Telecom Regulatory Authority of India

Recommendations

on

Privacy, Security and Ownership of the Data in the Telecom Sector

New Delhi

16th July 2018

Telecom Regulatory Authority of India

Mahanagar Doorsanchar Bhawan,

Jawahar Lal Nehru Marg,

New Delhi-110002

www.trai.gov.in

Index

Chapter-1: Introduction

1.1 Telecommunications has been an important growth engine in the development of modern India. It has enabled connectivity to the remotest corners of the nation which has not only benefited the citizens but also helped in better governance. Access to digital services and applications from remotest parts of the country is enabled by telecommunication connectivity. As per a study[1] doubling of mobile data usage increases the GDP by 0.5% points while a 10% increase in mobile telecom penetration increases Total Factor Productivity in long run by 4.2% points. As per a report on statistics of internet usage in India[2] there are total 462.1 million internet users (approx 34% of population, global average is 53%) out of these, 282 million are active internet users spending approximately 7 hours per day on the internet. Out of total 462.1 million internet users, 430.3 million use the internet from mobile phones (79% of the total web traffic). Active social media penetration in India is 19% of the total population; global average is 42% of the total population. A user spends approximately 2 hours 30 minutes daily on social media and has on an average seven mobile applications being used on his mobile device.

1.2 The eco-system used for delivery of digital services consists of multiple entities like Telecom Service Providers (TSPs), Personal Devices (Mobile Handsets, Tablets, Personal Computers etc), M2M (Machine to Machine) Devices, Communication Networks (consisting of Base Trans Receiver Stations, Routers, Switches etc), Browsers, Operating Systems, Over The Top (OTT) service providers, Applications etc. It is estimated that the global volume of digital data created annually was 4.4 zettabytes in 2013 and this would reach 44 zettabytes by 2020[3]. Further, it is expected that the number of devices connected to the IP

[1] https://www.gsma.com/publicpolicy/wp-content/uploads/2012/11/gsma-deloitte-impact-mobile-telephony-economic-growth.pdf
[2] 2018 Global Digital Report by We Are Social & Hootsuite
[3] The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Things', EMC Digital Universe with Research and Analysis by IDC (April 2014), available at:https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.html

Networks would be approximately three times the global population by 2021[4] . The growth in the number of connected devices imply that a large portion of data created would presumably consist of personal details relating to individuals, e.g purchases, places visited, demography, health statistics, financial transactions, education, work profile etc

1.3 Enterprises around the world have realized the value of user data; hence technologies are being developed for more accurate sifting of data and better understanding of consumer's requirements[5]. Enhancement in the computational powers of modern computers coupled with the rapid development of technology has made it possible to process voluminous data in order to identify correlations and discover patterns in all fields of human activity which can be utilized even for profiling. Data of individuals can be utilized for problem solving, ensuring targeted delivery of benefits, and bring new products and services to the market etc.

1.4 Technology, though beneficial to the mankind in general, does have collateral disadvantages e.g. increasing use of smart devices in everyday lives can lead to a loss of privacy for individuals, who may often not even be aware that they are being tracked or observed. Similarly, ubiquitous presence of smart devices like a mobile handset has many benefits but it may also be a source of loss of privacy of the user, e.g. when a user knowingly/unknowingly grants permission to access the camera and micro phone of a smart device to an application; the application may execute live streaming on the internet using camera and micro phone, run real time facial recognition algorithms, use advanced algorithms to create a three dimensional model of the users face, upload random frames of video stream being

[4] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html
[5] 10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations, IBM, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN.

accessed by the user etc. Data collated by such applications over a period of time may be utilized for predictive profiling of the individual which may seriously jeopardize the data privacy of the users.

1.5 As stated earlier, Digital services and applications are accessed using telecommunication connectivity. When a user accesses an online application or social media website, the data generated passes through the telecom network. It is therefore vital that user privacy is ensured appropriately in the telecommunications layer - both from external agents who may wish to cause harm to users (for instance, by stealing their personal data for purposes of fraud) and from entities in the telecom space who may wish to (mis)use user data that they have access to (for instance in the form of unsolicited targeted advertising). It is worth reiterating that Telecom Service Providers (TSPs) control the "pipes" through which information is exchanged. Due to increasing computing power, TSPs may have an increased ability to analyse the contents of the pipe i.e. the data flow of users, leading to obvious privacy concerns. In addition to TSPs, the widespread adoption of smart devices amongst the populace is also a trend that must be considered. Unlike in the past, when the intelligence was residing in the telecommunication networks only and user devices were not intelligent, now, smart devices (including Operating systems, Browsers, Applications etc) are increasingly playing a gate-keeping role over the network: they determine how users connect to and experience a network. As with TSPs, all user data flows through these smart devices, putting the Device Manufacturers, Browsers, Operating Systems, and Applications etc. in a prime position to collect and process the personal information of users. Given that all user data has to pass through the TSPs (analogous to pipes) and devices (analogous to faucets) it is essential that appropriate steps are taken to protect user privacy vis-a-vis these entities. In effect, the subject of data ownership, privacy, and security is multi-dimensional and

complex, and hence data consumers must be empowered to navigate safely and securely through the maze of the digital eco-system.

1.6 As the economy increasingly moves to the digital/online world, it is all the more important that users are appropriately protected from all entities in the ecosystem that may seek to take advantage of their gate-keeping power. A failure to adequately protect users from the very real possibility of harm (caused by the loss of privacy) may result in restricting the growth of the entire digital economy which include telecommunication services also.

1.7 Given the Authority's mandate to ensure user protection in the telecommunications space, it is essential that appropriate norms be laid out for privacy and protection of telecommunication consumers. Accordingly, with a view to bring out the multiple aspects of the data protection in the telecommunication sector, and to provide a suitable platform for discussion, TRAI issued a consultation paper (CP) on "Privacy, Security and Ownership of the Data in the telecom sector" on 09 August 2017. The objective of the CP was to identify the key issues pertaining to data protection in relation to the delivery of digital services through the telecommunication systems. Written comments on the CP were invited from the stakeholders. An Open House Discussion (OHD) was also conducted on 01st February 2018 at New Delhi. Based on the written submissions of the stakeholders and the discussions in the OHD, the issues have been examined in depth and recommendations have been framed.

1.8 The recommendations are also to be viewed in the light of the details in the following two paragraphs:

(a) In 2016, the Department of Telecommunications (DoT) sought the recommendations of the Authority on three aspects related to M2M communications (quality of service, roaming requirements and spectrum requirements). In its Consultation Paper on Spectrum, Roaming, and QoS related requirements in

M2M Communications (October 18, 2016, CP No. 21/2016), the Authority also raised issues pertaining to the privacy and security of M2M communications (apropos of which it received numerous responses from stakeholders). Pursuant to consultations and an analysis of responses, the Authority issued recommendations related to M2M communications on September 5, 2017. These recommendations however did not address the issues pertaining to privacy and security of M2M communications as it was decided to address them separately. In view of the similarity of issues raised in the CP on Privacy, Security and Ownership of Data and the issues pertaining to privacy and security of M2M communications, the present recommendations deal with both sets of issues in a holistic manner.

(b) On 24th August 2017, a nine-judge bench of the Supreme Court in Justice K.S. Puttaswamy vs Union of India unanimously recognized the constitutional right to privacy rooted in human dignity and individual autonomy. The Court declared that privacy constitutes an intrinsic part of the right to life and personal liberty under Article 21. It was recognized that privacy is a multidimensional construct encapsulating within it various rights such as informational privacy, bodily-integrity, and self-determination. The Court also noted both the positive and negative obligations arising out of the fundamental right to privacy and the dangers faced from private actors. The Court clarified that the right to privacy is not absolute and that the state can place reasonable restrictions on it in the interest of fulfilling objectives such as protecting national security,

preventing and investigating crime, encouraging innovation, and preventing the dissipation of social welfare benefits[6].

1.9 The Government is also seized of the matter concerning the privacy of data of users. It constituted a Committee of Experts on 31 July 2017, under the Chairmanship of Justice B N Srikrishna, Former Judge, Supreme Court of India to identify key data protection issues in India and recommend methods of addressing them. The terms of reference for this Committee are as follows:

(a) To study various issues relating to data protection in India.

(b) To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill.

1.10 The Authority is of the view that the larger issues relating to data protection framework applicable in general for all sectors of the economy would in any case be addressed by the Committee of Experts headed by Justice B N Srikrishna. TRAI, in its present recommendations has considered only the TSPs - which provide the connectivity and communication services; devices - which an end user uses to access the network and services; and the users of telecommunication services themselves. Further, the Authority is cognizant of the fact that the present recommendations may require updating /revision pursuant to introduction of a new data protection law/framework in the country. Once the data protection Law is enacted, the Authority may revisit the issue again in the specific context of the telecommunication sector.

1.11 The issues relating to data protection framework raised in the CP, responses received from the stakeholders, analysis, and the recommendations have been covered in Chapter 2. The responses

[6] Bhandari, Kak, Parsheera and Rahman, An analysis of Puttaswamy: the Supreme Court's privacy verdict, available at https://ajayshahblog.blogspot.in/2017/09/an-analysis-of-puttaswamy-supreme.html.

were widely divergent and the Authority has taken a holistic view of the different facets of privacy, security, and ownership of data to arrive at the recommendations. The summary of recommendations has been provided in Chapter 3.

CHAPTER 2: Data Protection Framework

2.1 The Digital Eco-system comprises of multiple entities like Devices (Mobiles, Laptops, Tablets, PCs etc), Telecom Service Providers (TSPs), Communication Networks (consisting of Switches, Routers, Base Trans-Receiver Stations etc), Browsers, Operating Systems, Applications, Over The Top (OTT) service providers, M2M devices etc. Most of these entities have capability of gate-keeping function, and an asymmetric advantage of accessing, collecting, and collating users' data. Thereby these entities could infringe upon the privacy of users. It is therefore important to ensure that the data is collected, stored, and processed in regulated manner with the informed and explicit consent of users.

2.2 In the backdrop of possible threats to the data privacy of the telecommunication consumers, the Authority raised the following issues in the CP, for obtaining the views of the stakeholders-

(a) Examine the present definition of personal data, and in light of recent advances in technology, suggest changes, if any.

(b) Sufficiency of existing data protection laws applicable to all the players in the digital ecosystem and additional measures, if any, which may be required to strengthen the framework.

(c) Identification of key issues of data protection pertaining to collection of data by various stakeholders in the digital ecosystem and measures that needs to be taken to address those issues.

(d) Examining the need to bring parity in data protection norms applicable to the TSPs and other communication service providers offering comparable services.

(e) Rights and responsibilities of Data Controllers and the suggested mechanism to regulate the Data Controllers.

(f) Need to establish a technology enabled architecture to audit use of personal data, and monitor the entire digital eco-system for compliance.

(g) Measures that need to be considered to strengthen the safety and security of telecom infrastructure and the digital eco-system as a whole.

(h) Measures to be undertaken to encourage creation of new data based businesses.

(i) Need for setting up Data Sandboxes by the government for development of newer services.

(j) Examine the legitimate exceptions to the data protection requirements imposed on TSPs and other stakeholders in the digital eco-system.

