CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY, DELHI

Comments to Telecom Regulatory Authority of India's Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

1. Introduction

It is clear that there is an immediate need for better laws and regulations on privacy and data protection in India, in the telecom sector as well as other sectors. We appreciate the Telecom Regulatory Authority of India's (TRAI) efforts in this regard.

We also note that the Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector (Consultation Paper) was published on August 9, 2017. Since then, the Supreme Court of India has affirmed that the right to privacy is a fundamental right under the Indian Constitution, in a detailed judgment in *Puttaswamy v. Union of India*[1]. The Ministry of Electronics and Information Technology (MEITY), Government of India has also set up a Committee of Experts to identify key data protection issues in India and recommend methods of addressing them[2]. The Committee of Experts is also expected to suggest a draft data protection bill.

Our comments draw upon the constitutional right to privacy (discussed in part 2 of this note), and criticisms of the current data protection regime from the report of the Group of Experts, headed by (Retd.) Justice A. P. Shah (discussed in part 3 of this note) to begin with. They then discuss the key concerns that any new data protection regime must address (part 4) of this note while noting that TRAI has limited jurisdiction and may wish to frame its recommendations taking this into account.

We address the specific questions raised by TRAI in part 5 of this paper. Our responses are based on the rest of this note and must be read in the context of parts 1 to 4.

[1] Writ petition (civil) no 494 of 2012, (2017)6MLJ267

[2] Office Memorandum No. 3(6)j2017-CLES, available at http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf (last visited on November 5, 2017)

2. Privacy as a Fundamental Right

Before we answer the specific questions set out in the Consultation Paper, we wanted to highlight a few of the observations made by the Supreme Court in *Puttaswamy v. Union of India*[3].

The Supreme Court has affirmed and recognised that the right to privacy is a fundamental right under Article 21 of the Constitution. It may also be drawn as a fundamental right under any of the other fundamental rights recognised under the Constitution. Accordingly, the Court has observed that although the right is not absolute, any restrictions imposed by the State on the right to privacy must be 'reasonable restrictions'. These reasonable restrictions must meet the various tests for limitations / violations of the right, applicable in relation to the relevant fundamental rights. At the same time, the Court has also noted that there is a positive obligation for the state to create a regulatory environment that allows individuals to enjoy their right to privacy.

In recognising privacy as a fundamental right, J. Chandrachud, J. Chelameswar, J. Kaul and J. Nariman have, in their various opinions have observed that informational privacy is an important aspect of such privacy in this day and age. J. Chandrachud has noted the setting up of the Committee of Experts, and recommended that the central government puts in place a robust data protection regulation in place in order to protect this right.

In the observations that lead up to his conclusions, J. Chandrachud has also noted that data protection regulation is a complex issue which needs to address many aims[4]. The first of these aims is the individual's right to be left alone. Second and more importantly, the regulation needs to ensure that the individual's identity is protected. Third, the individual's autonomy in making decisions about the use of data about them, and their right to know how this data is being used must be protected. Fourth, data protection regulation should ensure that data is not collected in a manner that is discriminatory towards anyone.

3. Current data protection laws

Our assessment is that the current data protection rules are insufficient to protect the interests of data subjects, including telecom subscribers.

The Consultation Paper has at various points referred to the report of the Group of Experts, headed by (Retd.) Justice A. P. Shah, in 2012 (GOE Report)[5]. We note that this GOE report

[3] Writ petition (civil) no 494 of 2012, (2017)6MLJ267

[4] Paragraphs 177 and 178, J. Chandrachud's opinion, Puttaswamy v. Union of India (2017)6MLJ267

[5] Report of the Group of Experts on Privacy, available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf (last visited on November 5, 2017)

found the various data protection rules that are currently applicable, inadequate[6]. The GOE Report has examined best practices and principles of data protection laws across the world, and recommended the incorporation of a set of 9 national privacy principles in any proposed privacy law[7]. The GOE Report has then gone on to find that the existing data protection regulations do not meet the requirements set forth in these principles[8].

