2020<sup>17</sup>

**Figure 3: Share of Prepaid Connections as a percentage of total mobile subscriptions**

**Share of prepaid connections as a percentage of total mobile subscriptions**



Source: GSMA Report March 2020<sup>17</sup>

2.0.2 In 2019, mobile technologies and services generated \$4.1 trillion of economic value added (4.7% of GDP) globally. This figure will approach \$5 trillion (4.9% of GDP) by 2024 as countries increasingly benefit from the improvements in productivity and efficiency brought about by increased take-up of mobile services. Further ahead, 5G technologies are expected to contribute \$2.2 trillion to the global economy between 2024 and 2034<sup>16</sup>.

2.0.3 In 2019, 4G became the dominant mobile technology. across the world with over 4 billion connections, accounting for 52% of total connections (excluding licensed cellular IoT). 4G connections will continue to grow for the next few years, peaking at just under 60% of global connections by 2023. Meanwhile, 5G is gaining pace: it is now live in 24 markets. By 2025, 5G will account for 20% of global connections, with take-up particularly strong across developed Asia, North America and Europe<sup>16</sup>.

## **2.1 Approaches Being Followed Worldwide for Addressing Security Concerns in Telecom Sector**

2.1.1 Most Governments across the world introduce mandatory SIM registration to address concerns over national security and criminal behaviour. In these countries, security services see SIM registration as a tool in their fight against terrorism and organised crime. However, this approach is not universal<sup>18</sup>.

- 2.1.2 There are also a number of countries that have no mandatory registration, choosing to address security concerns without requiring all customers to prove their identity to register for a mobile phone service<sup>18</sup>.
- 2.1.3 In some markets, mainly in Latin America, consumers are required to register their mobile handset's (IMEI) number, which may not always be registered against the specific consumer's mobile phone number (SIM). The regulatory focus in these markets is on addressing handset theft rather than the use of the phone for criminal activity by a named individual<sup>18</sup>.
- 2.1.4 In other markets, SIM registration has also been seen as a way to address antisocial behaviour, to reduce SPAM, to provide age verification and to help address mobile fraud. The requirements imposed on operators and the processes and solutions implemented in countries choosing to adopt mandatory SIM registration reflect these different priorities<sup>18</sup>.

## **2.2 Countries with Mandatory SIM Registration Policies**

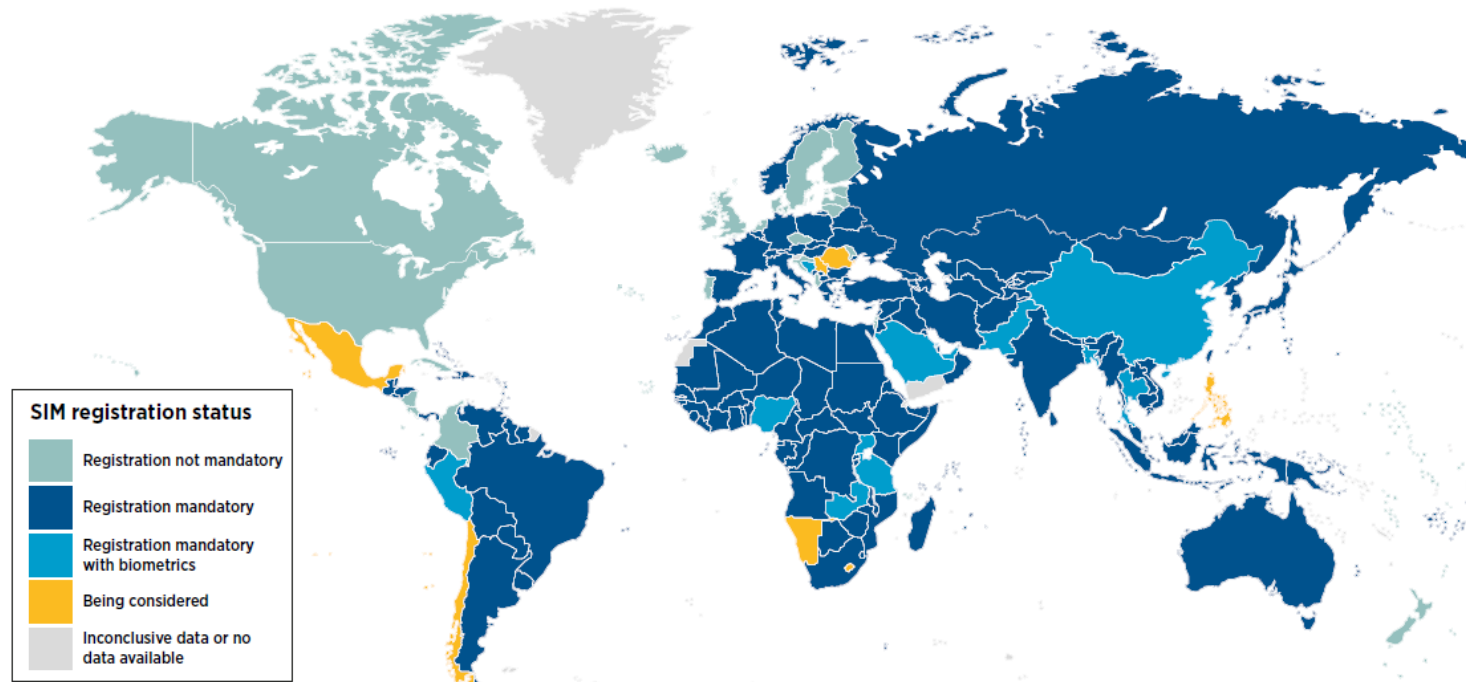
- 2.2.1 Mandatory SIM registration is a policy requiring users to provide personal information such as their name, national identification number, address and proof of identity credentials in order to register for or activate a prepaid SIM card. As a standard practice, existing users who fail to register their SIMs within a government-mandated time-period face network disconnection, resulting in loss of access to mobile services. As of January 2020, GSMA

research found that the governments of 155 countries mandate SIM registration policies<sup>17</sup>.

2.2.2 In some circumstances, governments require Mobile Network Operators (MNOs) to capture a photograph, fingerprints, and other biometric attributes of users in order to complete SIM registration. Eight per cent of countries require mobile operators to use biometric authentication processes when registering their prepaid SIM customers. In a few countries, MNOs are proactively introducing biometric authentication processes in anticipation of the government mandating this<sup>17</sup>.

**Figure 4: Status of SIM Registration Policies**

**Status of SIM registration policies (2020)**



Source: GSMA Report March 2020<sup>17</sup>



## **2.3 SIM Registration Implementation Models**

2.3.1 While, 155 countries require individuals to prove their identity in order to register and/or activate their prepaid SIM cards, governments take different approaches to implementing SIM registration policies. GSMA has grouped these approaches into the following three categories<sup>17</sup>:

### **(a) Capture and Store**

MNOs are required to capture and keep a record of a set of personal information about the SIM user. The required information varies from jurisdiction to jurisdiction. As of January 2020, about 81 per cent of the countries (126 of the 155) mandating SIM registration follow the capture and store approach.

### **(b) Capture and Share**

MNOs are required to proactively capture and share the SIM user's personal information with the government or regulator, rather than upon demand. As of January 2020, six per cent of the countries (10 of the 155) mandating SIM registration follow this approach.

### **(c) Capture and Validate**

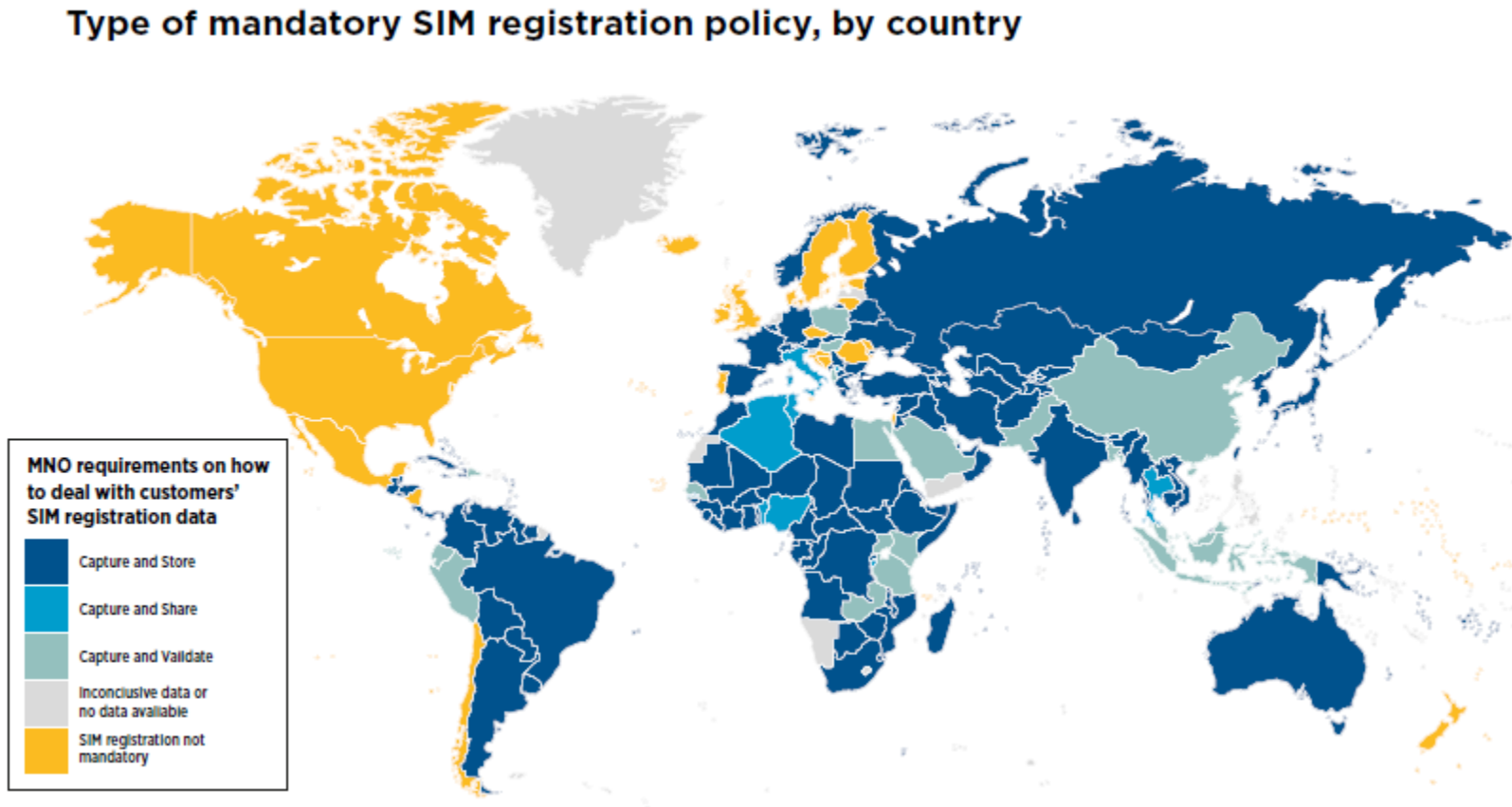
MNOs are required and enabled to validate their customers' identification credentials against a central government database (usually maintained by a Government Authority or regulator) or against a credential held by the customer (such as a chip-based smart ID card). As of January 2020, twelve per cent of countries (19 of the 155) who implement SIM registration allow mobile network providers to verify customers' identification credentials against an approved government database or credential to facilitate the validation process.

2.3.2 In countries where governments do not have credible databases against which mobile operators could conduct identity verification, the approach to proof of identity varies. For example, in some countries an attestation letter from their employers or village elders, as in the case of Nigeria, are acceptable forms of identification for SIM registration. However, such approaches are increasingly being phased out as they are perceived to be less robust and leave room for identity theft. An increasing number of governments, particularly in Sub-Saharan Africa, are seeking to establish comprehensive digital identification systems as part of their digital transformation strategies, seeking to achieve more robust identity verification when citizens and consumers attempt to access a suit of digital or electronic services (online or offline)<sup>17</sup>.