(k) Identifying and examining the potential issues arising from cross border data flow and measures that need to be considered to address them

A. Personal Data

2.3 Every time, a large quantity of data is generated when an individual/machine comes into contact with the digital ecosystem. Data generated may include information relating to an individual, meta-data, as well as M2M communication data that relates to an individual. The modes of collecting such data are changing rapidly as well as the uses that such data can be put to.

2.4 Accordingly, and in view of the need to ensure a proper understanding of the term 'personal data', the Authority requested responses on the issue of defining personal data.

2.5 In response, a large number of the respondents were of the view that the existing definition of personal data provided under the sensitive

Personal Data and Information (SPDI) Rules, 2011 is sufficient and should not be changed. They were of the view that the difference between personal information, non-personal, and aggregate information should be considered during framing of laws. Also, aspects of purpose, context, and proportionality are important in determining the classification of information. Different kinds of data that can be potentially personal should be treated differently depending on the risk that certain data poses to privacy. They had further submitted that certain types of data may be benign in one context, but when combined with other forms of data this may no longer be the case.

2.6 One stakeholder was of the view that technology changes occur at a very rapid pace. Hence, the regulatory framework should match or account for the pace of technical advancement. The current SPDI Rules were published in 2011 and ever since no amendment has been made. However, since 2011 there have been numerous technological changes especially in the social networking and M2M services domain; and that enable collection of large quantities of personal information about an individual. The information so generated has the ability to clearly identify an individual and, hence, there is a need to enlarge the list of information relating to an individual defined under SPDI Rules.

2.7 Some stakeholders submitted that:

(a) Personal data should also include: Online activity, information stored in personal devices, information obtained from personal use of M2M devices, personal details, family, lifestyle and social activities, employment details, financial details, goods or services procured etc.

(b) The scope and ambit of personal data should be widened so as to cover data secured by broadband service providers; mobile set manufacturers, device and software appliance developers.

2.8 Some stakeholders were of the view that new data protection framework, should not be overly restrictive for the data analytics industry by framing stringent definitions of personal data or incorporating mechanisms that are deterrent to the growth of the data industry. Entities operating in the digital ecosystem may be subjected to privacy rules of the country in which services are being offered.

2.9 Some other respondents were of the view that while defining personal data no distinction should be made with respect to the source of data. For instance, the data generated by a smart device and the data generated while availing telecom services should be subjected to same regulatory framework.

2.10 A few stakeholders were of the view that anonymous data is not personal data and, therefore, anonymised data may be accorded simpler, less stringent privacy protections. Only anonymised and aggregated data should be allowed to be used by companies for developing better services/products. Further, since anonymised data cannot be used to identify and locate/profile/track any individual, it should not be included under the definition of personal data. They were also of the view that pseudonymisation can provide safeguards to user data and hence it may be considered while framing the data privacy framework for the country.

2.11 In contrast to the above-mentioned submission, some stakeholders were of the view that complete anonymization of data is not achievable. Further, the respondents cited two research reports, one from the University of Texas[7] and the other from the Colorado Law Legal Studies Research[8] which showed the possibility of re-identification of users from the anonymised data sets. Thus, sufficient

[7] Narayanan, A. and Shmatikov, V, Robust De-anonymization of Large Sparse Datasets, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

[8] Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: https://ssrn.com/abstract=1450006

safeguards in the form of anonymization guidelines and standards are necessary if such a distinction is created including the prohibition of de-anonymization subject to stringent penalization. They were of the opinion that metadata should be accorded the same protection as applicable to personal data. They also submitted that metadata should not be used by the TSPs to identify the users.

2.12 One of the key issues raised in the consultation paper was that of the ownership of personal data. This is arguably one of the more fundamental issues with respect to determining the framework of rights and obligations over personal data. The Authority notes the difference between 'ownership' and 'control' of data. The former term refers to a proprietary right in a thing or claim, while the latter refers to the competence to take decisions concerning the data.

2.13 With regard to ownership of personal data, most of the stakeholders were of the view that the ownership of personal data should ideally be of the individual about whom such data is related and the individual should have the primary rights over such data. Some stakeholders caution about creating a purely property based framework around personal data as data can be replicated infinitely hence it can be infinitely distributed.

Analysis

2.14 It must be remembered that identifiability often depends on context. For instance, an IP (Internet Protocol) address or MAC (Media Access Control) address of a device, when seen independently may not qualify as 'personal data' but when aggregated along with the Meta-data of the user device or indeed subscriber information, may qualify to be personal data. Hence it is important to consider the context also while classifying a data as "personal data". The existing legal framework in

India defines the terms "data", "information', "personal information" and "sensitive personal data or information" as under:

(a) "***Data***" – defined in section *2(1)(o)* of the IT Act, 2000 as *a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.*

(b) "***Information***"– defined in section *2(1)(v)* of the IT Act,2000 as *a term including data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.*

(c) "***Personal information***"– defined in the SPDI Rules, 2011 as *any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*

(d) "***Sensitive personal data or information***"– defined in the SPDI Rules, 2011 as *such personal information which consists of information relating to:- password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as*

sensitive personal data or information for the purposes of these rules.

2.15 Personal data has been defined under *Article 4* of the ***EU GDPR***[9] in the following manner:

*'**Personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

2.16 As seen from above, the existing definition of personal information/ data under Indian Acts and Rules is in sync with the international trend. Since the definition of personal information/ data would have far reaching implications both in the digital as well as in the physical world, the Authority is of the view that present definitions be continued till the enactment of specific data protection law for the country.

2.17 The mode of collection of data may not necessarily effect its classification as the entity capturing the data in physical form may convert the same to binary digital data. Hence the mode of collection of personal data should be irrelevant. The personal data captured by a smart device, camera, microphone, applications etc must be treated in the same manner.

2.18 In order to ensure privacy of users, before processing their data, there is merit in ensuring that the same is anonymised/de-identified. However, keeping in view the risks of de-anonymisation/re-identification of users using latest computing techniques by unscrupulous entities for personal gains, the Authority is of the view

[9] https://gdpr-info.eu/art-4-gdpr/

that a technologically neutral approach be taken for annonymisation/ de-identification and that on that basis, certain standards for anonymisation/de-identification of data need to be put in place. Since, in certain cases, metadata can be used by the entities operating in the digital eco-system itself to identify the individual users, such entities must be restrained from using metadata to identify the users/individuals.

2.19 In respect of the ownership of personal data, the Authority is of the view that the individual must be the primary right holder qua his/ her data. While the right to privacy should not be treated solely as a property right, it must be recognized that controllers of personal data are mere custodians without any primary rights over the same. For instance, it would appear illogical/ inequitable to permit complete transfer of rights over an individual's personal data. This would imply that, the personal data can no longer be used/ accessed by the data owners – a situation which is quite clearly untenable. In the circumstances, there must be a recognition that while data controllers may indeed collect and process personal data, this must be subject to various conditions and obligations – including importantly, securing explicit consent of the individual, using the personal data only for identified purposes, etc. The entity that has control over personal data would be responsible for compliance with data protection norms.

2.20 **In light of the aforesaid, the Authority recommends:**

(a) The definitions of "Data" as provided under Information Technology Act, 2000, and "Personal Information" and "Sensitive Personal Data and information" as provided under Sensitive Personal Data and Information Rules, 2011, as reproduced below, are adequate for the present.

(i) "***Data***" – *defined in section 2(1)(o) of the Information Technology Act, 2000 as a representation of information, knowledge, facts, concepts or instructions which are being*

prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

(ii) *"**Personal information**"– defined in the Sensitive Personal Data and Information Rules, 2011 as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*

(iii) *"**Sensitive personal data or Information**"– defined in the Sensitive Personal Data and Information Rules, 2011 as such personal information which consists of information relating to:- password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.*

(b) Each user owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem. The entities, controlling and processing such

data, are mere custodians and do not have primary rights over this data.

(c) A study should be undertaken to formulate the standards for annonymisation/ de-identification of personal data generated and collected in the digital eco-system.

(d) All entities in the digital eco-system, which control or process the data, should be restrained from using metadata to identify the individual users.

B. Sufficiency of existing Data Protection Framework

2.21 Telecom sector is fairly organized and the TSPs are governed by a number of guidelines relating to protection of user data. There are a number of applicable legislation and policies that contain provisions with a bearing on the right to privacy and data security in the telecom sector in India. These include:

(a) IT Act, 2000: Sec 43A, Sec 69, Sec 69B, Sec 72A, Sec 67C, and Sec 79.

(b) IT Rules

(c) Indian Telegraph Act, 1885: Sec 5 and Sec 26,

(d) Indian Telegraph Rule 419A.

(e) Unified License condition 37, 38, 39 and 40.

(f) Guidelines, circulars, direction, and notifications issued by DoT and TRAI

2.22 Under Section 70 of the IT Act, 2000, Telecom Sector has been designated as one of the most important Critical Information Infrastructure by National Critical Information Infrastructure Protection Centre (NCIIPC) as incapacitation or destruction of this sector would result in debilitating impact on the national security, governance, economy and social well-being of the nation. In addition

to the above, in February, 2010, TRAI issued a directive to all TSPs requiring them to ensure compliance of the terms and conditions of the licence regarding confidentiality of information of subscribers and privacy of communications. The Authority had directed the service providers to put in place appropriate mechanisms to prevent the breach of confidentiality of information of subscribers and furnish the details of the steps taken in this regard. The source of generation of unsolicited calls and bulk SMSs may be attributed to unlawful access to consumer's personal information hence it poses a threat to consumer privacy. Unsolicited calls and bulk SMSs can also be used as a tool for phishing attacks. Hence, the National Customer Preference Register (NCPR) was created to protect the privacy of telecom subscribers.

2.23 In response to the questions on sufficiency of existing data protection framework and need to bring parity between the OTT service providers and TSPs raised in the CP, most of the TSPs and Telecom Sector Associations were of the view that the provisions included in the UASL related to the privacy of the customers and data protection are sufficient. They were, however, of the view that licensing framework is applicable only to the TSPs while other players in the eco-system like the OTT communication service providers, content providers, device manufacturers, browsers, operating system developers etc. are not covered with similar conditions, leading to a scenario wherein same data is governed by different set of rules in the same ecosystem.

2.24 A few stakeholders, comprising of Associations of Application Providers and companies in the software business were however of the view that OTT services are not comparable to the TSPs as the TSPs have an assured revenue business model, they own the infrastructure, and have the primary right over their spectrum. In the absence of assured revenue streams, OTT players have to devise innovative

models for revenue generation without charging the end users for the OTT services that are provided to them.

2.25 Some stakeholders from the Software Industry were of the opinion that there is there is no need to ensure parity as the internet-based services and TSP-services operate in completely different market segments with unique regulatory and economic concerns. Treating them at par would fail to recognize these crucial distinctions and result in inefficient regulation. Further, they submitted that there is no need for introduction of additional data protection requirements to bring parity as the data protection requirements as incorporated in the IT Act, 2000 apply to all the stakeholders in the internet ecosystem.