The existing data protection laws, including particularly the provisions under the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under the IT Act (IT Rules) have also been criticised by industry and civil society members alike[9]. The IT Rules are ambiguous and do not properly define the roles and responsibilities of data controllers and processors[10]. There is no clarity on the nature of the data that the rules are applicable to. Further, the provisions under the IT Act do not provide for penalties or consequences for failure to comply with the IT Rules, and provide only a compensation mechanism that is difficult to enforce[11].

We are in agreement with the part of Consultation Paper which points out that some of the principles set out in the GOE Report may need to be reformulated in today's age of big data[12]. However, we note that the data protection regulations fall short even of the outdated standards set forth in the principles listed by the GOE Report. More work will be necessary to define new standards and develop strategies to ensure that data protection framework meets these standards.

4. Formulation of new data protection regulations

[6] Report of the Group of Experts on Privacy, Chapter 4

[7] Report of the Group of Experts on Privacy, Chapter 3

[8] Report of the Group of Experts on Privacy, Chapter 4

[9] Outsourcing: India adopts new privacy and security rules for personal information, available at https://www.lexology.com/library/detail.aspx?g=9a9b9ec0-e390-45b8-a6f1-4363e29e9af3 (last visited on November 5, 2017); and Bhairav Acharya, Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, available at https://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011 (last visited on November 5, 2017)

[10] Smitha Krishna Prasad, Draft white paper on the IT Act and the data protection rules, (to be published, and available on request)

[11] Smitha Krishna Prasad, Draft white paper on the IT Act and the data protection rules, (to be published, and available on request)

[12] TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, Page 9

As mentioned above, MEITY has now set up a Committee of Experts to recommend a data protection framework for the country, and put together a draft data protection law[13]. The first question before the TRAI would then be whether there is a need for a separate regulatory framework for data within the telecom sector (please refer to part 4.7 of this note for a detailed discussion of TRAI's jurisdiction in this context).

Below, we have listed principles that we believe any data protection regulation, irrespective of the sector it applies to, should address. It is our recommendation that these principles be applied across sectors, industries and regions. Additionally, it is important to account for the fact that as Indian businesses grow and adopt new technology, they are increasingly beginning to function across sectors. In this context, we recommend that a basic data protection law that is applicable horizontally across sectors and regions, to cope with these cross-sectoral business models. Where required, we recommend that additional regulations may be made applicable to collection and processing of sector specific sensitive personal data.

4.1. Data protection principles

Any new data protection regulation, whether applicable across industries and sectors, or applicable only to the telecom sector, should be based on sound principles of privacy and data protection. As discussed in the Consultation Paper, the GOE Report identified 9 national privacy principles to be adopted in drafting a privacy law for India. These principles are listed below[14]:

(i) Notice: A data controller, which refers to any organization that determines the purposes and means of processing the personal information of users, shall give simple 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.

(ii) Choice and consent: 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.

(iii) Collection limitation: A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection.

(iv) Purpose limitation: Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed.

[13] Office Memorandum No. 3(6)j2017-CLES, available at http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf (last visited on November 5, 2017)

[14] Report of the Group of Experts on Privacy, Chapter 3, as summarised in the TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, pages 7-9

(v) Access and correction: Individuals shall have access to personal information about them held by a data controller and be able to seek correction, amendments, or deletion of such information, where it is inaccurate.

(vi) Disclosure of Information: A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure.

(vii) Security: A data controller shall secure personal information using reasonable security safeguards against loss, unauthorised access or use and destruction.

(viii) Openness: A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

(ix) Accountability: The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies, including training and education, audits, etc.

With the growth of businesses driven by big data, there is now a demand for re-thinking these principles, especially those relating to notice and consent[15].

While notice, consent and the other principles set forth in the GOE Report have formed the basis for data protection laws for many years now, additional principles have been developed in many jurisdictions across the world. In order to ensure that any new regulations in India are up to date and effective, it will be prudent to study such principles and identify the best practices that can then be incorporated into Indian law.