## **2.4 Alternative to Registration Solutions (Status in Developed Countries like USA, UK and Mexico)**

In these countries, SIM registration is not mandated. They follow other alternative processes for tackling the security concerns. The alternative processes used by security agencies in such countries are usually addressed by lawful interception of communications capabilities. These capabilities allow the real time monitoring of communication in such countries by the security agencies. Further, they are also allowed to access the past records or even the recorded past records. Mexico once had mandatory SIM registration but later on it repealed its mandatory SIM registration process called RENAUT and replaced it with Geolocalisation (geolocation) service<sup>18</sup>.

Figure 5: Type of Mandatory SIM Registration Policy, by Country



Source: GSMA Report March 2020<sup>17</sup>

**2.5** Status of SIM Registration Policies followed by all the countries of the world for issuance of SIM cards, particularly pre-paid SIM cards, is provided in Annexure-I.

## **2.6 Data Protections and Privacy Frameworks**

2.6.1 A research conducted by GSMA<sup>17</sup> showed that those in markets with legal frameworks around privacy and data protection feel more informed, supported, or confident in managing privacy rather than increasing trust in systems. It also showed that overall the appetite to access identity-linked services is universally high, regardless of the presence of legal frameworks, particularly if a clear benefit to consumers is perceived and the service is provided by a sufficiently trusted entity. This research highlighted the need for MNOs to be transparent with regards to how consumers data is used, clearly articulate how identity-linked services can tangibly benefit consumers, and consider ways to build and retain consumers' trust<sup>17</sup>.

2.6.2 Across the world, a significant number of countries still lack a data protection/privacy framework. Globally, the GSMA found only 59 per cent of countries mandating SIM registration have a Privacy and/or Data Protection framework in place of the countries mandating SIM registration<sup>17</sup>:

- In Africa 16 countries are without a privacy or data protection framework in place while six more are actively considering and five

have expressed their intent to introduce a data protection framework, but they have not entered into force yet.

- In Asia and the Pacific, 19 countries are without a privacy or data protection framework while six are actively considering it and one has expressed their intent to introduce a data protection law, but it has not entered into force yet.
- In Central and South America, nine countries are without a privacy or data protection framework while six are actively considering it and four have expressed their intent to introduce a data protection framework, but they have not entered into force yet.
- In Europe, one country is actively considering the implementation of a privacy or data protection framework and one has expressed their intent to introduce a data protection framework, but it has not entered into force yet.

2.6.3 Status of Data Protection and Privacy followed by all the countries of the world are provided in Annexure-I.

## **2.7 Mandatory SIM Registration Solutions**

2.7.1 Broadly, following two types of approaches are followed by different nations for SIM registration<sup>18</sup>:

(a) Verified Registration Solutions.

(b) Non-Verified Registration Solutions

### **2.7.2 Verified Registration Solutions**

2.7.2.1 The main advantage of having a solution with verification is that it is the most effective solution and is least likely to suffer from issues of identity fraud.

2.7.2.2 Where there is a national identity register and it is possible for mobile operators to check a person's details against this register, a verification check can be added to the registration process. The check confirms that the identity number and the personal details given by the mobile user at the point of registration correspond to the details on the national identity register<sup>18</sup>.

2.7.2.3 Real-time verification against a national identity register provides the most comprehensive mandatory mobile registration solution. This gives the government and the operator a high degree of confidence that the details presented by the mobile user during registration are correct and the person is who they say they are. The main advantages of this process are<sup>18</sup>:

- Verification ‘assures’ the identity of the registered user
- Least likely to suffer from identity fraud or compliance abuse
- Identity can be used for KYC on other services
- Reduces the risk to operators of unintentional compliance failures
- Only ‘authentication’ data needs to be stored and not identity data reducing the risk of privacy and identity fraud issues

### 2.7.3 **Non-Verified Registration Solutions**

2.7.3.1 In the majority of cases a variety of different identity documents are used to provide a proof of identity during the registration process. Legal registers and identity documents include birth certificates, passports and national identity cards, providing individuals with a proof of identity. Functional registries support specific services and include driving licences, voter rolls, health records, student cards and can include private sector ‘identity’ registers. Which of these forms of ID are appropriate to validate identity for SIM registration will depend on the market. In some markets driver licenses have a photograph and a home address and may be an appropriate form of ID to use for the registration, in others there may be a requirement for a secondary form of ID to be presented, especially if there is not a photograph on the license<sup>18</sup>.

2.7.3.2 The ‘authorisation’ of a person’s identity during a registration process is usually dependent on the physical presence of the person, providing one (or more than one) acceptable form of ID and completing the registration form.



Some markets allow for other verification methods. Although Identity documents are generally more widely available, this process has following advantages<sup>18</sup>:

- Lower assurance than a validated solution and harder to detect fraud
- Can require sensitive data to be stored as proof of ID (rather than an authorisation token)
- Risk of compliance failure and data quality problems, especially through independent channels

## **2.8 Telecom KYC Process in Australia**

2.8.1.1 Prior to 2013, as per KYC norms at that time, paper based was being followed in Australia for issuing pre-paid SIM cards by the mobile operators. As per these KYC norms, pre-paid mobile service providers were required to collect certain information from their customers in order to verify the identity of customers before activation of service i.e Non-Verified Registration Solution were being followed. The Audit conducted found the compliance levels to be poor<sup>179</sup>.

2.8.1.2 Australian Communications and Media Authority (ACMA) began a review of the KYC regulations. In the review, it was found that a number of changes have significantly reduced the effectiveness and efficiency of the existing KYC norms. ACMA found that existing KYC norms were put in place keeping in mind the centrally-focused business model i.e. SIM were sold by service providers only. However, now SIM were being sold

from some 30 000 third party retailers. This means that a greater range of entities are now required to verify the identity of prepaid mobile customers on behalf of the service providers<sup>19</sup>.

2.8.1.3 In the review, service providers stated that they have little scope for enforcement action against third party retailers. As identity checks are completed at the point of sale by a large number of retailers, it is therefore difficult to ensure compliance. Law enforcement and security agencies found that identity checks can be easily circumvented through identity fraud due to difficulties in validating identity documents by retail sales staff<sup>17</sup>. Further, the Parliamentary Joint Committee on the Australian Crime Commission stated that “the current requirements for recording SIM card user details are deficient and therefore represent a significant difficulty to authorities needing to accurately track suspect mobile phone users. This is a critical area needing urgent attention”<sup>19</sup>.

2.8.1.4 After the review, new KYC norms were proposed in 2013. As per these revised norms, mobile service providers were to be given access to a national online verification, managed by the Attorney- General’s Department, to perform real- time checks on the validity of selected government issued documents such as passports and Medicare cards<sup>20</sup>.

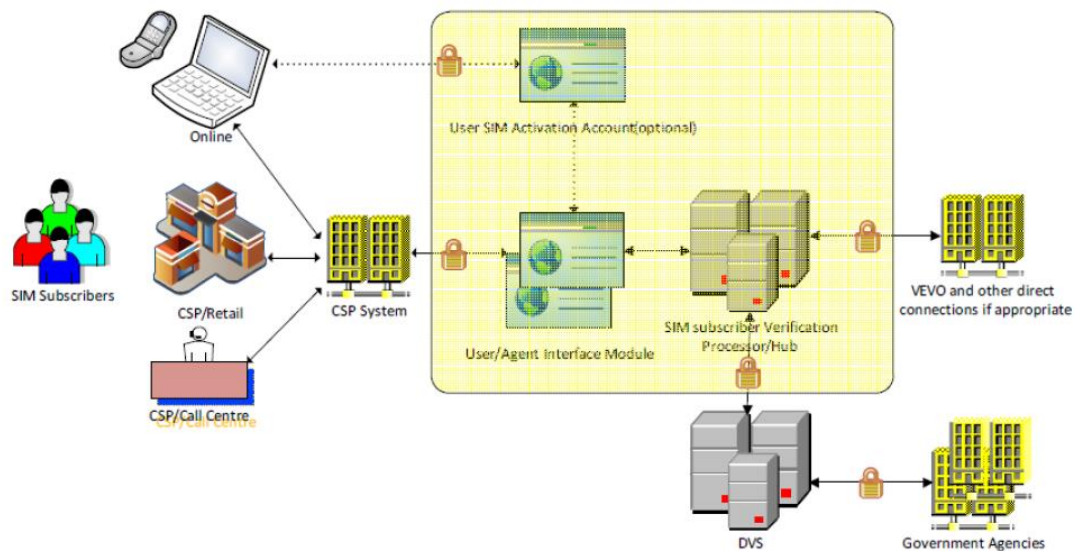
2.8.1.5 In the revised system, verification is obtained from the source database maintained by the government organisation that issued the relevant document. The system verifies the identity of information with a ‘blind

check’—accepting or rejecting it with a ‘yes’ or ‘no’ answer. Mobile service providers would not have access to issuing organisation’s database. For privacy reasons, the proposal prohibited mobile service providers from recording the identifying number of the document. Mobile Operators were allowed to use the information, during the verification process, to check that the document is authentic, accurate and up-to-date<sup>20</sup>.

2.8.1.6 Under the revised system, the details and validity of a government-issued document is verified using the National Document Verification Service (DVS) or Visa Entitlement Verification Online (VEVO). The diagram depicting the proposed system is reproduced below:

**Figure-6 Prepaid SIM verification using DVS and VEVO**

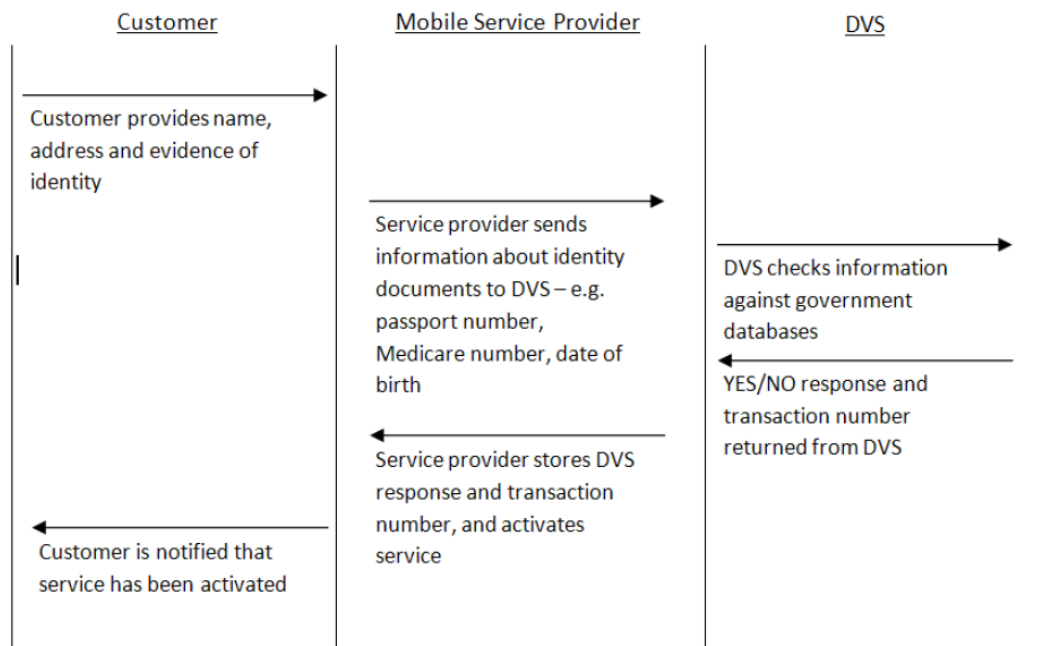
**A.1. Diagram 1: Overview of the one-step prepaid SIM verification solution using the DVS and VEVO**



**Source:** Australian Government Report<sup>19</sup>.

**Figure-7: Information Flow for Identity Verification Using DVS**

**A.2. Diagram 2: Information flow for identity verification using the DVS**



**Source:** Australian Government Report<sup>19</sup>.

2.8.1.7 The recurring identity cost get reduced from \$6.25 to \$2.15 per SIM in the above-said proposed solution of online identity verification through DVS in Australia. Further, following benefits are expected from the proposed approach<sup>19</sup>:

- (a) A higher level of confidence regarding a person's identity as information provided will be verified using trusted sources such as the DVS.
- (b) An estimated 30 000 third party retailers will no longer be required to undertake identity verification at the point of sale.