2.26 They further submitted that, TRAI, in the interim may seek information on the specific practices undertaken by TSPs to ensure compliance with Clause 37 of the UASL. Since OTT applications are unlicensed, they do not have to comply with TRAI regulations. They however have to abide by the provisions of the IT Act, 2000 and the complementing Rules. Also, OTT applications should not be subjected to licensing as it will hamper innovation. These stakeholders had also quoted that DoT had rightfully concluded in 2015 that licensing requirements for OTTs were not warranted and TRAI should likewise conclude the same here.

2.27 Some stakeholders had submitted that though certain enabling provisions are present in the statute books, the overall framework for data protection of users / telecom subscribers as well as enforcement mechanisms require development. For instance, while the UL requires TSPs to protect the privacy of their customer's data, there are no specific or detailed requirements on issues such as access, correction, data breach, etc.

2.28 A large number of respondents were of the view that in order to ensure that an individual's data privacy is protected an independent

statutory authority responsible for data protection should be set up in India under the proposed data protection law. The proposed authority should have jurisdiction over all entities dealing with the data of Indian residents – irrespective of their physical location. The functions of the data protection authority should include:

(a) Standard setting including through regulations and codes of conduct monitoring and supervision.

(b) Investigations and enforcement, including through punitive action.

(c) Grievance redressals to ensure users' rights are effectively protected.

(d) Coordination with privacy authorities and other relevant entities in other countries

(e) Making recommendations to the government on issues where intergovernmental action is required in the data privacy field.

2.29 Further, some stakeholders also mentioned that the IT Rules are ambiguous and do not define the roles and responsibilities of data controllers and processors and do not set out clearly the nature of the data that the rules are applicable to. Further, the IT Act provides only a compensation mechanism and does not provide for penalties or consequences for failure to comply with the IT Rules. With regard to data protection issues in the telecom sector, some stakeholders highlighted the following through their submissions:

(a) There is a need for an overarching principle based privacy law together with relevant enforcement mechanisms to protect the privacy of all Indian citizens.

(b) It is critical for government to ensure consumer education and awareness.

(c) Policy makers need to focus on principles, and leave implementation to the industry.

(d) Regulatory focus needs to shift from 'operational' risk management to 'design' risk management approach. Concepts like privacy by design within an accountability model are essential. Any standards which are notified may be as per international standards to enable the benefits of standardization

2.30 One of the stakeholders submitted that, the consumers are subjected to complex one-sided user privacy contracts. In many cases, the consent obtained from users is "pre-agreed" or default, and the user has no choice but to accept them. In other cases, the devices come with inbuilt pre-conditions of use which can seriously jeopardize the privacy and security of the users by accessing and transferring user data without his/her knowledge. According to the submission, the existing regulatory framework for data protection suffers from following limitations:

(a) Limited protection for personal information: The data protection rules under Section 43A of the IT Act,2000 apply only to a narrowly defined category of Sensitive Personal Data and not all forms of personally identifiable data.

(b) Lack of regulation of the Government sector: Section 43 A of the IT Act, 2000 apply only to Body Corporate and are not extended to Government sector resulting in a lack of data protection standards for collection and use of data by Government sector entities.

(c) Inadequacy of provisions on privacy policies: Requirements of Privacy Policies need to be strengthened in various respects like notice prior to collection, short and easy to understand terms and conditions of use, notification in case of any change in policies etc.

(d) Inadequacy of provisions on consent: Consent has been defined to be a onetime mechanism not requiring renewal when modifications are made to privacy policy. Section 43 A does not facilitate easy access and execution of opt out mechanism by the user.

(e) Limited access and correction protections: Data access for the users is limited to the information provided by them, ignoring present day mechanisms that collect data both directly and indirectly. There also no rules and standards that mandate availability of data to users in a structured, easy to understand format. There are also no provisions which allow the users to edit or move their collected data.

(f) Broad data retention terms: The purpose and collection limitations under Section 43A are applicable only to Sensitive Personal Data and Information and not to all personal data. The standards fail to connect the consent provided to purpose and duration of retention of data.

(g) Restrictions on encryption: Certain communication license agreements set out restrictions on encryption. For instance, the Internet Service Provider (ISP) License Agreement requires ISPs to obtain prior governmental approval to deploy encryption which is higher than 40 bits (Part 1, Clause 2(vii)). The Unified License agreement (Clause 37.1), the Unified Access Services License agreement (Clause 39.1), and the ISP license agreement (Part 1, Clause 2(vii)) all prohibit bulk encryption by TSPs.

2.31 The stake holders were of the view that TRAI, being a regulatory authority for telecom services providing internet access only, devising mechanisms to control other stakeholders like content providers and application service providers may be an overreach for the Authority and, perhaps, should be avoided. They were of the opinion that Device manufacturers, service providers, sellers, and all entities involved in

manufacturing, sale and provision of devices and services should not be allowed to interfere with secure data transfers and secure communications. These entities should be held responsible for any data breach due to their systems, software, or otherwise

Analysis

2.32 In the absence of a comprehensive data privacy framework, users of the telecommunication/ digital services are subjected to one sided user agreements which are complicated and are difficult to understand. In many cases, these consents are "pre-agreed" and the user has no choice but to accept them. In many cases, the devices come with pre-agreed conditions of use which can seriously jeopardize the privacy and security of the users by accessing and transferring user data without his/her knowledge. User's data may, therefore, not be protected while stored in the digital eco-system. The need for a more symmetric, all encompassing principles based and horizontally applicable data protection framework for all the players in the digital eco-system is therefore urgent and inescapable. Since the data is collected by private as well as government entities, the data protection framework should be equally applicable to both the Government as well as private entities.

2.33 Some categories of data of an individual are protected by the SPDI Rules, 2011. The enforcement / penal provisions provided under the IT Act, 2000 are not stringent enough to ensure protection of individual's personal information/ data. For example, section 43 A of the IT Act,2000 provides for punishments in the event of negligence in securing sensitive personal data, thereby leading to wrongful loss or gain to any person. The maximum penalty payable under Sec 43A of the IT Act,2000 is Rs five crore. Low penalties/ fines may not act as deterrent for the offenders and hence, there is a need to strengthen the existing data protection framework by imposing stringent norms for the entities and penalties for the offenders.

2.34 With the rapidly evolving technology, geographical boundaries have been obliterated in the digital ecosystem. Several multinational companies with minimal physical presence/ infrastructure in the country have large consumer base for communication/ digital services. There is a need to protect the rights of such consumers even qua these service providers.

2.35 Earlier, the telephone instruments used for establishing the calls and speaking with other side person were non-intelligent in the sense that the processing of data, decision making, and recording of the call details used to take place at the network plane. Due to exponential growth in technology, depending upon the use case, now substantial amount of data processing, decision making, and recording of the call details takes place at the device, browser, operating system and application level also. The devices are being packed with more and more intelligence, computing, and processing capabilities thereby playing an active role in the delivery of services to the consumers and accordingly these have become part of the network. It has enabled delivery of rich consumer experience but has also resulted in higher vulnerabilities to user's privacy and data security. Earlier, the service providers used to maintain users information in the form of call data records, records of access to internet etc but today, users data in the form of browsing history, call logs, location data, contact details etc are captured by the devices, browsers, Operating systems, and Applications also. Since these entities are not governed by the license conditions, applicable for Telecom Service Providers, the need for regulation of these entities of the digital eco-system to ensure protection of consumers' privacy and data security is urgent and inescapable.

2.36 Irrespective of whether the application service provider or any other entity in the digital eco-system has level playing field with TSPs or not, security and privacy of the individuals using telecommunication/

digital services, and protection of their personal data is essential. A need, therefore, exists to have uniformly applicable data protection framework for all the entities operating in the digital eco-system.

2.37 Existing laws and license conditions governing the TSPs may be sufficient from a broad perspective as they recognize the privacy rights of users. The Authority is of the view that till such time a general data protection law is notified by the government, the existing Rules/License conditions applicable to the Telecom Service Providers for protection of users should be made applicable to all the entities in the digital eco-system. Also, the government should notify the policy framework for regulation of Devices, Operating Systems, Browsers and Applications.

2.38 In order to ensure privacy of users, right from inception, data protection framework should be embedded and enforced at each point in the digital ecosystem. To accomplish this objective, adopting “Privacy by design” could be a possible approach. "Privacy by design" refers to the conceptualizing and building of systems with a view to ensuring privacy of users’ data. Adoption of Privacy by Design principle implies that appropriate policies, standards, and practices to protect privacy of users must be implemented at every stage where personal data is handled. Further, after obtaining explicit consent of the user, only bare minimum data, which is essential for provisioning of a particular service, should be collected. Collection of unrelated or unnecessary data by service providers in the digital eco-system must be barred. This concept of minimum data collection is referred as “Data Minimisation”. This should be an integral part of the “Privacy by Design” concept.

2.39 **In view of the above, the Authority recommends:**

(a) The existing framework for protection of the personal information/ data of telecom consumers is not sufficient. To protect telecom consumers against the misuse of their

personal data by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem, which control or process their personal data should be brought under a data protection framework.

(b) Till such time a general data protection law is notified by the Government, the existing Rules/ License conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem. For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers, and Applications.

(c) Privacy by design principle should be made applicable to all the entities in the digital ecosystem viz, Service providers, Devices, Browsers, Operating Systems, Applications etc. The concept of "Data Minimisation" should be inherent to the Privacy by Design principle implementation. Here "Data Minimisation" denotes the concept of collection of bare minimum data which is essential for providing that particular service to the consumers.

C. User Empowerment

2.40 The Supreme Court in its judgment on 24 August 2017 stated that the "right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution and as a part of the freedoms guaranteed by Part III of the Constitution". Further, it went on to recognize informational privacy as a facet of the right to privacy and directed the Union Government to put in place a robust data protection regime to ensure protection against the dangers posed to an individual's privacy by state and non-state actors in the information age.

2.41 The epicenter of the entire gamut of Data Ownership, Privacy, and Security revolves around the data consumers (Individuals or Machines). The end user may be more often at a position of low awareness as well as lower bargaining powers when compared to the various entities of the digital ecosystem. This asymmetry is exploited on many occasions by the entities to their advantage. The entities in the digital ecosystem may use personal data of individuals to improve their services; they may even monetize this data by sharing it with third parties. Users often get plagued with bursts of targeted marketing, social media engineering strategies etc not knowing that it was their own data submitted in the past which has enabled such campaigns/strategies. In the absence of necessary data protection framework, the end user does not have any recourse to deal with the exploitation by the entities in the digital ecosystem. Very many times the user is forced to part with his/her personal data with very little information about the scenarios/ uses that his/her personal data would be put to. He has no facilities to access, view, amend, or delete his data submitted. In case of any data breach, he may not even be informed about it till it gets reported. Keeping these concerns in mind, the suggestions of the stakeholders were sought through the CP to empower users so that they can take control of their personal data.

2.42 Most of the stakeholders agreed that the existing framework does not provide the requisite wherewithal to the users to protect their personal data in the digital ecosystem. They were of the view that user consent should be mandatory before sharing his/her personal data for commercial/ Non Commercial purposes. Further, the consent should be based upon the category and sensitivity of the information to be collected and the purpose for which the personal information will be used. Some stakeholders submitted that in case of anonymized data and / or data available in the public domain, users consent may not be required.