Graham Greenleaf has compared data protection laws across Europe and outside Europe and found that today, second and third generation 'European Standards' are being implemented across jurisdictions[16]. These 'European Standards', refer to standards that are applicable under European Union (EU) law, in addition to the original principles developed by the Organisation for Economic Co-operation and Development (OECD)[17]. The second generation European Standards that are most commonly seen outside the EU are:

---

[15] TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, Page 9; and Rahul Matthan, Beyond Consent: A New Paradigm for Data Protection, available at http://takshashila.org.in/takshashila-policy-research/discussion-document-beyond-consent-new-paradigm-data-protection/ (last visited on November 5, 2017)

[16] Graham Greenleaf, European data privacy standards in laws outside Europe, Privacy Law and Business International Report, Issue 149

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited on November 5, 2017)

(i) Recourse to the courts to enforce data privacy rights (including. compensation, and appeals from decisions of DPAs)
(ii) Destruction or anonymisation of personal data after a period
(iii) Restricted data exports based on data protection provided by recipient country ('adequate'), or alternative guarantees
(iv) Independent Data Protection Authority (DPA)
(v) Minimum collection necessary for the purpose (not only 'limited')
(vi) General requirement of 'fair and lawful processing' (not only collection)
(vii) Additional protections for sensitive data in defined categories
(viii) To object to processing on compelling legitimate grounds, including to 'opt-out' of direct marketing uses of personal data
(ix) Additional restrictions on some sensitive processing systems (notification; 'prior checking' by DPA.)
(x) Limits on automated decision-making (including right to know processing logic)

He also notes that there are several new principles put forward in the EU's new General Data Protection Regulation[18] (GDPR) itself, and that it remains to be seen which of these will become global standards outside the EU. The most popular of these principles, which he refers to as '3rd General European Standards' are[19]:

(i) Data breach notifications to the DPA for serious breaches
(ii) Data breach notifications to the data subject (if high risk)
(iii) Class action suits to be allowed before DPAs or courts by public interest privacy groups
(iv) Direct liability for processors as well as controllers
(v) DPAs to make decisions and issue administrative sanctions, including fines.
(vi) Opt-in requirements for marketing
(vii) Mandatory appointment of data protection officers in companies that process sensitive personal data.

We note that there exist other proposed frameworks that aim to regulate data protection and ease compliances required by businesses. Such additional frameworks may also be considered while formulating new data protection principles and regulations in India. However, it is recommended that the 'European Standards' described above, i.e. those set out in the GDPR may be adopted as the base on which any new regulations are built. This would ensure that India has greater chances of being recognised as having 'adequate' data protection frameworks by the EU, and improve our trade relations with the EU and other countries that adopt similar standards.

Professor Greenleaf's studies suggest that the 2nd and 3rd General European Standards are being adopted by several countries outside the European Union. We note here that adoption of

[18] General Data Protection Regulation, Regulation (EU) 2016/679

[19] Graham Greenleaf, Presentation on 2nd & 3rd generation data privacy standards implemented in laws outside Europe (to be published and available on request).

principles that are considered best practices across jurisdictions would also assist in increasing interoperability for businesses that operate across borders.

While adoption of these practices is likely to raise the cost of compliance, it is also likely to ensure that India remains a very competitive market globally for the outsourcing of services. In the long term, this will benefit Indian industry and the Indian economy. It will also safeguard the privacy rights of Indian citizens in the best possible manner.

4.2. Wide Definition of personal information

Any data protection law should be applicable to a wide category of personal information. The nature of data that is collected and processed is constantly changing with technology, and it is imperative that any data protection laws should be drafted in a manner that accommodates this change. Where required, additional protections may be provided for in relation to specific types or categories of data.

The IT Act and the IT Rules currently provide for regulation of two types of information –

(i) 'personal information'[20] - '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' and

(ii) 'sensitive personal data or information'[21] - any personal information which consists of information relating to: (i) passwords; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; and (vii) any details of information relating to the above that are provided to a body corporate for obtaining services, or received by a body corporate. This does not include any information that is freely available or accessible in public domain or furnished under any law, including specifically the Right to Information Act, 2005.

As mentioned in the Consultation Paper, in addition to identifying information that typically falls within the definition of personal information, telecom companies collect and have access to specific types of information about their subscribers such as call detail records, calling patterns, location data, data usage information[22]. Data protection rules applicable to these companies need to account for this and protect consumers from the privacy violations that result from these practices.