- (c) Efficiencies for service providers resulting from the use of online identity verification.
- (d) More timely and efficient retrieval of information for law enforcement and security agencies, as information will be stored electronically rather than in hardcopy.
- (e) Alignment of the identity verification process with the process to collect information for the Integrated Public Number Database, which also occurs when the SIM is activated.
- (f) Control will rest with the mobile service provider that is accountable under the Telecommunications Act.

2.8.1.8 Australian Government issued determination initially in the year 2013<sup>27</sup> and thereafter in 2017 known as “Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017”<sup>28</sup> wherein identity of the customer is online verified using “government online verification service” before activation of prepaid mobile services by the telecom service provider.

## **2.9 Identity Matching Services in Australia<sup>21</sup>**

2.9.1 In Australia, identity matching services are provided through a partnership between the Australian Government, state and territory governments, under the Intergovernmental Agreement on Identity Matching Services (2017). The range of services being provided are as under: The Identity Matching Services compare the personal information on identity document against

existing government records, such as passports, driver licences and birth certificates. They can be used to help verify the identity, and in limited cases, to identify unknown people. The services are provided through secure, online systems that operate 24 hours a day, seven days a week. Under the identity matching services, following services are provided:

#### 2.9.1.1 **Document Verification Service**

The Document Verification Service (DVS) checks whether the biographic information on your identity document matches the original record. The result will simply be 'yes' or 'no'. The DVS does not check facial images. The DVS makes it harder for people to use fake identity documents. The DVS has been operational since 2009. Both the public and private sector use the DVS.

#### 2.9.1.2 **Identity Data Sharing Service**

The identity Information held by the Commonwealth may be shared with states and territories, for use by those states and territories.

#### 2.9.1.3 **Face Verification Service**

The Face Verification Service (FVS) compares the photo against the image used on the identity documents, usually with the consent. The FVS can:

- make access to government services more convenient for customers by avoiding the need to attend a shopfront
- help victims of identity crime reclaim their identity faster
- help prevent identity theft by detecting fake or stolen documents.

The FVS can currently only be used by government agencies. In future, some local government and private sector organisations will be able use the FVS, but only with your consent.

#### 2.9.1.4 **Face Identification Service**

The Face Identification Service (FIS) compares a person's photo with other photos held in government records to identify them or detect multiple fake identities. The FIS:

- **canonly** be used by national security, law enforcement and anti-corruption agencies under limited circumstances.
- **can't** be used to investigate minor offences or conduct live facial recognition of people in public places (or what some people call mass surveillance).

Local government and private sector organisations will **not** have access to the FIS. All FIS responses will be reviewed by a person specifically trained in facial recognition and image comparison, to help protect against the

possibility of false matches—an identity decision will never be made by the technology alone.

### 2.9.2 **DVS Gateway Service Provider<sup>21</sup>**

A Document Verification Service (DVS) gateway service provider is a private organisation that:

- is conducting business in Australia or New Zealand
- has a direct connection to the DVS, either for their own use or for other users.

Gateway service providers are responsible for:

- advising the Department of Home Affairs of new applicants and reviewing applicants against the access policies
- sending match requests and match results to and from the DVS for business and government users
- making sure business and government users meet the terms and conditions of use.

\*\*\*\*\*



## Chapter-3

### KYC norms in Telecom Sector in India

#### 3.0 Brief Background of Telecom Sector in India

3.0.1 India's telecommunication network is the second largest in the world by number of telephone users (both fixed and mobile phone) with 1175.27 million subscribers as on 30<sup>th</sup> November 2020. It has one of the lowest call tariffs in the world enabled by mega telecom operators and hyper-competition among them. As on 30<sup>th</sup> November 2020, India has the world's second-largest Internet user-base with 742.06 million broadband internet subscribers in the country<sup>22</sup>.

3.0.2 Telecommunications in India began with the introduction of the telegraph. The Indian postal and telecom sectors are one of the world's oldest. In 1850, the first experimental electric telegraph line was started between Calcutta and Diamond Harbour. In 1851, it was opened for the use of the British East India Company. The Posts and Telegraphs department occupied a small corner of the Public Works Department, at that time<sup>23</sup>.

3.0.3 The construction of 4,000 miles (6,400 km) of telegraph lines was started in November 1853. These connected Kolkata (then Calcutta) and Peshawar in the north; Agra, Mumbai (then Bombay) through Sindwa Ghats, and Chennai (then Madras) in the south; Ootacamund and Bangalore. William O'Shaughnessy, who pioneered

the telegraph and telephone in India, belonged to the Public Works Department, and worked towards the development of telecom throughout this period. A separate department was opened in 1854 when telegraph facilities were opened to the public<sup>23</sup>.

3.0.4 In 1880, two telephone companies namely The Oriental Telephone Company Ltd. and The Anglo-Indian Telephone Company Ltd. approached the Government of India to establish telephone exchange in India. The permission was refused on the grounds that the establishment of telephones was a Government monopoly and that the Government itself would undertake the work. In 1881, the Government later reversed its earlier decision and a licence was granted to the Oriental Telephone Company Limited of England for opening telephone exchanges at Calcutta, Bombay, Madras and Ahmedabad and the first formal telephone service was established in the country<sup>23</sup>.

3.0.5 On 28 January 1882, Major E. Baring, Member of the Governor General of India's Council declared open the Telephone Exchanges in Calcutta, Bombay and Madras. The exchange in Calcutta named the "Central Exchange" had a total of 93 subscribers in its early stage. Later that year, Bombay also witnessed the opening of a telephone exchange<sup>23</sup>.

**Table -1**

<b>Developments and milestones<sup>23</sup></b>	
<b>Year</b>	<b>Milestone</b>
Pre-1902	Cable telegraph
1902	First wireless telegraph station established between Sagar Island and Sandhead
1907	First Central Battery of telephones introduced in Kanpur
1913–1914	First Automatic Exchange installed in Shimla
1927	Radio-telegraph system between the UK and India, with Imperial Wireless Chain beam stations at Khadki and Daund. Inaugurated by Lord Irwin on 23 July by exchanging greetings with King George V.
1933	Radiotelephone system inaugurated between the UK and India
1947	First Electronics & Telecommunications Engineering department started in India at the Government Engineering College, Jabalpur
1953 – 12	channel carrier system introduced
1960	First subscriber trunk dialling route commissioned between Lucknow and Kanpur
1975	First PCM system commissioned between Mumbai City and Andheri telephone exchanges
1976	First digital microwave junction

1979	First optical fibre system for local junction commissioned at Pune
1980	First satellite earth station for domestic communications established at Sikandarabad, U.P.
1983	First analogue Stored Programme Control exchange for trunk lines commissioned at Mumbai
1984	C-DOT established for indigenous development and production of digital exchanges
1995	First mobile telephone service started on non-commercial basis on 15 August 1995 in Delhi
1995	Internet Introduced in India starting with Laxmi Nagar, Delhi 15 August 1995

### **3.1 Evolution of Telecom KYC Norms in the Country**

3.1.1 Prior to advent of mobile services, fixed telephone services were provided by Government of India through Department of Telecommunications. In case of fixed line telephone service, bills were sent at the premises of the customers through posts. In this manner, customers premises were verified and traceability of the customer was ensured.

3.1.2 However, after the launch of mobile services around 1995-95 (as per 2004 policy of the Government) , particularly pre-paid one, the issue of KYC got more relevant. In case of pre-paid mobile services, no bill is sent at the customer premises and therefore, traceability of the customer remain an

issue. Keeping this aspect in mind and taking into security considerations, Government of India started to prescribe the KYC norms for Telecom Service Providers before enrolling them as customers. A large number of instructions were issued by Department of Telecommunications being dated 11.7.1996, 18.12.1998, 12.7.2000, 31.7.2000, 27.2.2001, 22.11.2001, 26.4.2002, 7.5.2002, 24.7.2002, 16.9.2002, 14.5.2003, 26.3.2003, 16.4.2004, 26.4.2004 etc<sup>24</sup>.

- 3.1.3 The relevant portion of the instructions dated 12 July 2000 issued by Department of Telecommunications for KYC of Cellular Mobile Telephone Service (CMTS) is reproduced below for ready reference:

*“The verification of identity of cellular subscribers is an important security requirement. Accordingly, it is required that in order to establish subscriber’s identity the relevant performae is filled up by the subscribers before providing the service.*

*2. Two performae are enclosed for this purpose – one for regular (post paid) subscribers and other for the pre-paid/ cash cards subscribers of CMTS.”*

- 3.1.4 Instructions were reviewed and fresh KYC instructions issued by Department of Telecommunications vide letter dated 29<sup>th</sup> December, 2004 (Annexure-2) regarding verification of identity of subscribers. The relevant portion of these instructions is reproduced for ready reference:

“2. It is come to the notice of the licensor that in many cases SIM cards/connections are being sold without proper verification of identity proof. The dealers of tie licence operator are either selling SIM cards without proper verification of identity of subscribers' bonafide to persons who furnishes falls addresses and forged documents or in some cases do not even ask for documents specified for verification of identity of the subscriber. The relevant proforma as annexed should be filled/taken duly filled before providing the mobile telephone service to any customer (Annexure I & II). All the operators can use these proformas with the mentioned columns. However, the operators may supplement [and not substitute] this proforma in accordance with their business considerations.

3. It is again emphasized that sale of SIM cards / connections without proper identity verification is a matter of concern and has serious security implications, a procedure needs to be evolved to ensure that SIM cards are not sold without proper identity verification. Also, it is emphasized to cross check the addresses of all the existing subscribers and it is felt that the service providers are already doing this exercise. In view of the above, it needs to be ensured by the service providers that there should not be any working number in their network without proper address of the subscriber. Further, it will be the responsibility of the licensee to maintain the records of the identity of their customers and produce the same on requisition. Therefore, necessary arrangements for

*obtaining the necessary records from the franchisees in a foolproof manner so as not to leave out even a single user of the service, should be made.”*

3.1.5 Government of India, vide instructions dated 22.11.2006<sup>25</sup> inter-alia prescribed imposition of a financial penalty of minimum Rs. 1000 per violation of subscriber number verification (KYC) on the telecom licensees apart from immediate disconnection of the subscriber number by the licensee. The relevant portion of the said instructions is reproduced below for ready reference:

*“3. The Licensees shall ensure that:*

- (i) The authorised person at the point of sale shall record in the application form that he has seen the subscriber and verified his documents with the original. In this regard licensee shall ensure that the point of sale is suitably advised of his responsibilities and consequent liabilities in the matter;*
- (ii) The connections are activated only after the requirement of filling up of customer acquisition form and copies of documentary proof as per requirement have been fulfilled by the customer; for this purpose, the licensee company's authorized representative (who is directly accountable to the licensee company) shall verify that all the documentary requirement has been completed before activating the SIM card,*
- (iii) Pre-activated SIM cards are not to be sold in the market.*

*4. The Licensee shall -also ensure that the information about the subscriber is entered in to Licensee's database correctly based on the information in Customer Acquisition Forms (CAF) / Subscriber Acquisition Forms (SAF) and supporting documents. For this purpose, the Licensee shall nominate separate officials, who shall be responsible for the process of entry of subscriber information in the database, cross-checking of information from the database with that from each and every original CAF/SAF & documents. If any discrepancy is found at any stage, the mobile connection shall be de-activated immediately and in any case not later than 72 hours. Observations made by each nominated official for the above activities shall be kept in record for scrutiny at a later date.*