2.43 A large number of respondents had submitted that *notice and consent mechanism* as proposed by the Justice A P Shah Committee[10] needs to be instituted for empowering the end users. They were of the view that the present system of agreement which a user is made to accept is very complicated. Usually, the agreements are lengthy, confusing, one-sided favoring the large data controllers, device manufacturers, application and content providers etc. The end user has no option but to accept these to avail the services. Many a time, if the user declines to agree with these agreements, he/she is denied the services. The users, therefore, do not have any other choice but to accept these agreements. Further, in case of data breach or misuse of his/her personal data, the user is neither informed nor does he he/she have *a mechanism for grievance redressal*.

2.44 Some stakeholders were of the view that users should have the right to know the purpose for which his/her personal data is being collected by the entity. Users should also have the right to access, view, edit, delete, and move their personal data collected by the entities in the digital eco-system. User should be able to monitor the usage of his personal data by various entities and no third party should be allowed to utilize a user's data without specific permission.

2.45 Many stakeholders submitted that there is a need to increase *consumer awareness about* digital privacy principles, user rights, and potential harm in case of breaches or consents given unknowingly. They suggested that every company, entity, digital player be required to place its *Data Protection, Security and Privacy Policy in the public domain/on its website*. The Policy may describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed and the reasonable security practices and procedures followed to safeguard the information.

[10] http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

2.46 A large number of respondents were of the view that the user should be informed about the duration for which his personal data would be held by the entities collecting/processing this data. Customer should have the right to stop the services along with the right to be forgotten by seeking the deletion of all the information, which an entity/individual has stored previously. The entities should not store and use the personal information of their customers once they stop using the services/products of that entity, beyond the mandated period under the law.

2.47 Some stakeholders were of the view that user should have the Right to Opt- in \Opt- out for data. Also, Inter Application data transfer that is compliant with the data protection laws should be enabled. User should be able to move his data on will, from one entity to another seamlessly.

2.48 A few stakeholders had submitted that the entities in the eco-system collect personal data from the users even though such data may not be actually required for the functioning of such applications/device.

2.49 Additionally, the stake-holders submitted the following measures to empower the end users/data consumers:

(a) Users should have the right to withdraw their consent for collecting, processing, and sharing of their personal data unconditionally unless it falls under the lawful obligation of the data controller.

(b) Every company, entity, digital player be required to place its Data Protection, Security and Privacy Policy in the public domain and on its website. The Policy may describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed and the reasonable security practices and procedures followed to safeguard the information.

(c) Foreign companies establishing their businesses (Content and App services, Device Manufacturing, Browser, OS etc) in India that connects with users through TSPs must ensure that their local entities adhere to the relevant Indian laws governing data privacy and secrecy.

(d) Data Controllers should not be able to use "pre-ticked boxes" to gain users consent nor imply their consent from other actions.

(e) Right against unfair denial of service in case he decides not to accept the pre-installed one sided end user agreements furnished by various entities before using their services.

(f) In case of a data breach whether reported/not reported, it would be mandatory on part of the Data Controller to inform the user about the data breach within 48 hours from the time of occurrence of breach/time of reporting to the user. The Data Controller should also intimate the user about the actions taken to prevent such breaches.

Analysis

2.50 As brought out earlier in the chapter under the sufficiency of the existing data protection framework, the Rights available to the consumers for data protection are limited. The Service Providers, Devices, Browsers, Operating Systems etc have an asymmetric advantage over the end user who is ultimately forced to accept the one-sided agreements/Terms and Conditions to avail the services, equipments etc.

2.51 Notice, Choice, and Consent are the most important rights that should be given to the data Consumers. As per the Justice A P Shah Committee report, Notice means that a data controller, which refers to any organization that determines the purposes and means of processing the personal information of users, shall give simple and easy to understand notice of its information practices to all individuals, in clear and concise language, before any personal

information is collected from them. Such notices should include disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc. Similarly, Choice and Consent implies that a data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Consent may be considered to be a powerful means of protecting an individual's information. An individual is best placed to decide the sensitivity of his/her information rather than the Government or any other agency deciding it on his behalf. For meaningful use of these rights by consumers, there is a need to increase consumer awareness about digital privacy principles, user rights, and potential harm in case of breaches or consents given unknowingly.

2.52 The issue of Consent has been addressed by the Government to some extent in the past where in the guiding principles for sharing of user data across services after obtaining user consent have been outlined in the following key policy documents:

(a) The policy on "Open Application Programming Interfaces (APIs) for the Government of India[11]" published by MeitY.

(b) The "National Data Sharing and Accessibility Policy (NDSAP)-201212" by the Department of Science and Technology.

Subsequently, the "Electronic Consent Framework[13]" has been developed by Meity incorporating the guiding principles mentioned in the policy documents mentioned above.

2.53 Subsequent to the development of the Electronic Consent Framework by MeitY, RBI, on behalf of all the Financial Sector Regulators, has

[11] http://meity.gov.in/writereaddata/files/Open_APIs_19May2015.pdf
[12] https://data.gov.in/sites/default/files/NDSAP.pdf
[13] http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

issued the master direction known as the "Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016" for all the Financial Sector participants. It has the concept of the data fiduciary (Account aggregator) that, after obtaining the consent of the customers electronically, collects the information from providers of information based on the standardized consent artifact and securely transmits the same to users of the information. This direction is for the benefit of financial sector consumers, as it empowers them to use their personal data, in the form of financial transactions history, for availing new services from any other competing service provider. In light of the same, there is a need to develop a similar consent framework for telecom sector. Once the framework for data privacy and security is approved by the Government, the Authority may work on such framework.

2.54 Many times, end user agreements/terms and conditions that a user is served at the time of availing any services, procuring any device etc are one-sided, complex, lengthy, full of legal jargon and in a language that a user may not understand. The user has no other choice but to accept them to avail the services of the entity. Since India is a multi-lingual country, these agreements, notices etc should be provided in an easy to understand, short, multi-lingual format for the benefit of the users.

2.55 In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism have to be built-in by the service providers. User should be able to selectively give his/her consent for each purpose separately rather than a blanket consent for all conditions. Also, the service provider should not deny all the services to user on the pretext that the user has not given blanket consent for all conditions. Any form of implied consent (water-fall model) by the service should also not be permitted. Further, in spite of the users' consent for specific purposes, data controllers as well as

data processors or any other entity handling personal data of the user should be made accountable in case of any unintended harm to the users. Mere accordance of consent by the user to use his/her personal data should not imply that the data controllers, data processors or any other entity in the digital eco-system have been absolved of their responsibilities from any unintended damage caused to the users.

2.56 On many occasions the end user of the device is served with one sided pre-stored agreements on these devices after he has bought them. In case the user decides not to agree with these terms of agreement he may not be able to use all the features of the device. Many of such devices are sold with a set of pre-installed applications, which otherwise are not necessary to operate the device. This usually includes a Search Engine, a messaging service, cloud storage, a video service, map services, and browser etc. These Apps in many cases are integrated with the operating system of the device. In case, he agrees to such conditional agreements; the operating system of the device and these pre-installed applications may transfer/upload/utilize the users' data stored/ being used on the device with/without his consent. Simultaneously, if a user wants to share his/ her own data, generated while using the telecommunication/ digital services, with any third party App, the data controller i.e. the operating system of the device or the corresponding application may not allow him/ her to share such data in spite of the fact that the primary right on such data is of the owner of the data. It has also been noted that such pre-installed Applications can neither be deactivated nor deleted. Such situations are detrimental to basic consumer rights and his right to privacy. User should therefore be empowered to delete such pre-installed applications which otherwise are not necessary to operate the device. Deletion of pre-installed applications, which are not part of the basic functionality of the device, should not hamper the functionality of these devices. The user must be free to install/ delete an application at his/her will and the device should in no manner

restrict/disallow the user to do so. Functionality of auto-upload of user data stored on the device should be disabled by default.

2.57 Many times, it has been noted that some entities in the digital eco-system collect personal data of the users even when such data may not be actually required for the functioning of such application/device e.g. for using an application that activates flashlight as a torch on a mobile device, the application seek permission for access to camera, microphone, and contact list etc. The flash light application simply creates a logical circuit between the battery and the camera flash light and does not require access to camera, microphone, or contact list for its operation. It has also been reported that the applications may deploy a waterfall model of consent wherein once an entity is given consent by the user for a particular application or service, the entity translates the consent to many other entities on its own without obtaining explicit consent/knowledge of the user which is a serious breach of users personal data, choice, and consent. Concept of Data Purpose limitation and Collection limitation was proposed by the Justice A P Shah Committee, wherein a data controller shall only collect personal information from data Consumers as is necessary for the purposes identified for such collection. It is, therefore, important that entities in the digital ecosystem should not be allowed to have indirect or inferred consents. It was brought out in paragraph 2.38 that data minimization should be incorporated as an integral part of 'privacy by design' principle. It is reiterated that the concepts of Purpose limitation and Collection limitation have to be enforced rigorously. It has been seen that there is no mechanism by which the user can know about the type of his personal data that is being collected by various entities, the potential use that this data would be put to by the entities, the duration for which this data would be held, the location of personal data, whether the data being sought by the entity is actually required to avail the services, the format in which this data would be stored. The end user neither has access to his

personal data, nor can he edit, delete or move his data at will. In view of the foregoing, the end users have to be empowered by bestowing upon them the rights which can facilitate them in enjoying better data privacy.

2.58 On many occasions it has been found that a user is stuck to a particular device, application or service as his personal data cannot be migrated to another device, applications etc. This limitation is exploited by the entities in the eco-system to their advantage. Even if the user discarded the device or unsubscribed services, his personal data continued to be available with the previous device or service provider. The issue can be addressed by implementation of data migration/ data portability policies in the data privacy framework. Related to this issue is the users right to be forgotten, where in it becomes obligatory on the part of the data controller to delete all the information of the data Consumers held with them. Provisions of Right to be forgotten have also been included under ***Article 17***[14] of the ***EU-GDPR***. The right to be forgotten would empower the user to delete past data that he may feel is unimportant or detrimental to his present position. Past data could be in terms of photographs, call records, video clippings etc that may potentially harm the reputation of the data consumers. Since information related to a person may be termed as his personal data and that the user owns such data hence he should be empowered to delete all such data at his discretion. It is also important to note that the "*Right to be Forgotten*" should be implemented with necessary safeguards as there may be requirements by the Law Enforcement Agencies/Licensing conditions etc wherein retention of data in terms of quantum as well duration would be necessary as per applicable legal framework, licensing conditions, hence "*Right to be Forgotten*" should be implemented with applicable restrictions. Further, to address the complaints of users about any misuse of their personal data or regarding violation of the data

[14] https://gdpr-info.eu/art-17-gdpr/

protection framework by any entity in the digital ecosystem, *a* mechanism for grievance redressal should be put in place.

2.59 **In view of the foregoing, the Authority recommends the following:**

(a) The Right to Choice, Notice, Consent, Data Portability, and Right to be Forgotten should be conferred upon the telecommunication consumers.

(b) In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.

(c) For the benefit of telecommunication users', a framework, on the basis of the Electronic Consent Framework developed by MeitY and on lines of the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users.

(d) The Right to Data Portability and Right to be Forgotten are restricted rights, and the same should be subjected to applicable restrictions due to prevalent laws in this regard.