[20] Rule 2(1)(i) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[21] Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[22] TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, Page 9

The European Union's new GDPR provides one example of the sort of wide definition that is necessary in this context: 'personal data' is simply defined as any information relating to an identified or identifiable natural person[23]. The definition goes on to provide that 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. While most of the data protection regulations in the GDPR apply in relation to all such personal information, additional safeguards are applicable to in relation to special categories of data[24]. We recommend the adoption of this approach.

4.3. Consent and user empowerment

As mentioned above, we note that the continuing relevance of existing notice and consent mechanisms, in the context of today's 'big data' world has been questioned. In this regard we note that the objections to the notice and consent mechanisms typically centre around the concept of 'meaningful consent'[25]. It is argued that data is collected and processed in a manner that is beyond description in a simple and clear manner that allows for data subjects to understand what they consent to.

Often users end up agreeing to broad privacy policies which allow companies to use personal data for means beyond what may be necessary to deliver the service in question. The argument made is that this places an undue burden on individuals who are not given the means of actually controlling what happens with their data[26].

Rights, risks and harm based approaches to data protection regulation have been proposed as alternatives to the existing models, in order to counter these issues[27].

---

[23] Article 4(1) of the General Data Protection Regulation, Regulation (EU) 2016/679

[24] Article 9 of the General Data Protection Regulation, Regulation (EU) 2016/679 deals with processing of special categories of personal data

[25] Rahul Matthan, Beyond Consent: A New Paradigm For Data Protection, available at http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf (last visited on November 5, 2017)and Fred H. Cate, Peter Cullen and Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century, available at https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (last visited on November 5, 2017)

[26] Fred H. Cate, Peter Cullen and Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century, available at https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (last visited on November 5, 2017)

[27] Rahul Matthan, Beyond Consent: A New Paradigm For Data Protection, available at http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf, Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal (last visited on November 5, 2017)

While the implementation of notice and consent mechanisms may pose certain problems, doing away with such mechanisms may not be the solution. The requirements for provision of notice, or obtaining consent, ensure that the user / data subject is made aware that their data is being collected and used by certain companies for certain purposes.

It is our recommendation that additional accountability and transparency mechanisms should be implemented to help users retain more control over their data. The European Standards mentioned above include examples of some such measures. An indicative list of measures that may be adopted to provide users with additional control over their data is provided below:

(i) Opt-in and opt-out mechanisms, including complete or partial opt-out or withdrawal of consent
(ii) Data breach notification requirements
(iii) Accessible redressal and dispute resolution mechanisms
(iv) Right to access, review and correct data[28]
(v) Right to data portability[29]

Regular privacy impact assessments and audits will help increase users' trust in data collectors and processors, and allow for more meaningful implementation of the above-mentioned principles / measures[30].

The development of big data analytics has led to a significant problem with the traditional consent mechanism – the creation of new data that may be personally identifiable, using existing data collected by application of traditional consent mechanisms. Crawford and Schultz have noted that as a result, with increasing use of big data, there is an increase in the 'predictive privacy harms'[31]. Crawford and Schultz have argued that existing regulatory schema appear

---

frameworks http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (last visited on November 5, 2017) and Fred H. Cate, Peter Cullen and Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century, available at https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (last visited on November 5, 2017)

[28] European Data Protection Supervisor, Opinion 7/2015, Meeting the challenges of big data, available at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (last visited on November 5, 2017)

[29] European Data Protection Supervisor, Opinion 7/2015, Meeting the challenges of big data, available at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (last visited on November 5, 2017)

[30] United Kingdom Information Commissioner's Office, Conducting privacy impact assessments, code of practice, available at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (last visited on November 5, 2017) and Michael L. Whitener, Conducting a Privacy Audit, available at https://iapp.org/media/pdf/knowledge_center/Conducting_a_Privacy_Audit_-_The_Corporate_Counselor_-_July_2012.pdf (last visited on November 5, 2017)

[31] 'Predictive privacy harms' are harms that may not directly constitute a violation of traditional data protection laws, but are still derived from collecting and using information that centers on an individual's data behaviours

incapable of keeping pace with these advancing business norms and practices, and that there is need for a procedural due process like framework to address these harms[32].