5. *The above guidelines shall be followed by all the Licensee companies scrupulously with immediate effect and any deviation from the above procedure shall be treated as breach of terms and conditions of the License Agreement.*

6. *For ensuring that the complete subscriber information is available with all the service providers and the same is duly verified, it has also been decided that each . Licensee shall take up re-verification of the existing subscribers on priority and ensure that the re-verification of the existing subscribers is completed by 31<sup>st</sup> March 2007. By re-verification, it is meant that there shall be 100% check of CAF/SAF, documentary proof of identity and documentary proof of address and it would be ensured that the subscriber information available in service provider's database matches with that in CAF/SAF and enclosed documents. Further, the Licensee company shall cross-verify the information from the actual user by calling the respective subscriber. There shall not be any connection working after 31<sup>st</sup> March 2007 in the Licensee's network without having above subscriber information duly verified.*

7. *As already mentioned above, the corrective measure of re-verification of subscribers is for the purpose of ensuring that the complete subscriber information is available with all the service providers and the same is duly verified and this may not be construed as any exemption or relaxation from fulfilling the license conditions.*

8. *After 31<sup>st</sup> March 2007, if any subscriber number is found working without proper verification, a minimum penalty of Rs. 1000 per violation of subscriber number verification shall be levied on the licensee apart from immediate disconnection of the subscriber number by the licensee.*

9. *In addition the Licensor reserves the right to take suitable action also in all cases where the service providers might have failed to comply with the existing instructions of 100% verification of subscribers in accordance with the provisions of License Agreement.”*

3.1.6 Department of Telecommunications, vide letter dated 24<sup>th</sup> December, 2008<sup>25</sup> inter-alia prescribed graded penalty for violation of License Agreement in respect of subscriber verification cases i.e. violation of KYC norms by Telecom Licensees. The relevant portion of the said instructions is reproduced below for ready reference:



*“Subject : Scheme of Financial Penalty for violation of terms and conditions of the License Agreement in respect of Subscriber verification failure cases.*

*This has reference to CMTS/ UAS License condition(s), which inter-alia provides that:*

*“.....The licensee shall ensure adequate verification of each and every customer before enrolling him as a subscriber; instructions issued by the licensor in this regard from time to time shall be scrupulously followed... g; and*

*“... The Licensor may also impose a financial penalty not exceeding Re. 50 crores for violation of terms and conditions of licence agreement... and*

*the instructions issued from time to time regarding subscriber verification including the provision that after March, 2007, if any number is found working without proper verification, minimum penalty of Rs. 1000 per violation of subscriber number verification shall be levied on the licensee apart from immediate disconnection of the subscriber number by the licensee.*

*2. In spite of the above provisions/ instructions regarding subscriber verification, it has been observed from the report of TERM Cells that the service providers are not complying with the requirement of subscriber verification fully. Accordingly, the matter has been reviewed and it has been decided to introduce a scheme of penalty for subscriber verification failure cases at graded scales w.e.f. 1<sup>st</sup> April 2009, so that it works as a deterrent. The graded scales are based on correct subscriber verification percentage i.e. correct subscriber verification percentage of a service provider in any service area will be ascertained and based on this percentage, a financial penalty of corresponding amount for each detected case of unverified subscriber shall be levied on account of violation in respect of subscriber verification failures from the service provider in that service area, According to the said scheme, the correct subscriber verification percentage vis-à-vis financial penalty per unverified subscriber shall be as per table below'*

<i>Correct Subscriber Verification Percentage in a Service Area</i>	<i>Amount of financial penalty per unverified subscriber</i>
<i>Above 95%</i>	<i>Rs. 1000/=</i>
<i>90%- 95%</i>	<i>Rs. 5000/=</i>

85% - 90%	Rs. 10000/=
80% - 85%	Rs. 20000/-
Below 80%	Rs. 50000/-

3. *The CMTS/ UAS licensees may tighten their subscriber verification process accordingly so as to avoid imposition of financial penalty for violation of terms and conditions of License Agreement and instructions regarding subscriber verification.”*

3.1.7 Government of India prescribed the norms for lodging of complaint/ FIR for dealing with the use of forged document for obtaining the mobile connections by the subscribers. Relevant portion of the instructions dated 23<sup>th</sup> March, 2009<sup>25</sup> issued by the Department of Telecommunications in this regard is reproduced below for ready reference:

“2. Lodging Complaint / FIR:

*In order to deal with the issue of forged documents for obtaining mobile connections, Complaint / may be lodged with the LEA, under law of the land. It has been decided that,*

- (i) In case of forgery of documents detected, Complaint / FIR shall be lodged by the Franchisee/Service Provider against the customer. .*
- (ii) In case Franchisee fails to lodge Complaint / FIR as above, Service Provider shall lodge Complaint / FIR against the customer and franchisee.*
- (iii) In case no action is taken by Service Provider as above, the TERM Cell may lodge Complaint / FIR, including against the Service Provider.”*

3.1.8 Government of India vide instructions dated 07<sup>th</sup> October 2009<sup>25</sup> prescribed the documents to be accepted as Proof of Identity and Proof of Address for KYC of mobile subscribers in telecom sector. The details of prescribed documents are reproduced below for ready reference:

<i>For Proof of Identity (All Identity proof to have Photo)</i>	<i>For Proof of Address</i>
<i>Passport</i>	<i>Passport</i>
<i>Arms License</i>	<i>Arms License</i>
<i>Driving License</i>	<i>Driving License</i>
<i>Election Commission ID Card</i>	<i>Election Commission ID Card</i>
<i>Ration Card with Photo, for the person whose photo is affixed</i>	<i>Ration Card with address</i>
<i>CGHS/ ECHS Card</i>	<i>CGHS/ ECHS Card</i>
<i>Certificate of address having Photo issued by MP/ MLA/ Group- A Gazetted officer in letter head</i>	<i>Certificate of address having Photo issued by MP/ MLA/ Group- A Gazetted officer in letter head</i>
<i>Certificate of address with photo from Govt. recognised educational institutions (for students only)</i>	<i>Certificate of address with photo from Govt. recognised educational institutions (for students only)</i>
<i>Certificate of photo identity issued by Village Panchayat head or its equivalent authority (for rural areas)</i>	<i>Certificate of address issued by Village Panchayat head or its equivalent authority (for rural areas)</i>
<i>Income Tax PAN Card</i>	<i>Water Bill (not older than last three months)</i>
<i>Photo Credit Card</i>	<i>Telephone Bill of Fixed Line (not older than last three months)</i>
<i>Address card with photo issued by Deptt. of Posts, Govt. of India</i>	<i>Electricity Bill (not older than last three months)</i>
<i>Smart card issued by CSD, Defence/ Paramilitary</i>	<i>Income Tax Assessment Order</i>
<i>Current Passbook of Post Office/ any scheduled bank, having photo</i>	<i>Vehicle Registration Certificate</i>

<i>Photo Identity Card (of Central Govt./ PSU or State Govt./ PSU only)</i>	<i>Registered Sale/ Lease Agreement</i>
<i>Photo Identity Card issued by Govt. recognised educational institutions (for students only)</i>	<i>Address card with photo issued by Deptt. of Posts, Govt. of India</i>
<i>Cast and Domicile Certificate with photo issued by State Govt. like Assam and other states</i>	<i>Current Passbook of Post Office/ any Scheduled Bank</i>
<i>Pensioner Card having photo</i>	<i>Photo Identity Card having address (of Central Govt./ PSU or State Govt./ PSU only)</i>
<i>Freedom Fighter Card having photo</i>	<i>Credit Card statement (not older than last three months)</i>
<i>Kisan Passbook having photo</i>	<i>Cast and Domicile Certificate with address and photo issued by State Govt. like Assam and other states</i>
	<i>Pensioner Card with address</i>
	<i>Freedom Fighter Card with address</i>
	<i>Kisan Passbook with address</i>

3.1.9 A Public Interest Litigation (PIL) being Writ Petition (Civil) No. 285 of 2010 titled as Avishek Goenka vs Union Of India & Anr was filed before the Hon'ble Supreme Court attempting to highlight the grave issue of non-observance of norms/regulations/guidelines related to proper and effective subscriber verification by various service providers. It was also alleged that there is rampant flouting of norms/regulations/guidelines relating to this subject matter and there is no proper verification of the subscribers prior to selling of the pre-paid mobile connections to them. Further, it was alleged that the SIM cards are provided without any proper verification, which causes serious security threat as well as encourages malpractices in the telecom

sector. It appears that 65 per cent of all pre-paid SIM cards issued in Jammu & Kashmir and 39 per cent of all pre-paid SIM cards in Mumbai, may have been issued without verification; which means that 1 out of every 6 pre-paid SIM cards is issued without proper verification. The petitioner also averred that such unverified SIM cards are also used in terrorist attacks. Finally, the petitioner prayed that there should be strict implementation of subscriber verification guidelines, physical verification be compulsory in future and physical re-verification of existing subscriber base be conducted in a transparent manner.

- 3.1.10 During the pendency of above-said PIL, DoT filed instructions dated 14<sup>th</sup> March, 2011 before the Hon'ble Supreme Court, relating to various aspects involved in the case and specifically, on the manner of verification of new mobile subscribers (pre-paid and post-paid). These instructions, inter alia, dealt with the verification and activation of mobile connections, special guidelines for issue of mobile connections to foreigners and outstation users, bulk mobile connections, change in the name of subscriber, disconnection, lodging of complaints and even imposition of penalties. Clause 3(vii) of these instructions provided that pre-activated SIM cards are not to be sold. In case of sale of pre-activated SIM cards, a penalty of Rs. 50,000/- per such connection shall be levied upon the service provider/licensee, in addition to immediate disconnection of the mobile connection.
- 3.1.11 The Hon'ble Supreme Court was pleased to partially allow the above-said writ petition. The instructions dated 14<sup>th</sup> March, 2011 issued by DoT were

accepted by the Hon'ble Supreme Court subject to certain conditions/directions. The relevant portions of the judgment dated 27<sup>th</sup> April, 2012<sup>26</sup> delivered by the Hon'ble Court in the said matter are reproduced below for ready reference:

*“.....In this Public Interest Litigation, the petitioner has attempted to highlight the grave issue of non-observance of norms/regulations/guidelines related to proper and effective subscriber verification by various service providers. In fact, according to the petitioner, there is rampant flouting of norms/regulations/guidelines relating to this subject matter and there is no proper verification of the subscribers prior to selling of the pre-paid mobile connections to them.*

*3. .... Different random studies in relation to pre-paid Subscriber Identity Module (SIM) cards show widespread violation of guidelines for Know Your Customer (KYC) and even other common guidelines. The SIM cards are provided without any proper verification, which causes serious security threat as well as encourages malpractices in the telecom sector. It appears that 65 per cent of all pre-paid SIM cards issued in Jammu & Kashmir and 39 per cent of all pre-paid SIM cards in Mumbai, may have been issued without verification; which means that 1 out of every 6 pre-paid SIM cards is issued without proper verification. The averment is that such unverified SIM cards are also used in terrorist attacks.*

*4. This Court, in the case of State (NCT of Delhi) Vs. Navjot Sandhu alias Afsan Guru [(2005) 11 SCC 600] had, with some caution, referred to a large number of calls which had been made by terrorists from instruments containing unverified SIM cards. It is further averred by the petitioner that around 80 per cent of the pre-paid SIM cards may be purchased in pre-activated form which is in violation of the notifications issued by the DoT, dated 22.11.2006 and 23.3.2009 respectively, banning the sale of pre-activated SIM cards. Another significant fact that has been brought out in this petition is that, pre-paid SIM cards, which are the most commonly issued without verification, constitute 96 per cent of the total SIM cards sold. This indicates the seriousness of the problem as well as the security hazard that emerges from the telecom sector.*

*5. Thus, the petitioner has prayed that there should be strict implementation of subscriber verification guidelines, physical verification be compulsory in future and physical re-verification of existing subscriber base be conducted in a transparent manner. He also seeks the prevention of inflated subscriber base. On all matters in relation to these prayers, he pleads for issuance of appropriate writ, orders or directions. Upon notice, the DoT as well as the TRAI had put in appearance and placed on record the guidelines issued by the DoT, as well as the comments of TRAI, respectively.*

20. In view of our above discussion, we partially allow the writ petition. The instructions dated 14<sup>th</sup> March, 2011 issued by DoT be and hereby are accepted by the Court subject to the following conditions:

(i) We hereby direct the constitution of a Joint Expert Committee consisting of two experts from TRAI and two experts from DoT to be chaired by the Secretary, Ministry of Communications and Information Technology, Government of India.