(e) Multilingual, easy to understand, unbiased, short templates of agreements/ terms and conditions be made mandatory for all the entities in the digital eco-system for the benefit of consumers.

(f) Data Controllers should be prohibited from using "pre-ticked boxes" to gain users consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.

(g) Devices should disclose the terms and conditions of use in advance, before sale of the device.

(h) It should be made mandatory for the devices to incorporate provisions so that user can delete such pre-installed applications, which are not part of the basic functionality of the device, if he/she so decides. Also, the user should be able to download the certified applications at his/ her own will and the devices should in no manner restrict such actions by the users.

(i) Consumer awareness programs be undertaken to spread awareness about data protection and privacy issues so that the users can take well informed decisions about their personal data.

(j) The Government should put in place a mechanism for redressal of telecommunication consumers' grievances relating to data ownership, protection, and privacy.

D. Rights and Responsibilities of Data Controllers

2.60 Data Controllers are those entities in the digital eco-system who, either alone or with others, determine the purposes and means of processing of personal data. Control refers to the competence to take decisions about the contents and use of data.[15] The entity that controls the data i.e. determines the purposes of processing, the means of processing, the sharing of data etc., should be primarily responsible for the compliance with data protection requirements. Data processors on the other hand are those entities who process data on behalf of data controllers.

2.61 In practice Data Controllers can be providers of Devices, Operating Systems, Applications, Web Browsers, Service Providers etc. as they collect, store, and control telecommunication consumers personal data.

---

[15] Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowofpersonaldata.htm#part1.

2.62 As discussed in the previous sections, users in India have limited rights to access, edit, or delete personal data held by various entities. The recent instances of data breaches/data thefts in the world demonstrate the tremendous power that data controllers and processors can have – insofar as data analytics has purportedly been used to influence voter behavior in different countries. At the same time, it is also worthwhile to note that data is required for creating and driving new businesses and innovation, and further that unnecessary or excessive regulatory costs on data driven businesses may only hamper growth of the sector.

2.63 Keeping in mind the balance required to be struck between the rights of data consumers and the need to encourage data driven businesses, the Authority posed a question concerning the rights and responsibilities of data controllers in the digital ecosystem.

2.64 In response to the question, a majority of the stakeholders were of the view that the rights of the data controllers cannot supersede the rights of the data consumers over his personal data. A few respondents submitted that the rights and responsibilities of data controllers should be similar to other entities of the ecosystem while some others had proposed that separate sectoral guidelines may be proposed for data controllers of each sector.

2.65 Many stakeholders were of the view that a data controller should collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual, and only after the individual has consented to the new purpose, should the data be processed for such purposes.

2.66 One respondent submitted that there needs to be clear reporting requirements for data controllers to publish periodic transparency reports. These reports should include information about data processing practices for better information of users. Further, the

reports should also highlight any security incidents and steps taken by the data controllers to address the issues. Accordingly, the policies prohibiting disclosures about interception, monitoring, and decryption need to be modified.

2.67 Some stakeholders had opined that responsibilities for data controllers should include adherence to and expert knowledge of all applicable data protection laws, regulations and practices affecting the organization in question. In addition, data controllers must always maintain a direct reporting access to the highest level(s) of an organization; issues like information and data security are enterprise-level concerns, and those responsible for their safeguarding should liaise directly with the decision makers at the pinnacle of the organization. Creating a Data Control Authority (possibly as a division of a proposed Data Protection Authority) as a mechanism for governing, regulating and educating data controllers is strongly recommended. Centralizing these functions would enable better information dissemination to all involved.

2.68 Many respondents were of the view that regulatory principles are required to be defined for the data controllers, data processors etc by the government. Once defined, a centralized Data Protection Authority should regulate and enforce the framework on all the stakeholders.

2.69 Some stakeholders had submitted that it was best left to the industry to self regulate the data controllers by having in-house industry best practices to govern and regulate. The data controllers would be ranked by the industry itself based on their performances and the best practices followed by the data controllers.

2.70 Some stakeholders have proposed the following responsibilities of the data controller:

(a) Data controllers must be held responsible for ensuring the security of personal and sensitive personal data. There should be

an oversight mechanism for Rule 8 of the SPDI Rules, to ensure that data controllers are taking enough measures to protect the data.

(b) Data controllers must give notice of data breaches to CERT-in, sectoral regulators and affected data consumers.

(c) Data controllers must notify data consumers about what data will be collected, for what purpose, by whom, who to contact in case of grievance, what would be the effect of agreeing to or disagreeing to the collection of any data. Such notices should be simple and easy to understand, and must be available in English as well as the vernacular language of the region in which the data controller is providing their services.

(d) Data controllers must ensure that anyone with whom personal information or sensitive personal data or information is shared obeys the same standards of security and privacy as are applicable on the data controller. The transfer of data should not be allowed without explicit consent from the data consumers. Transfer of data must not be allowed to another country unless the country to which the data is being transferred offers similar levels of protection to personal and sensitive personal data.

(e) Personal data must not be published openly. Any exceptions such as for journalism, research, household use etc., must be narrowly defined. Broad exceptions would serve as a source of exploitation.

(f) Any collection, use, storage or transfer of personal data must not be done without prior explicit informed consent from the data consumers.

(g) Data controllers must be transparent about their security procedures and practices, and data collection, use and transfer policies and these should be published in the form of a privacy policy.

(h) Data controllers must train their staff in security procedures.

(i) Data controllers must ensure that access to personal and sensitive personal data is restricted to only those people who must necessarily have access to it in order to perform their duties. In all other instances, such data must be out of reach for employees and outsiders.

Analysis

2.71 Currently, the term "data controller" is not defined in any legislation or regulation in India. The IT Act utilizes the term 'Body corporate' which limits the application of extant privacy law (for instance by excluding certain government agencies such as Ministries and Departments). There is, therefore, an urgent need for defining the concept of data controllers and data processors in a comprehensive manner, keeping in view the variety of entities who may gather and process personal data of individuals. Thereafter, the privacy framework may lay out relevant obligations and practices that should be observed by all such entities.

2.72 Segregation of entities into data controllers and data processors is useful in apportioning responsibilities on the various parties involved in dealing with personal data in the digital ecosystem. Often, entities will merely collect and pass on personal data to external entities for further analysis. It is therefore necessary to ensure privacy protections of individuals from all entities in the digital ecosystem.

2.73 Since data controllers collect and store users' data; they gain unhindered access to such data which can be put to use by them at their discretion. The user has no control over this data in the absence of any regulatory framework. Hence, the scope of powers that data controllers have should be strictly limited by the nature of consent provided to the data consumers or as otherwise required in the law.

2.74 One of the first steps in ensuring adequate privacy protection for users is to provide meaningful choice and ensure appropriate

information is provided to users about the privacy practices and policies of data controllers. Accordingly, appropriate responsibilities and obligations must be placed on data controllers to ensure proper notice regimes are implemented, there is transparency about information practices, users are empowered through data portability mechanisms, informed of data breaches, provided adequate remedies, etc. In addition, it should be incumbent on data controllers and processors to implement appropriate security measures, privacy by design principles, etc. The "Principle of Accountability" should be made applicable to the data controllers as well as processors so that they can be held accountable for any unintended use or misuse of data.

2.75 In addition, it is important to recognise that ownership rights of the individual/user over his/her personal data are supreme and should normally not be superseded by the rights of data controllers, data processors, or any other entity in the eco-system. This necessarily implies that appropriate systems of transparency and accountability must be implemented by all data controllers and processors. This should include internal systems of grievance redress as well as institutional systems of enforcement.

2.76 The rights and responsibilities of Data Controllers and Data Processors have to be similar for all sectors of the economy. Accordingly, such rights and responsibilities of Data Controllers and Data Processors may become part of the Data Protection Framework being developed by the Experts Committee under Justice B. N. Srikrishna. Therefore, the Authority at this juncture has decided not to make any recommendations on the Rights and Responsibilities of Data Controllers. However, the Authority may revisit this issue later on.

E. Technology Enabled Architecture to audit use of Personal Data and monitor the Digital Ecosystem.

2.77 Enforcement of the Data protection framework requires that Complaint Registration, Investigation, Auditing, Imposition of Penalties, and grievance redressal mechanisms to be in place. Audit is required to ascertain the compliance of systems, policies, and practices by an entity with the data protection framework.

2.78 With the development of newer technologies, the degree of sophistication, and speed of data thefts are growing day by day. Due to voluminous data on the internet, it becomes very difficult to monitor compliances and carryout real time audit. Moreover, automated audit mechanism would require deep packet inspection of every data packet moving on the internet; which may in itself tantamount to intrusion in privacy of the data consumers.

2.79 The entities in the digital eco-system are increasing exponentially. Further, the situation would become alarming when viewed with the number of M2M devices in near future. The personal data collected by the data controllers and processed by the data processors would be in several Zetta Bytes. Hence, it would be humanly impossible to monitor the entire eco-system to check incidents of data breach or data misuse. Enforcement of data protection framework would therefore not be possible in the absence of a robust Audit framework.

2.80 The Authority, having realized the criticality of the issue, had raised questions in the CP and views of the stakeholders on the necessity to establish technology enabled architecture to audit use of personal data and monitor the digital ecosystem were sought. Further, stakeholders were also required to comment on the efficacy of establishing of such a system by the government.

2.81 In response to the question on technology enabled architecture to audit use of personal data and monitor the digital eco-system, some

stakeholders submitted that though audits are important but they have limited utility, as they can only look at aspects of procedural compliance and need to be complemented with robust mechanisms for redressal and comprehensive policy. Adoption of a technical framework without adequate development of a rights based data protection framework may not provide any solution for data security or individual privacy. Further, an automated audit system would by itself lead to data centralization and pose risks to users. There would be further problems in its implementation as it would in a sense be a universal backdoor to all internet applications and services. Hence, without adequate security such a compliance system by itself may pose as a security risk.

2.82 Some stakeholders submitted that creation of technology enabled audit architecture is not recommended due to following reasons:

(a) Higher compliance costs.

(b) Frequent obsolescence of technology.

(c) Differences in business models, products/services, data collection practices, and the complexity of algorithms of various entities in the digital ecosystem.

(d) It may create geo-fences for cross-border businesses.

In view of the forgoing the stakeholders recommended that self-regulation coupled with internal and third party external audits. Further, they said that format, structure, periodicity of certifications may be worked out in consultation with stake holders. They were of the view that all players in the eco-system be subjected to these audits.

2.83 One respondent submitted that there are limitations to an audit based system in which users have little recourse or remedy. A mix of proactive reporting requirements such as transparency reports and

data breach notification requirements, enforcement and adjudication forums are some of the measures which may safeguard user interest.

2.84 Few TSPs were of the view that TSPs already have well established, adequate mechanism for users' data protection and there is no need for creation of technology based audit mechanism as technology alone cannot do the entire audit, human intervention would be required.

2.85 Some stake-holders, however, supported the concept to create a technology-enabled architecture to audit the use of personal data and associated consent. Such a mechanism would not only benefit the government but also protect the data consumers. Some stakeholders submitted that a central register containing information for each data controller should be created.