Crawford and Schultz have noted that adoption of such a framework may address the individual's concerns about the procedural process, even in spite of an unfavourable outcome[33]. Three main principles of data due process are proposed:

(i) Notice: Differing slightly from the traditional concept of notice in relation to data collection, this principle requires "*those who use Big Data to "adjudicate" others—i.e., those who make categorical or attributive determinations—to post some form of notice, disclosing not only the type of predictions they attempt, but also the general sources of data that they draw upon as inputs, including a means whereby those whose personal data is included can learn of that fact*"[34]

(ii) Opportunity for a hearing: this principle argues for allowing the evidence used, i.e. the data input and the algorithmic logic applied, and an opportunity for the data subject to be heard, and the data in question to be corrected if necessary. Security and proprietary concerns may be noted, and impartial trusted third parties may be appointed for the purpose of examining the algorithms [35]

(iii) Impartial Adjudicator and Judicial Review: This principle addresses the fact that big data outputs are not always free from bias, and suggests that "*a neutral data arbiter could field complaints and investigate sufficient allegations of bias or financial interest that might render the adjudication unfair*"[36].

---

[32] Kate Crawford and Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, available at http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr (last visited on November 5, 2017)

[33] Kate Crawford and Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, available at http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr (last visited on November 5, 2017) and Robert J. MacCoun, Voice, Control, And Belonging: The Double-Edged Sword of Procedural Fairness, available at http://conium.org/~maccoun/MacCoun_ARLSS2005.pdf (last visited on November 5, 2017)

[34] Kate Crawford and Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, available at http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr (last visited on November 5, 2017), page 34

[35] Kate Crawford and Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, available at http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr (last visited on November 5, 2017), page 36

[36] Kate Crawford and Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, available at http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr (last visited on November 5, 2017), page 36

We recommend that similar processes are provided for in order to empower and allow data subjects an opportunity to address concerns with processing and use of big data in a manner that affects them.

4.4. Data Protection Authority

The GOE Report suggested the establishment of offices of privacy commissioners, at the central and regional levels[37]. It also suggested establishment of a co-regulation regime, where companies would be entrusted with ensuring compliance with the data protection laws. These companies would then report to, and be subject to minimum oversight by the privacy commissioners.

There has been a significant increase in data driven business, and associated concerns in relation to protection of personal information since the GOE Report was published. With any new data protection regulation, the establishment of regulators (or separate departments / offices within existing regulatory bodies) for implementation of the regulation will become imperative. These regulators will need to monitor data processors and controllers to ensure compliance with the new data protection regulation (and possibly any other law that deals with data protection / privacy in any form). Increasingly, data protection authorities also have administrative and quasi-judicial functions and are being allowed to decide on complaints of non-compliance and impose penalties and fines[38].

The OECD's revised privacy guidelines[39] (OECD Guidelines) also provide for establishment of privacy enforcement authorities. The OECD Guidelines provide that these privacy enforcement authorities are

(i) Required to have the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;

(ii) to be to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy.

The OECD Guidelines also suggest that these privacy enforcement authorities engage in cross-border co-operation with similar authorities in other jurisdictions to ensure global interoperability of data protection regulations[40].

The EU's GDPR also provides for establishment of 'supervisory authorities', i.e. public authorities that oversee the implementation of the GDPR in each member state. The GDPR

[37] Report of the Group of Experts on Privacy, Chapter 5

[38] See 2nd and 3rd generation European Standards described in section 4.1 above.

[39] The OECD Privacy Framework, available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited on November 5, 2017)

[40] The OECD Privacy Framework, available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, page 107 (last visited on November 5, 2017)

contains extensive provisions on the establishment, competence, tasks and powers of the supervisory authorities[41]. In certain situations, data processors and controllers are required to appoint data protection officers who, among other things, cooperate with the supervisory authority.

It may be relevant to note that the existence of a supervisory authority with enforcement powers, is one of the elements that is considered in order for a non-EU member state to obtain an adequacy decision in its favour[42]. In this context, it would be useful for the TRAI and / or MEITY to consider the provisions governing the establishment and role of supervisory authorities under the GDPR while drafting the new data protection laws in India.