(ii) This Committee shall discuss and resolve the issues on which TRAI in its affidavit has given opinion divergent to that declared by DoT in its instructions dated 14<sup>th</sup> March, 2011. Following are the points of divergence that require examination by the Joint Expert Committee :

(a) Whether re-verification should be undertaken by the service provider/licensee, the DoT itself or any other central body?

(b) Is there any need for enhancing the penalty for violating the instructions/guidelines including sale of pre-activated SIM cards?

(c) Whether delivery of SIM cards may be made by post? Which is the best mode of delivery of SIM cards to provide due verification of identity and address of a subscriber?

(d) Which of the application forms, i.e., the existing one or the one now suggested by TRAI should be adopted as universal application form for purchase of a SIM card?

(e) In absence of Unique ID card, whether updating of subscriber details should be the burden of the licensee personally or could it be permitted to be carried out through an authorized representative of the licensee?

(f) In the interest of national security and the public interest, whether the database of all registered subscribers should be maintained by DoT or by the licensee and how soon the same may be made accessible to the security agencies in accordance with law?

(iii) The above notified Committee shall resolve the above specified issues and any other ancillary issue arising therefrom and make its recommendations known to the DoT within three months from today.

(iv) The DoT shall take into consideration the recommendations of the Joint Expert Committee. The instructions issued by DoT dated 14<sup>th</sup> March, 2011 shall thereupon be amended, modified, altered, added to or substituted accordingly. They shall then become operative in law and binding upon all concerned.

*(v) Composite instructions, so formulated, shall positively be issued by the DoT within 15 weeks from today and report of compliance submitted to the Registry of this Court.”*

3.1.12 In compliance of above-said Hon’ble Supreme Court judgment dated 27.04.2012, Department of Telecommunications issued detailed instructions dated 09.08.2012<sup>25</sup> on verification of new mobile subscribers. The broad features of these instructions are as under:

- (i) A unique number to be assigned to every Customer Acquisition Form (CAF) before activation of SIM.
- (ii) Authorized person on Point of Sale to record in CAF that he has seen the subscriber and matched the photograph attached on the CAF with the subscriber and verified his copies of documents of proof of address and proof of identity attached with the CAF.
- (iii) After the activation of SIM, subscriber shall be tele-verified.
- (iv) Pre activated SIM not to be sold. In case of sale of pre-activated SIM, penalty of Rs. 50,000/- per such connection to be imposed in addition to immediate disconnection of SIM.
- (v) In case of use of forged documents for obtaining SIM cards, FIR to be lodged.

3.1.13 Department of Telecommunications issued instructions on 14.01.2011 for taking “Aadhaar”, the unique identification number issued by Unique Identification Authority of India (UIDAI) as valid Proof of Address and Proof of Identity for issuing telephone connections.



- 3.1.14 Department of Telecommunications on 16.0.2014<sup>25</sup> issued instructions to Telecom Service Providers for collecting Aadhaar Number of all the customers alongwith Customer Acquisition Form (CAF) and store the same in their database.
- 3.1.15 Department of Telecommunications on 16.08.2016<sup>25</sup> launched Aadhaar e-KYC (Electronic Know Your Customer) service for issuing mobile connections to the subscribers as an alternative process. In e-KYC service, customer online authorises UIDAI using his/ her Aadhaar number and biometrics to transfer his/ her demographic details (name, address, date of birth and gender) to the Telecom Service Provider at the time of issuance of SIM. This data is stored by Telecom Service Providers in their database.
- 3.1.16 Department of Telecommunications issued circular dated 23<sup>rd</sup> March 2017<sup>25</sup> mandatory verification of all the existing mobile customers through e-KYC process.
- 3.1.17 A nine Judge constitutional bench in Justice K.S.Puttaswamy (Retd) Vs Union of India vide judgment dated 24<sup>th</sup> August 2017<sup>26</sup> determined that right to privacy is a part of fundamental rights which can be traced to Articles 14, 19 and 21 of the Constitution of India.
- 3.1.18 Hon'ble Supreme Court rendered judgment dated 26.09.2018 in Writ Petition No. 494 of 2012 titled as Justice K.S. Puttaswamy (Retd.) and Another Vs

Union of India and Others<sup>26</sup> on various issues. Hon'ble Supreme Court declared the circular dated 23<sup>rd</sup> March 2017 issued by Department of Telecommunication for mandatory linking of mobile number with Aadhaar unconstitutional. The relevant portion of the said judgement on some of the issues is reproduced below for ready reference:

**“Linking of Mobile Number with Aadhaar**

437) *By a Circular dated March 23, 2017, the Department of Telecommunications has directed that all licensees shall reverify the existing mobile subscribers (pre-paid and post-paid) through Aadhaar based e-KYC process. In fine, it amounts to mandatory linking of mobile connections with Aadhaar, which requirement is not only in respect of those individuals who would be becoming mobile subscribers, but applies to existing subscribers as well.*

438) *It was the submission of the petitioners that such a linking of the SIM card with Aadhaar number violates their right to privacy. It is argued that since it is a fundamental right, the restrictions/curb thereupon in the form of said linking does not satisfy the tests laid down in K.S. Puttaswamy inasmuch as it is neither backed by any law nor it serves any legitimate state aim nor does it meet the requirement of proportionality test.*

439) *At the outset, it may be mentioned that the respondents have not been able to show any statutory provision which permits the respondents to issue such a circular. It is administrative in nature. The respondents have, however, tried to justify the same on the ground that there have been numerous instances where non-verification of SIM cards have posed serious security threats. Having regard to the same, this Court had given direction in Lokniti Foundation v. Union of India & Anr for the linking of SIM card with Aadhaar and it is pursuant to those directions that the Telecom Regulatory Authority of India (TRAI) recommended this step. Therefore, as per the respondents, Circular dated March 23, 2017 is the outcome of the aforesaid directions and recommendations which should be treated as backing of law. According to them, direction of this Court is a law under Article 141 of the Constitution. In addition, it is also argued that since Section 4 of the Indian Telegraph Act, 1885 empowers the Central Government to issue licenses for establishing, maintaining and working telegraphs, it is within the power of the Central Government to grant such licenses with condition and, therefore, Circular dated March 23, 2017 may be read as condition for grant of licenses. On this premise, attempt is to show*

*that the Circular is issued in exercise of the powers contained in Section 4 of the Indian Telegraph Act, 1885 which is the force of law.*

440) *In order to appreciate the respondents' contentions, we reproduce the relevant portion of Circular dated March 23, 2017, which reads as under:*

*"Hon'ble Supreme Court, in its order dated 06.02.2017 passed in Writ Petition (C) No. 607/2016 filed by Lokniti Foundation v/s Union of India, while taking into cognizance of "Aadhaar based e-KYC process for issuing new telephone connection" issued by the Department, has inter alia observed that "an effective process has been evolved to ensure identity verification, as well as, the addresses of all mobile phone subscribers for new subscribers. In the near future, and more particularly, within one year from today, a similar verification will be completed, in case of existing subscribers." This amounts to a direction which is to be completed within a time frame of one year.*

2. *A meeting was held on 13.02.2017 in the Department with the telecom industry wherein UIDAI, TRAI and PMO representatives also participated to discuss the way forward to implement the directions of Hon'ble Supreme Court. Detailed discussions and deliberations were held in the meeting. The suggestions received from the industry have been examined in the Department.*

3. *Accordingly, after taking into consideration the discussions held in the meeting and suggestions received from telecom industry, the undersigned is directed to convey the approval of competent authority that all Licensees shall re-verify all existing mobile subscribers (prepaid and postpaid) through Aadhaar based e-KYC process as mentioned in this office letter No. 800-29/2010VAS dated 16.08.2016. The instructions mentioned in subsequent paragraphs shall be strictly followed while carrying out the re-verification exercise."*

441) *In the first instance, it may be noticed that reference is made to the judgment of this Court in Lokniti Foundation which has prompted the Ministry of Communications to issue this circular. Paragraph 1 of the Circular itself states that the observations of the Court in Lokniti Foundation amount to a direction. Thus, the Circular is not issued in exercise of powers under Section 4 of the Indian Telegraph Act, 1885 (though that itself would be debatable as to whether Section 4 gives such a power at all). Insofar as observations of this Court in that case are concerned, it is clear that in the said brief order, this Court did not go*

*into the issue as to whether linking of SIM card with Aadhaar would be violate of privacy rights of the citizens. In that petition filed as a Public Interest Litigation, a prayer was made to the effect that identity of each subscriber and also the numbers should be verified so that unidentified and unverified subscribers are not allowed to misuse mobile numbers. In response, the Union of India had filed the counter affidavit bringing to the notice of the Court that the Department had launched Aadhaar based e-KYC for issuing mobile connections. Based on this statement, orders were passed by this Court. Lis, which is the subject matter of instant petitions, was not raised in the said case. Obviously, the Court did not deliberate on the aspects of necessity of such a provision in the light of right to privacy. It was a case where both the sides were at ad idem. In the absence of any such issue or discussion thereupon, such a case cannot be treated as precedent and as a corollary it cannot be termed as 'law' within the meaning of Article 13 or Article 141 of the Constitution. Moreover, we are unable to read the order in Lokniti Foundation as a direction of the Court. It simply disposed of the petition after recording the submission of the Union of India to the effect that the grievance of the petitioner therein stood redressed by evolving the procedure of linking. On that the Court simply observed that undertaking given to this Court will be seriously taken and given effect to. No doubt, the Central Government, as a licensor, can impose conditions while granting licenses under Section 4 of the Indian Telegraph Act, 1885. However, such directions/conditions have to be legally valid. When it affects the rights of the third parties (like the petitioners herein who are not party to the licenses granted by the Government to the Telecom Service Providers) they have a right to challenge such directions. Here, the case made out by the petitioners is that it infringes their right to privacy.*

442) *We are of the opinion that not only such a circular lacks backing of a law, it fails to meet the requirement of proportionality as well. It does not meet 'necessity stage' and 'balancing stage' tests to check the primary menace which is in the mind of the respondent authorities. There can be other appropriate laws and less intrusive alternatives. For the misuse of such SIM cards by a handful of persons, the entire population cannot be subjected to intrusion into their private lives. It also impinges upon the voluntary nature of the Aadhaar scheme. We find it to be disproportionate and unreasonable state compulsion. It is to be borne in mind that every individual/resident subscribing to a SIM card does not enjoy the subsidy benefit or services mentioned in Section 7 of the Act.*

*We, therefore, have no hesitation in declaring the Circular dated March 23, 2017 as unconstitutional."*

3.1.19 In compliance of above-said Hon'ble Supreme Court judgment dated 26.09.2018 setting aside the circular dated 23<sup>th</sup> March, 2017, Department of Telecommunications issued instructions on 26<sup>th</sup> October 2018<sup>25</sup> for discontinuation of Aadhaar e-KYC service for issuing new mobile connections and re-verification of existing mobile connections.