2.86 Some respondents submitted that human intervention with support of technology based audit architecture (for checking and keeping track of the consent logs) will help in compliance monitoring and assessment by the entities for e.g., a "fair processing notice" is expressed in a myriad of different ways and contexts, so it is hard for a computer to understand whether the notice is sufficient. In such cases, best practice is for the companies to document their policies and processes and adopt principles that increase accountability. The compliance can be self-assessed by these entities or by accredited standard bodies like ISO for security; or by auditing firms that have the requisite expertise and capability.

Analysis

2.87 Audit is an important facet for enforcement of data privacy framework. The Audit framework should not be restrictive yet at the same time it should be adequate to protect the interests of the stakeholders in the ecosystem.

2.88 In India, the internet proliferation as well as the consumer awareness is less when compared with developed nations. As brought out earlier,

existing legal framework available in India to address the data privacy issues is in-adequate.

2.89 A purely human/manual audit approach may not be advisable due to the magnitude of data being handled, complexities of the technologies at each level, and the need for real time audit of the systems. Moreover, the technology changes occur at a very rapid pace and it would be virtually impossible for the pool of auditors to keep in sync with these changes.

2.90 Complete Technology based audit mechanism may also have challenges due to algorithmic biases, justified interpretation of laws by machines may not be possible e.g., a "fair processing notice" is expressed in a myriad of different ways and contexts, so it is hard for a computer to understand whether the notice is sufficient or not.

2.91 A hybrid approach with a combination of Technology and the human intervention may be more suited to our context. In case of EU GDPR, it can be seen that a hybrid approach to Audit mechanism has been adopted (Ref Article 28[16],39[17],47[18] and 58[19] of EU GDPR).

2.92 The issue of technology enabled audit and monitoring of the digital ecosystem is complex and would have to be derived based on the overall data privacy framework of the country. Primarily, such monitoring and audits would be applicable for data controllers and data processors. As discussed earlier, issues relating to rights and responsibilities of the data controllers may be revisited later-on after the Data Protection Law would be in place. In view of the foregoing, the Authority has decided not to make any recommendations on this issue at this stage. Once the data privacy laws for the country are enacted, the Authority may, if necessary, revisit the issue.

[16] https://gdpr-info.eu/art-28-gdpr/
[17] https://gdpr-info.eu/art-39-gdpr/
[18] https://gdpr-info.eu/art-47-gdpr/
[19] https://gdpr-info.eu/art-58-gdpr/

F. Security of Data and Telecom Networks.

2.93 Telecom networks may be viewed as carriers of voluminous data traffic between the entities of the digital eco-system. The need to ensure security and privacy of data being carried on these networks as well as the security of the telecommunication networks are therefore of paramount importance. TPSs may also qualify as Data Controllers as they capture large amount of users' data in the form of call logs, browsing history, personal details etc. Since data controllers are responsible for the security and privacy of consumers data, it is important to examine the various provisions under the regulatory framework applicable to the TSPs to ascertain whether adequate measures exists to ensure the security of telecom networks as well as the traffic which these networks carry.

2.94 Against this background, the Authority raised the questions pertaining to the measures required to ensure safety and security of telecom networks in the CP.

2.95 The TSPs were of the opinion that the existing regulatory framework for the security of telecom networks is adequate. However, some of them felt that use of mandatory 40 bit encryption keys for securing the data on telecom networks was outdated and there was a need to re-examine the basic encryption standards applicable to the TSPs. One of the TSPs recommended the creation of a platform for all the TSPs to share amongst themselves the vulnerabilities and information about the breach incidents to initiate proactive strategies to deal with such eventualities.

2.96 One of the stakeholders submitted that following additional steps need to be taken to ensure the security of telecom infrastructure and the digital ecosystem as a whole:

(a) Companies should have in place and disclose information about their process for responding to data breaches, and must publish

periodic reports about any security incidents and how they have been responded to.

(b) All user communications should be encrypted and this should be enabled by default.

(c) Companies should regularly publish educational material on security for users.

2.97 One of the stakeholders was of the view that information related to various incidents - network threats, breaches, malware, DOS attacks, etc must be shared proactively with the relevant players in the ecosystem and telecom subscribers, in a time-bound manner to reduce potential damage.

2.98 Some respondents submitted that one of the preferred approaches could be to encourage the White-Hat community to constantly monitor and proactively report possible threats to the appropriate authority. Use of bug-bounty programs may be encouraged, community building and other such measures may be adopted to build a large base of volunteers/professionals who ensure that the security of critical systems is up-to-date.

Analysis

2.99 Since the TSPs are licensed entities in the digital ecosystem, they are governed not only by the License conditions and sector specific laws but they are also required to adhere to several other laws. Some of the important security conditions and standards applicable to TSPs are listed below:-

(a) Adoption of ISO27001 or sectoral-standard (***Sec 43 A, IT Act,2000***);

(b) For Network elements: ISO/IEC 15408 (***UL Condition 39.6***);

(c) For Management: ISO 27000 (***UL Condition 39.7***),

(d) 3GPP2 security standards: (***UL Condition 39.7***).

(e) Certification : (***UL Condition 39.7***)

(f) Incorporation of contemporary security standards: (***UL Condition 39.8***).

(g) Technical Scrutiny and Inspection: (***UL Condition 39.2***)

(h) Facilities for monitoring of all intrusions, attacks and frauds: (***UL Condition 39.10***)

(i) Facilities for monitoring by designated security agencies: (***UL Condition 39.12***)

(j) Organizational security policy, management, network forensics, hardening, penetration test, risk assessment: (***UL Condition 39.5***)

(k) Maintaining records of software details etc: (***UL Condition 39.9***).

(l) Adequate and timely measures to ensure that the information transacted through a network by the subscribers is secure and protected.(***UL Condition 39.23(iv)***)

(m) Data Localization of traffic: (***UL Condition 39.23(iii))***

In view of the foregoing, it may be inferred that the TSPs have a fairly robust regulatory framework for ensuring the data privacy and security of its consumers.

2.100 Encryption is an important aspect for ensuring the safety and security of the content. In case of the TSPs, use of bulk encryption as well as deployment of high order encryption standards has been prohibited. Since the TSPs provide connectivity to various entities in the ecosystem, the robustness/ strength of the data protection is dependent upon the encryption standards used by each entity. Presently, non-uniform encryption standards are being followed by

various sector regulators. Encryption standards stipulated by various sector regulators are as follows:

(a) SEBI[20]- Guidelines on Internet Trading: 64/128 bit encryption.

(b) RBI[21]- Guidelines on Internet Banking: Minimum SSL/128 bit encryption.

(c) UIDAI - AADHAAR authentication API specification -Version 2.5[22]: Personal Identity Data (PID) block, data should be encrypted with a dynamic session key using AES-256 symmetric algorithm (AES/GCM/No Padding). Session key, in turn, is encrypted with 2048-bit UIDAI public key using asymmetric algorithm (RSA/ECB/PKCS1Padding)

(d) DoT: Mandates evaluation and approval of encryption equipment, Prohibits bulk encryption and mandates use of maximum 40 bit Key length for encryption. For higher level encryption, DoT mandates seeking of written permission and deposit of decryption keys with them.

Robustness of the user's data privacy and data protection in the digital ecosystem depends upon the weakest link in the ecosystem. Different sectors are following different encryption standards, hence there is a need for harmonization of Encryption standards across the sectors in our country. Accordingly, the Government should notify the National Policy for Encryption of personal data, generated and collected in the digital eco-system.

2.101 For ensuring the end-to-end security of the personal data, its encryption during the motion as well as during the storage in the digital ecosystem is necessary. Decryption could be permitted on a

[20] https://www.sebi.gov.in/sebi_data/commondocs/anncir2_p.pdf
[21] [21] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf
[22] https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf

needs basis by authorized entities pursuant to consent or as per requirement of the law.

2.102 In case of breaches, data thefts etc timely sharing of information with the data consumer and various entities in the digital ecosystem is essential to mitigate the losses/ breaches and prevent their future occurrences. It has been seen that a system of rewards/incentives for compliance and penalties for willful defaulters works best. Hence, a system of voluntary disclosure of information between the entities should be created and incentives/rewards should be given to the service provider/entity giving advance information about any cyber threat/incident. A platform for sharing of such real-time information should be created and it should be made mandatory for all the service providers to be a part of this platform. Active sharing of information about possible threats and vulnerabilities among the service providers would facilitate plugging of gaps in the existing systems, evolution of best practices and voluntary sharing of information. This in turn would result in creating a safe and secure telecom network.

2.103 **In view of the foregoing, the Authority recommends that:**

(a) Department of Telecommunication should re-examine the encryption standards, stipulated in the license conditions for the TSPs, to align them with the requirements of other sectors.

(b) To ensure the privacy of users, National Policy for Encryption of personal data, generated and collected in the digital eco-system, should be notified by the Government at the earliest.

(c) For ensuring the security of the personal data and privacy of telecommunication consumers, personal data of telecommunication consumers should be encrypted during the motion as well as during the storage in the digital

ecosystem. Decryption should be permitted on a need basis by authorized entities in accordance to consent of the consumer or as per requirement of the law.

(d) All entities in the digital ecosystem including Telecom Service Providers should be encouraged to share the information relating to vulnerabilities, threats etc in the digital ecosystem/ networks to mitigate the losses and prevent recurrence of such events.

(e) All entities in the digital ecosystem including Telecom Service Providers should transparently disclose the information about the privacy breaches on their websites along with the actions taken for mitigation, and preventing such breaches in future.

(f) A common platform should be created for sharing of information relating to data security breach incidences by all entities in the digital ecosystem including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem including telecom service providers to be a part of this platform.

(g) Data security breaches may take place in-spite of adoption of best practices/ necessary measures taken by the data controllers and processors. Sharing of information concerning to data security breaches should be encouraged and incentivized to prevent/ mitigate such occurrences in future.

G. <u>Measures to encourage creation of new data based businesses</u>.

2.104 Data Analytics is an important emerging area that may transform the delivery of services and products in future. It may have immense societal and economic benefits. Data Analytics may be useful in solving several issues like the traffic congestion, disaster

management, supply chain management, etc. It may also facilitate targeted product delivery system, better health care management, personalized education to students, better policy formulation, better law enforcement etc.

2.105 The most fundamental commodity required to operate a data based business is the data itself. Making available large amount of data that is being generated by the individuals or the machines in the ecosystem without any safeguards may not be advisable as it may lead to compromising the privacy and security of the users data. It may also tantamount to the violation of users privacy rights. While it is important to safeguard the interests of the users, it is also important to ensure that new products and services are introduced for the betterment of the society. In view of the foregoing, the Authority sought the views of the stakeholders on the measures that may be adopted to encourage the data based businesses in our country.

2.106 In response, many stakeholders were of the view that public policy focus should be on providing regulatory certainty and consistency, preventing harm to users, preventing misuse of Personal Information/Personal data of the users and making companies accountable through self-regulation. Further, they felt that Government should focus on building an adequate implementation ecosystem, including institutional capacities and capabilities, effective grievance redressal system, user awareness, active civil society, and impetus to research and development. They also submitted that the regulatory framework should be applicable uniformly to all the players in the ecosystem. Some respondents suggested following measures to achieve the creation of new data based businesses :-

(a) Anonimization of data sets.
(b) Enabling Data Portability.
(c) Creation of public data sets.
(d) Encouraging business related to compliance and data security.

2.107 Some stakeholders were against the data driven businesses and submitted that there should be no relaxation in rules or regulations in order to promote new businesses monetizing users data.

2.108 Few stakeholders representing the software industry were of the opinion that over-regulating the market can interfere with the freedom of trade and dis-incentivize competition, investment, trade, and create business inefficiencies. The government's role should be only of a catalyst and it should create a favorable environment for doing business.

2.109 Some TSPs have submitted that to encourage data driven businesses, the government should implement programs and implement measures that increases consumer awareness and helps in building trust of individuals whose data is being collected by various entities.

2.110 One respondent had submitted that there should not be any relaxation in the rules or any prejudiced application of regulations in order to promote new businesses monetizing data, as it may lead to compromising the privacy and security of user's data.

Analysis

2.111 Data Analytics industry may be considered as a new growth engine of the future as it would be instrumental in solving many modern day issues[23],[24]. Some of the attributes of Data Analytics business are that it is technology intensive, rapidly evolving, high investment in R&D, requires specialist work-force etc. World over, entrepreneurs, MNCs, Governments etc have realized the importance and the capability of Data Analytics and significant efforts are being made to develop this industry.

[23] http://asiandatascience.com/wp-content/uploads/2017/11/eBook-Big-Data-2017-Market-Statistics-Use-Cases-and-Trends.pdf

[24] https://wikibon.com/executive-summary-big-data-vendor-revenue-and-market-forecast-2011-2026/

2.112 Being a large country with a young and upwardly mobile population, India offers a unique opportunity to the entrepreneurs to service the large consumer base. Government may also use data-analytics for the larger good of the citizens. For the people/consumers to share their valuable personal data with the entities in the ecosystem, it is important that the consumers have confidence and trust in the agencies collecting their data. The trust and confidence can be built by having in place a robust data protection framework for the country.

2.113 Data Analytics may act as a force-multiplier in development of our country due to its multi-dimensional benefits. The government is sanguine with the importance of the issue, however equally important is the issue related to data privacy of its citizens. Government has constituted an Experts Committee under Justice B N Srikrishna who are developing the data privacy framework for the country hence the Authority has decided not to give any recommendations at this juncture on this issue.

H. Data Sand-Box

2.114 A Data Sand Box may be visualized as an entity that anonymises data sets which can be utilized by the service providers/ businesses to design new products and services for the benefit of customers and growth of their businesses.

2.115 The Authority, with a view to understand the need, mechanisms, controls, access, and the entities who should be made responsible to establish data sandboxes, raised the question in the CP.

2.116 In response to the question most of the respondents were of the view that Govt. or its authorized authority shouldn't set up a data sandbox that may allow regulated companies to create anonymous data sets due to following reasons:

(a) It may create roadblock to emerging dynamic business models by chocking investments and innovation incentives.

(b) Aggregation of information in the form of freely available data sets may lead to higher vulnerabilities.

(c) Govt has limited incentives in investing in cutting edge technologies.

(d) It would result in violation of Article 300A of the constitution which prohibits the state from depriving someone of their private property except through statutory law.

(e) It would be difficult to implement concepts of notice, choice, consent, purpose limitation, collection limitation, or right to object in a data sandbox.

Further, they submitted that sharing of anonymized data between the entities can be preferably based on mutual contracts.

2.117 Some respondents were of the view that the Government may set up a data sandbox only if entities can participate on a voluntary basis and only if the data that is shared on such a data sandbox is raw data and not processed or analyzed data. Further, datasets should be anonymised to ensure privacy of users personal information.

2.118 Few stakeholders had submitted that government should continue to promote publication of data by government. agencies under the open data policy. The regulators and government have a significant amount of data that can be anonymised and included in the open data sandbox that would improve transparency and help in development of newer services.

2.119 Some respondents had submitted that establishment of data sandboxes may benefit the consumers as well as the businesses. The consumers would get access to better services and products while the

businesses would be able to generate revenues by offering these services and products to the consumers.

2.120 One of the respondent was of the view that Re-profiling from anonymised data is possible and hence anonymisation may not help in data protection. Further, the respondent cited two research reports, one from the University of Texas[25] and the other from the Colorado Law Legal Studies Research[26] which showed the possibility of re-identification of users from the anonymised data sets. Since possibilities of re-identification exist, Re-Identifying, De-Identifying data should be treated as an offence.

Analysis

2.121 Development of Goods and services undergo several iterations and testing before they are launched commercially, this may be necessary to ascertain their operational and commercial viability by the consumers as well as the service providers/ manufacturers. With the modern day technologies, it may be possible to create more robust and efficient algorithms that can be utilized to create better services and products. Testing of algorithms on data sets before production of goods/services may be a cost effective methodology since the testing can be carried out on computers with minimal resources.

2.122 Annonymised data sets carved out of existing personal data held with various entities in the digital eco-system for testing the algorithms may be a dangerous proposition due to possibilities of Re-profiling/ Re-Identification of the users[27]. As mentioned earlier, suitable standards for de-identification/annonymisation would have to be

[25] Narayanan, A. and Shmatikov, V, Robust De-anonymization of Large Sparse Datasets, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf
[26] Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: https://ssrn.com/abstract=1450006
[27] 5 Nate Anderson, "Anonymized" data really isn't—and here's why not, available at https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

arrived at before permitting use of de-identified/annonymised data sets for the data sand boxes.

2.123 Government, has been publishing open data sets of its various Ministries regularly on their websites, and, in a way, it does provide data sets to the industry/service providers. However, mandatory sharing of data by all the entities with the government and establishing of data sandbox by the government would entail substantial investment in IT infrastructure like data centres, storage farms, power etc on the part of government. Presently the data protection framework for the country is under development. Moreover, the issue of data sand box would require further deliberations post implementation of the data privacy law for the country. In view of the foregoing, the Authority has decided not to make any recommendations related to data sand box at this juncture.

I. Legitimate exceptions to privacy regulation

2.124 The Authority has previously noted the importance of putting in place adequate privacy protections to protect the personal data of users. However, as noted by the Supreme Court in the Puttuswamy case, privacy is not an absolute right and must be balanced, based on the context, with other rights and obligations - for instance the duty of the state to ensure territorial integrity and security of citizens. Accordingly, it is essential that well tailored exceptions are crafted for any privacy policy permitting inter alia exceptions for law enforcement, for purposes of research, and so forth. Any exceptions must however be necessary and proportionate - implying that they must be narrowly tailored to meet specific and legitimate requirements. Further, appropriate systems of checks and balances must be introduced to ensure that the balance between privacy rights and the exceptions thereto are appropriately maintained.

2.125 The Authority therefore requested inputs from stakeholders on the legitimate exceptions to the application of data privacy framework and

the checks and balances that need to be instituted to meet the legitimate requirements of the law enforcement agencies.

2.126 In response to the question raised in the CP, most of the stakeholders were of the view that exceptions to the application of data protection framework should include the following:

(a) Issues when there is a threat to national security and territorial integrity;

(b) To maintain public order;

(c) Investigations of crime by law enforcement agencies (LEAs).

2.127 Some stakeholders were of the view that TSPs are governed by a licensing framework which puts them under obligation to provide LEAs with personal data of users (for instance, call data records and location). They further submitted that Over-The-Top (OTT) service providers are under no corresponding obligations to provide such data to LEAs. These stakeholders argue that all entities in the digital eco-system that provide similar services should be subject to the same regulatory requirements.

2.128 Some TSPs submitted that they should be provided with a legal process to challenge requests by the LEAs when they believe that requests for data may exceed the LEAs authority or are otherwise deficient in some manner.

2.129 One stakeholder submitted that the existing data access requests system is governed by the IT Act and the Indian Telegraph Act, 1885. Both the statutes provide varying standards and procedures for interception thereby creating differences in the interception regimes. These differences have led to creation of an ambiguous regulatory regime which is prone to misuse. Further the stakeholder cited the recommendations of Justice A P Shah committee which proposed harmonization of the interception regime in India and inter alia

suggested that each relevant legislation be amended to comply with the National Privacy Principles. This stakeholder recommended that any data protection law should clearly establish the circumstances under which Government authorities may issue demands for personal information and further there must be a requirement for judicial interventions and oversight over such activities.

2.130 A few respondents submitted that companies should be permitted to report publicly on the number of demands that they receive for personal information on a periodic basis, in order to increase transparency and to inform public debate about the relevant laws.

Analysis

2.131 When it comes to the issue of legitimate exceptions to the privacy regime concerning TSPs, there are primarily three issues at hand:-

(a) Exceptions concerning requests by law enforcement agencies and /or as may be required under law,

(b) Exceptions for purposes of carrying out research and statistical analysis,

(c) Exceptions for the purpose of ensuring optimum quality of services.

It was pointed out by the Supreme Court of India in the Puttuswamy case, all exceptions in addition to meeting a legitimate aim, must be necessary and proportionate. Hence the same principles must be applied to carving out exceptions for TSPs.

2.132 The data privacy framework for the country is under development, and the exceptions to the privacy can be mandated under law only. In view of the foregoing the Authority has decided not to make any recommendations in respect of legitimate exceptions to the Privacy regulatory framework.

J. Cross Border Data Flow

2.133 Data is the new oil for growth in the world today. The need to remain connected 24 X 7 through various modes of communication implies the need for data flow across the geographical boundaries. Businesses in their aspiration to provide better services to the clients and to enhance their global footprint tend to establish their offices, datacenters, logistic facilities etc across the globe. This results in cross border flow of data which includes personal data of customers, business data, employee data etc. The global enterprises in their bid to overcome catastrophic failures due to natural/ manmade disasters, establish Business Continuity Systems at diverse locations to store data pertaining to customers, employees and businesses.

2.134 India, being a software giant and a growing economy has been benefited due to its services business like the BPOs (Business Promotion Offices). Considering the importance of this issue, in the CP, the Authority had sought stakeholder's view on it.

2.135 In response, some stakeholders were of the view that regulator should refrain from making prescriptive policy guidelines that restrict cross border data flow and mandate localization. Cross border data transfer should in turn be regulated not restricted to fully harness the benefits of cloud computing. Geographical mandates may be construed as significant trade barriers and will have negative consequences as there will be possibilities of other countries also start imposing such restrictions which will severely impact the export market. Also, hosting a platform in every country would lead to inferior QoS as the interplay of many platforms cause issues in many aspects and very high costs for the service providers which will discourage investments. Moreover, navigating the data regulation and policy rules across borders can slow implementation of a valuable solution and delay innovation. The restrictions may hamper India firms to overcome in

order to compete in the global economy. The stakeholders opined that it should be user's choice where to keep their data.

2.136 The stakeholders further stated that regulatory requirements can be fulfilled by imposing guidelines on organizations to use good security standards and to check and enforce those standards on behalf of their consumers. In instances where companies are storing particularly sensitive data, they can determine additional security measures, including where data is stored, at the contract level.