3.1.20 After discontinuation of Aadhaar e-KYC service, Department of Telecommunication issued instructions dated 03<sup>rd</sup> April 2019<sup>25</sup> for Digital KYC process (DKYC) for issuing new mobile connections to subscribers. This process inter-alia has the following features:

- (i) Process to be done by Point of Sale through APP only.
- (ii) Customer has to bring original Proof of Identity and Proof of Address while visiting Point of Sale for new mobile connections.
- (iii) Live Photograph of customer is to be taken by PoS and the same shall to be embedded in CAF.
- (iv) System Application of Licensee shall put a water mark in readable form having CAF number, GPS coordinates, POS name, unique POS Code and Date (DD:MM:YYYY) & time stamp (HH:MM:SS) on the captured live photograph of the customer.

3.1.21 After declaration of the circular dated 23<sup>rd</sup> March, 2017 unconstitutional by the Hon'ble Supreme Court vide judgement dated 26<sup>th</sup> September, 2018, Government enacted the amendment in "The Indian Telegraph Act, 1885" through 'The Aadhaar And Other Laws (Amendment) Act, 2019 No. 14 of

2019”<sup>1</sup>. Through this amendment, provisions have been made for KYC of customers in Section 4 of the Indian Telegraph Act, 1885. Prior to this, KYC process in telecom was being enforced through Administrative Circulars without any Statutory backing. The relevant parts of “The Aadhaar And Other Laws (Amendment) Act, 2019 No. 14 of 2019” regarding amendment in Indian Telegraph Act, 1885 are reproduced as under:

*“26. In section 4 of the Indian Telegraph Act, 1885, after sub-section (2), the following sub-sections shall be inserted, namely:—*

*‘(3) Any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India, shall identify any person to whom it provides its services by—*

- (a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or*
- (b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or*
- (c) use of passport issued under section 4 of the Passports Act, 1967; or*
- (d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf.*

*(4) If any person who is granted a license under the first proviso to sub-section (1) to establish, maintain or work a telegraph within any part of India is using authentication under clause (a) of sub-section (3) to identify any person to whom it provides its services, it shall make the other modes of identification under clauses (b) to (d) of sub-section (3) also available to such person.*

*(5) The use of modes of identification under sub-section (3) shall be a voluntary choice of the person who is sought to be identified and no person shall be denied any service for not having an Aadhaar number.*

*(6) If, for identification of a person, authentication under clause (a) of sub-section (3) is used, neither his core biometric information nor the Aadhaar number of the person shall be stored.*

*(7) Nothing contained in sub-sections (3), (4) and (5) shall prevent the Central Government from specifying further safeguards and conditions for compliance by any person who is granted a license under the first proviso to sub-section (1) in respect of identification of person to whom it provides its services.*

*Explanation.—The expressions “Aadhaar number” and “core biometric information” shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.’.*

3.1.22 In accordance with the above-said provisions contained in the Indian Telegraph Act, 1885, Department of Telecommunications, Ministry of Communication has issued instructions dated 29.09.2020<sup>25</sup> for use of “Aadhaar Number/ Virtual ID” e-KYC service of Unique Identity Authority of India (UIDAI) as an alternate process for issuing mobile connections. Broad features of this process put in place through instructions dated 29.09.2020 are as under:

- (a) Customer online authorises UIDAI using his/ her Aadhaar number/ Virtual ID and biometrics to transfer his/ her demographic data as in their database (name, address, date of birth and gender) alongwith his/ her photograph to the Telecom Licensee at the time of issuance of SIM. This data is stored by Telecom Service Providers in their database.
- (b) Licensee displays the Aadhaar Number/ Virtual ID in masked form at the Point of Sale terminal (POS) and ensures that the Aadhaar number/ Virtual ID of the customer/ POS agent is not stored anywhere in the system/ application/ database.
- (c) For the purpose of identification of a person, neither core biometric information nor the Aadhaar Number/ Virtual ID of the person is to be stored.
- (d) Live photograph of the customer is taken and the same is embedded in the CAF. System Application of Licensee puts a water mark in readable



form having CAF number, GPS coordinates, POS name, unique POS Code and Date (DD:MM:YYYY) & time stamp (HH:MM:SS) on the captured live photograph of the customer.

(e) Fingerprint/ iris data of customer shall nowhere be stored or displayed.

### **3.2 Current KYC Norms in Telecom Sector**

As on date, there are three KYC processes for issuing mobile connections (Details of all these three processes are submitted in earlier paragraphs) in telecom sector:

(i) First process put in place by Department of Telecommunications through instructions dated 09.08.2012<sup>25</sup> in compliance of Hon'ble Supreme Court judgment dated 27.04.2012. In this case, physical CAF is filled up by the customer. Further, copies of proof of address and proof of identity are obtained by point of sale from the customer. This is a non-verified process i.e. no-online verification of the customer is done before activation of SIM cards.

(ii) Second process known as Digital KYC process put in place by Department of Telecommunications through instructions dated 03.04.2019<sup>25</sup>. In this process, customer has to bring original Proof of Identity and Proof of Address while visiting Point of Sale for new mobile connections. Live Photograph of customer is to be taken by PoS and the same shall to be embedded in CAF. System Application of Licensee

shall put a water mark in readable form having CAF number, GPS coordinates, POS name, unique POS Code and Date & time stamp on the captured live photograph of the customer. This is also a non-verified process i.e. no-online verification of the customer is done before activation of SIM cards.

(iii) Third process known as Aadhaar eKYC process put in place by Department of Telecommunications through instructions dated 29.09.2020<sup>25</sup>. Customer online authorises UIDAI using his/ her Aadhaar number/ Virtual ID and biometrics to transfer his/ her demographic data as in their database (name, address, date of birth and gender) alongwith his/ her photograph to the Telecom Licensee at the time of issuance of SIM. This data is stored by Telecom Service Providers in their database. Live photograph of the customer is taken and the same is embedded in the CAF. System Application of Licensee puts a water mark in readable form having CAF number, GPS coordinates, POS name, unique POS Code and Date & time stamp on the captured live photograph of the customer. Aadhaar number, core biometric information or fingerprint/ iris data of customer is not stored. This is verified process i.e. customer is verified through biometrics before activation of Sim cards.

(iv) All these three processes are optional i.e. customer can avail telecom services by following either of the three processes.

(v) In case of violation of norms, prescribed penalty is to be imposed on Telecom Service Providers.

### **3.3 Data Protection and Privacy**

Right to privacy has been declared to be part of fundamental rights by the Hon'ble Supreme Court in Aadhaar case. Further, "The Data Protection Bill" was introduced by the Government in the Parliament and the same has been referred to a Joint Parliamentary Committee for detailed examination. As such, presently there is no comprehensive privacy and data protection law in the country.

### **3.4 Effectiveness of existing KYC Regulatory Norms in the Country**

3.4.1 Effectiveness of existing Know Your Customer regulatory norms in telecom sector of the Country is being examined in this document from the angle of use of fake/ forged documents and identity theft.

3.4.2 It is noted that telecom facilities are misused by miscreants for committing various types of crimes without coming into physical contact and sitting at remote locations. Miscreants find telecom services as one of the easiest mode of committing various types of crimes. In such case, telecom facilities are obtained by miscreants in the name of other persons by using fake and forged identities and identity theft etc.

3.4.3 According to facts narrated in the judgment dated 10<sup>th</sup> March, 2016 rendered by Telecom Dispute Settlement and Appellate Tribunal (TDSAT) in Petition No. 163 of 2015 titled as M/s Bharti Airtel Ltd. Vs UOI, 1000s of connections were issued in the same name. Further, 251 SIMs were obtained in one name from 163 different points of sale situated in 57 different cities. In another

case, 218 SIMs were obtained in one name on different dates from 157 points of sale located in 59 different cities. These SIMs were obtained by forging of documents<sup>6</sup>. The relevant portion of TDSAT judgment is reproduced below for ready reference:

*“The facts of the case are simple and may be stated thus. On analysis of its customer data base submitted by the petitioner for the month of September, 2014 (that showed the number of its subscribers as 1,09,04,632), it was found that a very large number of connections (according to respondent, running into thousands) had the same customer name and same customer’s father’s .....*

*The manner in which SIM cards were obtained using 469 forged CAFs would further make the position clear and it is ironical that the details in that regard come from the counter affidavit filed on behalf of DoT . The CAFs in question were examined by the TERM Cell in great details and the anomalies appearing therein are enumerated in Annexure R5 and summarised in a Table given at paragraph 24 of the counter affidavit. The table is as under:*

S. No .	Name of the Customer	Father’s Name	Photo Used	No. of SIMs Sold to	No. of cities from where SIM has been sold to	Number of Point of Sale involved	Year of SIM Sold	No. of Voter ID Cards Used	No of places from where Voter ID Card issued	Year of Voter ID Card issued
1	Bapina Samal	Dibakar Samal	Photo1 – Person1	78	17	47	2013 & 14	36	24	2013
			Photo2 – Person2	45	13	29	2013 & 14	23	14	2013
			Photo5 – Person5	81	15	52	2013 & 14	40	21	2013
			Photo6 – Person6	47	12	35	2013 & 14	25	19	2013
<b>Total</b>				<b>251</b>	<b>57</b>	<b>163</b>		<b>124</b>	<b>78</b>	

2	Bharat Lanka	Hrudana nd Lenka	Photo3 – Person3	87	19	64	2013 & 14	36	20	2013
			Photo4 – Person4	49	16	34	2013 & 14	27	16	2013
			Photo7 – Person7	58	14	40	2013 & 14	31	16	2013
			Photo8 – Person8	24	10	19	2013 & 14	15	9	2013
<i>Total</i>				<b>218</b>	<b>59</b>	<b>157</b>		<b>109</b>	<b>61</b>	

*From the table it appears that the Sim cards against the 469 CAFs were issued in the year 2013 and 2014. The exact period over which the SIM cards were issued can be gathered from Annexure R5 which shows that the Sim cards were activated over the period from 15.02.2013 to 29.08.2014. From the above table it further appears that 251 SIM cards were obtained in the name of Bapina Samal on different dates from 163 Point of Sale situated in 57 different cities. In case of Bharat Lenka, 218 SIM cards were similarly obtained on different dates from 157 different Point of Sale situated in 59 different cities.*

-----

*.....The investigations made by the TERM Cell further showed that a number of forged Voter ID cards were used as PoI and PoA for obtaining the SIM cards.....”*

3.4.4 Similarly, in Punjab, 185 pre-activated SIM cards in fake names and documents of fake addresses were recovered in Punjab by Police<sup>7</sup>.

3.4.5 Two persons were booked for selling SIM card on fake ID by Punjab Police. The SIM was used for sending objectionable and threatening messages to many peoples<sup>8</sup>.

- 3.4.6 A SIM card issued on fake and forged documents was used in a ransom case in Bihar<sup>9</sup>. Similarly, a SIM card issued on fake identity was used in making ransom calls in Punjab<sup>10</sup>. SIM card issued in the name of fake person was used for making fishing calls in Jharkhand<sup>11</sup>. Haryana police identified 685 SIM cards issued on fake and forged documents. Out of these 392 SIM cards issued on forged documents were deactivated by Haryana Police. These SIM were being used in fraudulent activities<sup>12</sup>. In Telangana, Police seized 4000 SIM cards which were procured using forged ID proofs and photographs and were used for cheating major companies through marketing campaigns<sup>13</sup>.
- 3.4.7 Maharashtra Police busted racket of illegal purchase-sale of SIM cards and impounded 11,345 activated SIM cards, 49,500 photographs, 9,400 fake Aadhar card copies, 3,072 copies of fake voters ID cards<sup>14</sup>.
- 3.4.8 As per reply given in Rajya Sabha in response to a Parliament Question on 22<sup>nd</sup> December, 2017 on the subject “Illegal Use of Identity Papers”, 938 complaints covering 65,991 mobile connections have been received in the last five years with regard to sale of SIMs on fake identity proofs and disconnection was carried out in all such cases. In E-KYC process no separate document for Proof of Address/ Proof of Identity are required to be submitted, therefore the possibility of forgery/misuse of documents submitted by the subscribers can be avoided<sup>15</sup>.