2.137 One stakeholder expressed that some of the concerns about cross border data transfer relate to national security can be mitigated through:

(a) Formulating a list of countries that provide adequate protection of personal data and restricting personal data transfer only to countries on the list

(b) Enforcing use of modal contractual clauses to regulate transfer of data (as it had been done in the EU)

(c) Enforcing approved binding corporate rules where transfer is conducted within the same group of entities which are located in different jurisdictions

(d) Achieving mutual understanding with the relevant regulators within the foreign jurisdiction on the facilitation of cross border transfer (such as the US-EU Privacy Shield that is currently being developed).

2.138 According to some stakeholders, instead of restricting cross border data flow, there is a need to develop mechanisms for cooperating informally or, alternatively, resorting to what is typically referred to as requests for "Mutual Legal Assistance" for requesting and obtaining evidence for criminal investigations and prosecutions from a foreign sovereign state. Though India has Mutual Legal Assistance Treaties

(MLATs) agreements with 39 countries[28], India should focus on strengthening its MLATs and similar mechanisms for international law enforcement assistance.

2.139 One stakeholder opined that MLATs apart, assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. To obviate such situations, especially if the data hosting country is not inclined to India's interests, local hosting of servers and storage should be mandated.

2.140 On the other hand, a few stakeholders were of the view that for national security and for the protection of sensitive personal data, the Authority should mandate the M2M cloud platform and application providers have their servers located in India and abide necessary licensing and IT Act terms for delivery of services, giving Indian customers the ability to delete the stored data, if needed. The confidential data of consumer must be protected and should not be transferred to another jurisdiction without the consent of the consumer. Many stakeholders in response to the M2M CP had submitted that from security perspective, the National M2M Roadmap prescribes all M2M gateways and application servers to be physically located in India. Also, by requiring them to host in India it will be possible to address the unforeseen security challenges.

Analysis

2.141 The available options and their advantages and disadvantages are listed below:

(a) Restrict cross border data flow and mandate localization

Advantage

[28] http://cbi.nic.in/interpol/mlats.php

- Sensitive data (personal data, banking details, etc.) and data that could affect nation's security will remain in the country
- Efficient access to data for law enforcement purposes
- Easy for Law Enforcement Agencies (LEAs) to Lawful Intercept.
- Create Jobs
- Service provider would be required to follow Indian laws
- Infrastructure development

Disadvantage

- Very high cost for service provider -discourage investment
- trade barrier –impact the export market if other countries start imposing such restrictions
- inferior QoS as the interplay of many platforms cause issues in many aspects
- slow implementation –delay innovation
- Forced localization undermines competitiveness

(b) Allow cross border data flow

Advantage

- Encourage investments
- Economies of scale –beneficial for all type and size of companies
- Allow many small and medium-sized businesses to reach new customers inexpensively
- Allows companies to allocate resources more efficiently, access foreign markets, and participate in global supply chains
- Facilitate economic growth, reduce the cost and time of doing business, and enable efficient and affordable services for consumers
- Allow companies to provide innovative pricing solutions, manage risks, and where appropriate, work with regulators to prevent fraud and protect consumers.

Disadvantage

- Creates jurisdictional challenges

- Sensitive personal data and data that could affect nation's security will move across national borders
- Difficult for LEAs to Lawful Intercept.
- Service provider wouldn't be obligated to follow Indian laws

(c) Restrict cross border data flow and mandate localization of only those services which have high potential impact on national security or sensitive industry (Defence, Internal security, healthcare, finance etc)

2.142 As per the international experience, most of the countries allow cross border data transfer. The majority of the world's largest Internet companies are headquartered in the United States.

2.143 The government may foster the growth of data based businesses in India by allowing cross border data flow but at the same time critical data related to national security and sensitive data such as data related to healthcare and finance, needs to be protected. There is a need to identify services that contain critical and sensitive data and these may be mandated to locate data servers in India. This must be assessed on a case by case basis, as in many circumstances obtaining individuals consent may well be sufficient provided that the data does not involve national secrets or violate national security. The government has to task some organization to identify critical and sensitive services which requires data localization.

2.144 The security threats are evolving and are in dynamic stage. The government should address them dynamically. In today's connected world, free movement of data is important to its appropriate place and to where it is needed. However protection of critical and sensitive data cannot be neglected. Instead of restricting cross border data flow, the government should regulate it. To address the difficulties faced by

LEAs to Lawful Intercept, the government should focus on increasing and strengthening MLATs.

2.145 According to Google transparency[29]report[30], for the period of January to June 2016, the number of requests made by Indian Government for disclosure of user data from Google accounts or services was 3452. Out of which 55% of the requests were answered with some data. This shows that not all the requests were responded as required.

2.146 The MLATs can be considered as a solution for law enforcement agencies, for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws but they are not always successful because assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. In order to overcome this, government should allow data transfer to only those countries where there is adequate jurisdictions to provide data privacy and security and India also has MLATs with them.

2.147 Issues relating to cross border data flow can also be addressed to large extent by rapidly developing the data centre's and associated data analytics sector in the country. Availability of such facilities within the country would not only promote the use of local facilities for data processing but also help in signing of MLATs on fairer terms.

2.148 As brought out in para 1.9, Committee of Experts headed by Justice B N Srikrishna would be addressing the larger issues related to data protection framework applicable in general to all sectors of the economy. Since the issue of cross-border data flow is pertinent to all the sectors of the economy and would be addressed by the committee

[29] A transparency report is a statement issued on a regular basis by a company, disclosing a variety of statistics related to requests for user data, records, or content. Transparency reports generally disclose how frequently and under what authority governments have requested or demanded data or records over a certain period of time.
[30] https://www.google.com/transparencyreport/userdatarequests/IN/

of experts, the Authority, at this juncture, has decided not to make any recommendations on the issue of cross-border data flow.

Chapter 3: Summary of recommendations

3.1 Personal Data

The Authority recommends that: (*Refer paragraph 2.20*)

(a) The definitions of "Data" as provided under Information Technology Act, 2000, and "Personal Information" and "Sensitive Personal Data and information" as provided under Sensitive Personal Data and Information Rules, 2011, as reproduced below, are adequate for the present.

(i) "***Data***" – *defined in section 2(1)(o) of the Information Technology Act, 2000 as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.*

(ii) ***"Personal information"****– defined in the Sensitive Personal Data and Information Rules, 2011 as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*

(iii) *"****Sensitive personal data or Information****"– defined in the Sensitive Personal Data and Information Rules, 2011 as such personal information which consists of information relating to:- password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the*

above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

(b) Each user owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem. The entities, controlling and processing such data, are mere custodians and do not have primary rights over this data.

(c) A study should be undertaken to formulate the standards for annonymisation/ de-identification of personal data generated and collected in the digital eco-system.

(d) All entities in the digital eco-system, which control or process the data, should be restrained from using metadata to identify the individual users.

3.2 Sufficiency of existing Data Protection Framework

The Authority recommends that: (*Refer paragraph 2.39*)

(a) The existing framework for protection of the personal information/ data of telecom consumers is not sufficient. To protect telecom consumers against the misuse of their personal data by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem, which control or process their personal data should be brought under a data protection framework.

(b) Till such time a general data protection law is notified by the Government, the existing Rules/ License conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem. For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers and Applications.

(c) Privacy by design principle should be made applicable to all the entities in the digital ecosystem viz, Service providers, Devices, Browsers, Operating Systems, Applications etc. The concept of "Data Minimisation" should be inherent to the Privacy by Design principle implementation. Here "Data Minimisation" denotes the concept of collection of bare minimum data which is essential for providing that particular service to the consumers.

3.3 User Empowerment

The Authority recommends that: (*Refer paragraph 2.59*)

(a) The Right to Choice, Notice, Consent, Data Portability, and Right to be Forgotten should be conferred upon the telecommunication consumers.

(b) In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.

(c) For the benefit of telecommunication users, a framework, on the basis of the Electronic Consent Framework developed by MeitY and the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users.

(d) The Right to Data Portability and Right to be Forgotten are restricted rights, and the same should be subjected to applicable restrictions due to prevalent laws in this regard.

(e) Multilingual, easy to understand, unbiased, short templates of agreements/ terms and conditions be made mandatory for all the entities in the digital eco-system for the benefit of consumers.

(f) Data Controllers should be prohibited from using "pre-ticked boxes" to gain users consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.

(g) Devices should disclose the terms and conditions of use in advance, before sale of the device.

(h) It should be made mandatory for the devices to incorporate provisions so that user can delete such pre-installed applications, which are not part of the basic functionality of the device, if he/she so decides. Also, the user should be able to download the certified applications at his/ her own will and the devices should in no manner restrict such actions by the users.

(i) Consumer awareness programs be undertaken to spread awareness about data protection and privacy issues so that the users can take well informed decisions about their personal data.

(j) The Government should put in place a mechanism for redressal of telecommunication consumers' grievances relating to data ownership, protection, and privacy.

3.4 Data Privacy and Security of Telecom Networks

The Authority recommends that: (*Refer paragraph 2.103*)

(a) Department of Telecommunication should re-examine the encryption standards, stipulated in the license conditions for the TSPs, to align them with the requirements of other sectors.

(b) To ensure the privacy of users, National Policy for encryption of personal data, generated and collected in the digital eco-system, should be notified by the Government at the earliest.

(c) For ensuring the security of the personal data and privacy of telecommunication consumers, personal data of telecommunication consumers should be encrypted during the motion as well as during the storage in the digital ecosystem. Decryption should be permitted on a need basis by authorized entities in accordance to consent of the consumer or as per requirement of the law.

(d) All entities in the digital ecosystem including Telecom Service Providers should be encouraged to share the information relating to vulnerabilities, threats etc in the digital ecosystem/ networks to mitigate the losses and prevent recurrence of such events.

(e) All entities in the digital ecosystem including Telecom Service Providers should transparently disclose the information about the privacy breaches on their websites along with the actions taken for mitigation, and preventing such breaches in future.

(f) A common platform should be created for sharing of information relating to data security breach incidences by

all entities in the digital ecosystem including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem including all such service providers to be a part of this platform.

(g) Data security breaches may take place in-spite of adoption of best practices/ necessary measures taken by the data controllers and processors. Sharing of information concerning to data security breaches should be encouraged and incentivized to prevent/ mitigate such occurrences in future.

List of Abbreviations

API	Application Programming Interface
App(s).	Application(s)
BPO	Business Promotion Offices
CERT-in	Indian Computer Emergency Response Team
CP	Consultation Paper
DoT	Department of Telecommunication
EU-GDPR	European Union- General Data Protection Regulation
GDP	Gross Domestic Product
IP	Internet Protocol
IRDA	Insurance Regulatory and Development Authority
ISO	International Organization for Standardization
IT	Information Technology
LEA	Law Enforcement Agency
M2M	Machine-To-Machine
MAC	Medium Access Control
MLAT	Mutual Legal Assistance Treaties
MNC	Multi National Company
NCPR	National Consumer Preference Register
NDSAP	National Data Sharing and Accessibility Policy
OHD	Open House Discussion
OTT	Over the Top
PFRDA	Pension Fund Regulatory and Development Authority
PID	Personal Identity Data

QoS	Quality of Service
R&D	Research and Development
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
SPDI	Sensitive Personal Data and Information
TSP	Telecom Service Provider
UASL	Universal Access Service License
UL	Universal License