3.1 From the above documents, it may be concluded:

- (g) That SIM cards are getting issued to the subscribers by use of fake/ forged documents and also through identity theft.
- (h) That in Aadhaar based E-KYC process using biometrics, there is practically no possibility of issuance of SIM cards using forged/ fake documents.
- (i) That in Aadhaar based E-KYC process using biometrics, issuance of SIM cards through identity theft is also avoided .
- (j) That in other processes wherein no online verification of subscribers is done before activation of SIM cards, SIM cards are found to be issued by use of fake/ forged documents.
- (k) That SIM cards are found to be issued through identity theft in case of process wherein no online verification of subscribers is done before activation of SIM cards.
- (l) Thus, KYC Regulatory Norms in Telcom Sector of the Country are not effective.

\*\*\*\*\*

## **Chapter-4**

### **Conclusion and Suggestions**

- 4.1 As per analysis in Chapter-3, existing KYC Regulatory Norms in the Country are not effective on the parameters of issue of SIM on fake/ forged identity and address documents and identity theft and improvements are required in these norms.
- 4.2 As on date, following three KYC norms are being followed by telecom service providers for issuing mobile connections:
- (i) First process put in place by Department of Telecommunications through instructions dated 09.08.2012 in compliance of Hon'ble Supreme Court judgment dated 27.04.2012. In this case, physical CAF is filled up by the customer.
  - (ii) Second process known as Digital KYC process put in place by Department of Telecommunications through instructions dated 03.04.2019.
  - (iii) Third process known as Aadhaar eKYC process put in place by Department of Telecommunications through instructions dated 29.09.2020.



4.3 In case of EKYC process for which initial instructions were issued on 16.08.2016 and more or less same instructions have been reiterated on 29.09.2020 after Hon'ble Supreme Court judgment dated 26<sup>th</sup> September, 2018, except few minor modifications relating to privacy of customer. In EKYC process, customer is authenticated by biometric means. Digitally signed EKYC data (name of the customer, address, date of birth, and gender and photograph) is online transferred by UIDAI to the database of telecom operators before of issuing mobile connections. As per reply given in Rajya Sabha by the Government, in E-KYC process no separate document for Proof of Address/ Proof of Identity are required to be submitted, therefore the possibility of forgery/misuse of documents submitted by the subscribers can be avoided<sup>10</sup>.

Accordingly, it may be very well concluded that in EKYC process being followed for issuing mobile connections, almost no possibility of forgery/ misuse arises and it is an effective process for issuing mobile connections.

4.4 In other two processes i.e. DKYC (digital KYC) process put in place by Department of Telecommunications as per instructions dated 03.04.2019 and the first process put in place by Department of Telecommunications through instructions dated 09.08.2012, the documents provided by the customers as Proof of Identity (PoI) and Proof of Address (PoA) are taken as it is by the Point of Sale. In such cases, identity checks can be relatively easily circumvented through identity fraud due to difficulties in validating identity documents by retail sales staff. It is practically not possible for the sales staff

to verify the truthfulness or correctness of the documents provided by the customers in support of his proof of identity and proof of address. The staff at point of sale has no method or tool for detecting forged/ fake documents produced by the miscreants for obtaining mobile connections.

As has been observed in the judgment dated 10<sup>th</sup> March, 2016 rendered by Telecom Dispute Settlement and Appellate Tribunal (TDSAT) in Petition No. 163 of 2015 titled as M/s Bharti Airtel Ltd. Vs UOI, 251 SIMs were obtained in one name from 163 different points of sale situated in 57 different cities. In another case, 218 SIMs were obtained in one name on different dates from 157 points of sale located in 59 different cities. These SIMs were obtained by forging of documents<sup>1</sup>.

Therefore, in these two processes in which customer provides physical copy of proof of identity and proof of address and no verification of these documents is possible regarding their correctness or truthfulness, there are chances of issuing mobile connections on the basis of forged and fake documents. Many instances of such cases of issuance of mobile connections on the basis of forged and fake documents have been provided in Chapter-3 above.

- 4.5 The concern of issuance of mobile connections on forged/ fake documents can be resolved by using “Verified Registration Solutions”. In this process, the documents produced by the customers are online verified from the concerned authority which has issued such documents before activation of

service. The main advantage of having a solution with verification is that it is the most effective solution and is least likely to suffer from issues of identity fraud.

Such process is already being used in Australia for online verification of customers before issuing pre-paid mobile connections. The mobile service providers have been given access to a national online verification service, managed by the Attorney- General's Department, to perform real- time checks on the validity of selected government issued documents such as passports and Medicare cards. The details and validity of a government-issued document is verified using the National Document Verification Service (DVS) or Visa Entitlement Verification Online (VEVO).

Verification is obtained from the source database maintained by the government organisation that issued the relevant document. The system verifies the identity of information with a 'blind check'—accepting or rejecting it with a 'yes' or 'no' answer. Mobile service providers would not have access to issuing organisation's database. For privacy reasons, the proposals prohibit mobile service providers from recording the identifying number of the document. They are only allowed to use the information, during the verification process, to check that the document is authentic, accurate and up- to- date<sup>16</sup>.

4.6 Thus, following improvements are suggested in the KYC regulatory norms of telecom sector:

- (i) Government should launch an Identity Verification Service for online verification of identity and address documents presented by the customers against the records maintained by the issuing authority of such documents.
- (ii) Identity Verification Service should be launched through a partnership between the Central Government, State Government and Local Bodies as identity and address documents to be verified are issued by them.
- (iii) Identity Verification Service should have provision for:
  - (a) Document Verification Service – checks whether the biographic information on the document matches the original record.
  - (b) Identity Data Sharing Service – For sharing information held by document issuing agency with the requesting agency as per consent of customer.
  - (c) Face Verification Service – comparing the photo against the image used on the identity documents with the consent of customers.
- (iv) Identity Verification Service should be made available for use of private organisations (Telecom, Banking, Insurance etc.) as well as Government Agencies.

- (v) Government should made provision for Identity Gateway Service Providers for having connectivity between Identity Verification Service and the users of the service.
- (vi) As Government has time and again reiterated that it has no business to be in business, Government should authorise private organisations (either through license or otherwise) to act as Identity Gateway Service Providers.
- (vii) The SIM cards should be issued to the customers only after online verification of the identity documents produced by them through Identity Verification Service.
- (viii) The identity document presented by the customers for obtaining SIM cards should be online verified using “Document Verification Service” under Identity Verification Service for avoiding use of any fake/ forged document.
- (ix) Live photograph of the customer desirous of obtaining SIM cards should be matched with the photograph maintained by the identity document issuing authority using “Face Verification Service”. It will ensure the avoidance of identity theft cases.
- (x) Once photograph is matched, the demographic data maintained by the identity issuing authority should be transferred using “Identity Data

Sharing Service” to Mobile Operators similar to Aadhaar based E-KYC service.

- (xi) Presently SIM cards are being issued through about 25 types of identity and address documents. Some of these documents are issued using digital platform thereby verifiable online and some are issued without digital platform which may not be verifiable online using Identity Verification Service.

Either the Government should restrict the issuance of SIM cards:

- (a) only through online verifiable documents

OR

- (b) in case of non-online verifiable documents, SIM cards should be restricted to be issued only through “Telecom Service Provider Operated” Point of Sale by following some special verification procedure. In such case SIM cards should not be issued through retailers.

- (xii) As in all the above-mentioned suggestions, private and sensitive data/information of the citizens shall be involved, it is also recommended that Government should enact a very strict privacy and data protection laws in order to avoid any remotest possibility of misuse of data / information of the customers.

\*\*\*\*\*

**Bibliography/ References:** The list of various research papers, judgments, orders, media reports analysed till now for the preparation of the synopsis are as under:

- (1) [https://www.uidai.gov.in/images/news/Amendment\\_Act\\_2019.pdf](https://www.uidai.gov.in/images/news/Amendment_Act_2019.pdf)(Accessed on 1<sup>st</sup> March, 2021)
- (2) Dissent on Aadhaar, Big Data Meets Big Brother , Edited by Reetika Khara and Foreward by Justice (Retd) A.P.Shah (2019)
- (3) Telecom KYC and mobile banking regulation: An exploratory study, Ketkar, S., Shankar, R. & Banwet, D. Telecom KYC and mobile banking regulation: An exploratory study. J Bank Regul 15, 117–128 (2014) <https://doi.org/10.1057/jbr.2013.1>
- (4) Digitalisation & Data Protection – Changing Landscape of Indian Telecom Sector, SASWATA DHAR Executive Vice President Legal & Country Counsel, Vodafone India Ltd, India, International In-house Counsel Journal Vol.11, No. 44, Summer 2018, 1
- (5) Unique Identification Project for 1.2 billion People in India Can it fill Institutional Voids and enable ‘Inclusive’ Innovation? By Vanita Yadav, South Asia Institute (SAI) at Harvard University: Working Paper, June 2013
- (6) Telecom Disputes Settlement and Appellate Tribunal order dated 10<sup>th</sup> March 2016 in Petition No. 163 of 2015 (<https://tdsat.gov.in/Delhi/services/judgment.php>)
- (7) Punjab & Haryana High Court Order dated 12<sup>th</sup> April 2013 in Criminal Misc. No. M-10401 of 2013 { Vinod Kumar @ Bunty Vs State of Punjab} – Available at <https://highcourtchd.gov.in/>

- (8) <https://timesofindia.indiatimes.com/city/ludhiana/2-booked-for-selling-sim-card-on-fake-id/articleshowprint/72301374.cms>
- (9) Patna High Court order dated 22nd May 2015 in Criminal Writ Jurisdiction Case No.277 of 2013 {Balinder Singh vs The State Of Bihar} – Available at <http://patnahighcourt.gov.in/>
- (10) Punjab & Haryana High Court order dated 28th February 2017 in CRM-M-34288 of 2016 {Pawan Kumar Vs State of Punjab} - Available at <https://highcourtchd.gov.in/>
- (11) Jharkhand High Court order dated 21.08.2018 in B.A. No. 3140 of 2018 {Rohit Mandal @ Rohit Kumar vs State of Jharkhand} – Available at <https://jharkhandhighcourt.nic.in/>
- (12) <https://timesofindia.indiatimes.com/city/chandigarh/392-mobile-sim-cards-issued-on-forged-documents-deactivated-inharyana/articleshowprint/76482887.Cms>
- (13) <https://www.deccanchronicle.com/nation/crime/240117/hyderabad-digital-marketing-racket-busted-4000-sims-seized.html>
- (14) <https://www.outlookindia.com/newscroll/racket-of-illegal-purchasesale-of-sim-cards-busted-7-held/973632>
- (15) Reply given by Government in Rajya Sabha Question No. 868 on 22.12.2017
- (16) GSMA Report on “The Mobile Economy 2020” – Available at <https://www.gsma.com/mobileeconomy/>
- (17) GSMA Report on “Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkage” – Available at



- [https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access\\_to\\_mobile\\_services\\_2020\\_Singles.pdf](https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf)
- (18) GSMA Report of April, 2016 on “Mandatory registration of prepaid Sim cards – Addressing challenges through best practice” ([https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA\\_2016\\_Report\\_MandatoryRegistrationOfPrepaidSIMCards.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA_2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf))
- (19) Australian Government, Department of Broadband, Communications and the Digital Economy, Regulation Impact Assessment document February, 2013 – Proposed Changes to Identity Verification Requirements for Prepaid Mobile Services (<https://ris.pmc.gov.au/sites/default/files/posts/2013/05/02-Changes-to-identify-verifacation-requirements-for-Prepaid-Mobiles.doc>)
- (20) GSMA white paper November, 2013 on “The Mandatory Registration of Prepaid SIM card Users” - [https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013\\_WhitePaper\\_MandatoryRegistrationofPrepaidSIM-Users.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf).
- (21) Australian Identity Matching Services - <https://www.idmatch.gov.au/our-services>
- (22) Press Release No. 3 of 2021 released on 28th January, 2021 by Telecom Regulatory Authority of India (<https://www.trai.gov.in/>).-
- (23) [https://en.wikipedia.org/wiki/Telecommunications\\_in\\_India#:~:text=Telecommunications%20in%20India%20began%20with,the%20British%20East%20India%20Company.-23](https://en.wikipedia.org/wiki/Telecommunications_in_India#:~:text=Telecommunications%20in%20India%20began%20with,the%20British%20East%20India%20Company.-23)

- (24) TDSAT Judgment dated 12.04.2012 in Petition No. 252 of 2011 (Cellular Operators Association of India & Ors Vs. Department of Telecommunications & Anr.) – <https://tdsat.gov.in/Delhi/Delhi.php>
- (25) <https://dot.gov.in/access-services/subscriber-verification> (Accessed on 1<sup>st</sup> March, 2021)
- (26) <https://main.sci.gov.in/judgments>
- (27) <https://www.legislation.gov.au/Details/F2013L01844> (Accessed on 1<sup>st</sup> March, 2021)
- (28) <https://www.legislation.gov.au/Details/F2017L00399> (Accessed on 1<sup>st</sup> March, 2021)

\*\*\*\*\*

SIM Registration Policy Landscape by Country<sup>23</sup>Africa<sup>23</sup>

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Algeria	√						√		√					
Angola	√					√			√					
Benin	√						√		√					
Botswana*	√					√			√					
Burkina Faso	√					√			√					
Burundi	√						√			√				
Cabo Verde				√										
Cameroon	√					√				√				
Central African Republic	√					√				√				
Chad	√					√			√					
Comoros				√										
Congo	√					√			√					
Congo Dem. Republic	√					√				√				
Cote d'Ivoire	√					√			√					

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Djibouti					√									
Egypt	√							√	√					
Equatorial Guinea	√					√			√					
Eritrea	√					√				√				
Ethiopia	√					√					√			
Gabon*	√					√			√					
Gambia	√						√			√				
Ghana	√					√			√					
Guinea	√					√				√				
Guinea – Bissau	√					√				√				
Kenya	√							√	√					
Lesotho			√										√	
Liberia	√					√				√				
Libya	√					√				√				
Madagascar	√					√			√					
Malawi	√					√				√				
Mali	√					√			√					
Mauritania	√					√			√					
Mauritius	√					√			√					
Morocco	√					√			√					
Mozambique	√					√				√				
Namibia			√											√

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Niger*	√					√			√					
Nigeria		√					√		√		√			
Rwanda	√					√								
Sao Tome and Principe	√					√			√					
Senegal	√							√	√					
Seychelles*	√					√			√					
Sierra Leone	√					√				√				
Somalia	√					√				√				
South Africa	√					√			√					
South Sudan	√					√				√				
Sudan	√					√				√				
Eswatini	√					√					√			
Tanzania		√						√			√			
Togo	√					√			√					
Tunisia	√						√		√					
Uganda		√						√	√		√			
Zambia		√						√			√			
Zimbabwe	√					√					√			

\*Countries who are in the process of introducing a data protection law, however, it has not yet entered into force.

Asia and the Pacific<sup>23</sup>

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Afghanistan	✓					✓				✓				
Armenia	✓					✓			✓					
Australia	✓					✓			✓					
Azerbaijan	✓					✓			✓					
Bahrain		✓						✓	✓					
Bangladesh		✓						✓		✓				
Bhutan	✓					✓				✓				
Brunei Darussalam	✓					✓				✓				
Cambodia	✓					✓				✓				
China		✓						✓		✓				
Fiji	✓					✓				✓				
Georgia	✓			✓		✓			✓					
Hong Kong				✓										
India	✓					✓					✓			
Indonesia	✓							✓			✓			
Iran	✓					✓					✓			
Iraq	✓					✓				✓				
Israel				✓										
Japan	✓					✓			✓					
Jordan	✓					✓					✓			

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Kazakhstan	√					√			√					
Kiribati				√										
Korea, North	√					√				√				
Korea, South	√					√					√			
Kuwait	√					√			√					
Kyrgyzstan	√					√			√					
Laos	√					√			√					
Lebanon	√					√			√					
Macao	√					√			√					√
North Macedonia	√					√			√					
Malaysia	√							√	√					
Maldives	√					√				√				
Marshall Islands				√										
Micronesia				√										
Mongolia	√					√				√				
Myanmar	√					√				√				
Nauru				√										
Nepal	√					√			√					
New Zealand				√										
Oman	√					√			√				√	
Pakistan		√						√			√			
Palau					√									

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Palestine	√					√				√				
Papua New Guinea	√					√				√				
Philippines			√										√	
Qatar	√					√			√					
Samoa				√										
Saudi Arabia		√						√		√				
Singapore	√					√			√					
Solomon Islands				√										
Sri Lanka*	√					√			√					
Syria	√					√				√				
Taiwan	√					√			√					
Tajikistan	√					√			√					
Thailand		√					√		√					
Timor – Leste	√					√				√				
Tonga	√					√				√				
Turkey	√					√			√					
Turkmenistan	√					√			√					
Tuvalu					√									
United Arab Emirates		√				√			√					
Uzbekistan	√					√			√					



Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Vanuatu				√										
Vietnam	√					√					√			
Yemen					√									

\*Countries who are in the process of introducing a data protection law, however, it has not yet entered into force.

## Europe<sup>23</sup>

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Albania	✓							✓	✓					
Andorra	✓					✓			✓					
Austria	✓					✓			✓					
Belarus*	✓					✓			✓					
Belgium	✓					✓			✓					
Bosnia and Herzegovina				✓										
Bulgaria	✓					✓			✓					
Croatia				✓										
Cyprus	✓					✓			✓				✓	
Czech Republic				✓										
Denmark				✓										
Estonia				✓										
Finland				✓										
France	✓					✓			✓					
Germany	✓					✓			✓					
Greece	✓					✓			✓					
Greenland														
Hungary	✓							✓	✓					
Iceland				✓										

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Ireland				√										
Italy	√						√		√					
Kosovo	√						√				√			
Latvia				√										
Liechtenstein				√										
Lithuania				√										
Luxembourg	√					√			√					
Malta			√										√	
Moldova				√										
Monaco	√					√			√					
Montenegro	√					√			√					
Netherlands				√										
Norway	√					√			√					
Poland	√							√	√					
Portugal				√										
Romania			√										√	
Russian Federation	√					√			√					
San Marino	√						√		√					
Serbia			√										√	
Slovakia	√					√			√					
Slovenia				√										
Spain	√					√			√					
Svalbard	√					√			√					

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy
Sweden				√										
Switzerland	√					√			√					
Ukraine	√					√			√					
United Kingdom				√										

\*Countries who are in the process of introducing a data protection law, however, it has not yet entered into force.

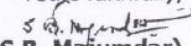
North and Latin America<sup>23</sup>

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data privacy framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Antigua and Barbuda	✓					✓			✓					
Argentina	✓					✓			✓					
Bahamas	✓					✓			✓					
Barbados	✓					✓								
Belize	✓					✓				✓				
Bolivia	✓					✓				✓				
Brazil*	✓					✓			✓					
Canada				✓										
Chile			✓										✓	
Colombia	✓					✓			✓					
Costa Rica	✓					✓			✓					
Cuba	✓					✓				✓				
Dominica	✓					✓								
Dominican Republic	✓						✓		✓					
Ecuador	✓						✓							
El Salvador	✓					✓								
French Guiana					✓	✓								
Grenada	✓					✓				✓				
Guatemala	✓					✓				✓				

Country	SIM Registration Mandated	SIM Registration Mandated using Biometrics	SIM Registration under Consideration	SIM Registration not Mandated	State of SIM Registration Inconclusive	“ Capture and Store” SIM user information	“ Capture and Share” SIM user information	“ Capture and Validate” SIM user information	Mandate SIM Registration and have a data privacy framework	Mandate SIM Registration but lack a data privacy framework	Mandate or Considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM Registration and have no data protection framework	Considering SIM Registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Guyana	√					√				√				
Haiti	√					√				√				
Honduras	√					√								
Jamaica	√					√								
Mexico				√									√	
Nicaragua				√										
Panama	√					√			√					
Paraguay	√					√							√	
Peru		√					√		√					
St. Kitts and Nevis*	√					√			√					
St. Lucia	√					√			√					
St. Vincent and the Grenadines*	√					√			√					
Suriname	√					√				√				
Trinidad and Tobago*	√					√			√					
United States of America				√										
Uruguay	√					√			√					
Venezuela	√					√				√				

\*Countries who are in the process of introducing a data protection law, however, it has not yet entered into force.

**Instructions dated 29<sup>th</sup> December 2004 regarding verification of identity of subscribers**

	<p><b>Government of India</b>  <b>Ministry of Communications &amp; I.T.</b>  <b>Department of Telecommunications</b>  <b>Licensing Cell (Basic Services Group)</b>  <b>Room No. 1406, 20, Ashoka Road, Sanchar Bhawan, New Delhi</b></p>	<p><u>ANNEXURE II</u></p>
	<p><b>No. 10-10/2003-BSII (Vol.V)</b></p>	<p><b>29<sup>th</sup> Dec. 2004</b></p>
<p>To</p> <p align="center"><b>All BSOs / UASOs including MTNL &amp; BSNL</b></p>		
<p><b>Sub: <u>Verification of Identity of subscribers.</u></b></p>		
<p>With reference to the subject mentioned above and Part IV Security condition No. 41.15 of the Unified Access Services Licence, the undersigned is directed to state that 100% of verification of identity proof is to be carried out before sale of postpaid/prepaid SIM cards or any kind of telephone connection.</p>		
<p>2. It is come to the notice of the licensor that in many cases SIM cards/connections are being sold without proper verification of identity proof. The dealers of the licence operator are either selling SIM cards without proper verification of identity of subscribers' bonafide to persons who furnishes falls addresses and forged documents or in some cases do not even ask for documents specified for verification of identity of the subscriber. The relevant proforma as annexed should be filled/taken duly filled before providing the mobile telephone service to any customer (Annexure I &amp; II). All the operators can use these proformas with the mentioned columns. However, the operators may supplement [and not substitute] this proforma in accordance with their business considerations.</p>		
<p>3. It is again emphasized that sale of SIM cards / connections without proper identity verification is a matter of concern and has serious security implications, a procedure needs to be evolved to ensure that SIM cards are not sold without proper identity verification. Also, it is emphasized to cross check the addresses of all the existing subscribers and it is felt that the service providers are already doing this exercise. In view of the above, it needs to be ensured by the service providers that there should not be any working number in their network without proper address of the subscriber. Further, it will be the responsibility of the licensee to maintain the records of the identity of their customers and produce the same on requisition. Therefore, necessary arrangements for obtaining the necessary records from the franchisees in a foolproof manner so as not to leave out even a single user of the service, should be made.</p>		
<p>4. Verification of identity of subscribers before provisions of Telephone Service as per above instructions for security reasons is an important requirement. You are, therefore, required to furnish an undertaking per attached proforma to the effect that the instructions issued as above are scrupulously followed (Annexure-III).</p>		
<p>5. Above said instructions are to be completed without fail in respect of all types of subscriber (present/future). Action taken report in this regard is to be submitted by 31.1.2005. Further, It is mentioned that instances of non-verification of identity of subscriber(s) shall be treated as breach of terms and conditions of the Licence Agreement and the action would be taken accordingly.</p>		
<p>Encls. As above</p>		
		<p>Yours faithfully,    <b>(S.B. Majumdar)</b>  <b>ADG (BS-II)</b>  <b>Tel. No. 23036536</b></p>
<p>Copy for information to:-          Sr.DDG( Vigilance / VAS)          Association of Unified Telecom Service Provider of India / Cellular Operators Association of India.</p>		