4.5. Legitimate exceptions, limitations and restrictions to data protection regulation

The order of the Supreme Court in *Puttaswamy v. Union of India* states that "*the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution*". Informational privacy has been recognised as an integral part of this fundamental right[43] by J. Chandrachud. J. Nariman and J. Kaul have also recognised the right to informational privacy in their observations

With the recognition of privacy as a fundamental right, the State must ensure that any actions that may limit or violate such a right fall within the existing parameters for reasonable restrictions to fundamental rights. Any State actions that require or regulate the use of personal data should also be considered from this perspective.

The Supreme Court in *Puttaswamy v. Union of India* has not explicitly provided or enumerated such reasonable restrictions, and observations by various judges suggest that these restrictions need to be identified on a case to case basis. As per the Supreme Court's order in *Vishaka v. State of Rajasthan*, in the absence of specific case law or legislation dealing with such issues, the contents of International Conventions and norms are significant for the purpose of interpretation of the rights guaranteed under the Constitution[44].

First, we refer to the International Convention on Civil and Political Rights, to which India is a state party[45]. Article 17 of the ICCPR states:

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

---

[41] Chapter VI, General Data Protection Regulation, Regulation (EU) 2016/679

[42] Article 45, General Data Protection Regulation, Regulation (EU) 2016/679

[43] Puttaswamy v. Union of India, (2017)6MLJ267

[44] Vishaka & Ors v. State of Rajasthan & Ors, AIR 1997 SC. 3011, available at https://indiankanoon.org/doc/1031794/ (last visited on November 5, 2017)

[45] International Covenant on Civil and Political Rights, available at http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (last visited on November 5, 2017)

2. Everyone has the right to the protection of the law against such interference or attacks."

The ICCPR notably does not contain a limitations clause to Article 17, which recognises the right to privacy. However, the permissible limitations to this right are elaborated in the Human Rights Committee's general comments[46], and can also be drawn from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights[47]. Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful[48]. The Human Rights Committee's General Comment 16 explains that "*the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant*"[49].

In her report on 'The right to privacy in the digital age'[50], the (then) United Nations High Commissioner for Human Rights has explained these concepts in greater detail as follows:

"*To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.16 Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights,*

[46] Available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11 (last visited on November 5, 2017)

[47] Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, Human Rights Council Twenty-seventh session, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited on November 5, 2017)

[48] Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, Human Rights Council Twenty-seventh session, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited on November 5, 2017)

[49] Human Rights Committee, General Comment 16, available at http://hrlibrary.umn.edu/gencomm/hrcom16.htm (last visited on November 5, 2017)

[50] Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, Human Rights Council Twenty-seventh session, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited on November 5, 2017)

including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary"

It is recommended that these factors are accounted for in the drafting of any legislation on data protection or privacy.

In *Puttaswamy v. Union of India*[51] J. Kaul has referred to the restrictions allowed under EU's GDPR as an example of the restrictions that may be considered reasonable in India. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[52] (Convention 108), which is widely recognised as the only international convention that deals with data protection, also provides for some limited restrictions to the data protection obligations of member states.

We've listed below some of the accepted purposes for which states may restrict obligations of data protection under the GDPR and Convention 108[53]:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
(e) other important objectives of general public interest, including important economic or financial interests (such as tax collection and exchange control), and scientific research;
(f) the protection of judicial independence and judicial proceedings;
(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(h) the protection of the data subject or the rights and freedoms of others;
(i) the enforcement of civil law claims

More importantly, these international norms provide that any national legislation that purports to safeguard the above, must be necessary and proportionate for such purpose. Such legislation must respect fundamental rights and freedoms. The GDPR also provides that, where possible, such legislation must contain provisions regarding[54]:

(i) the purposes of the processing or categories of processing;
(ii) the categories of personal data;

---

[51] Puttaswamy v. Union of India, (2017)6MLJ267

[52] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108

[53] Article 23 (1), General Data Protection Regulation, Regulation (EU) 2016/679, Article 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, and Explanatory Report to Convention 108 available at https://rm.coe.int/16800ca434 (last visited on November 5, 2017)

[54] Article 23 (2), General Data Protection Regulation, Regulation (EU) 2016/679

(iii) the scope of the restrictions introduced;
(iv) the safeguards to prevent abuse or unlawful access or transfer;
(v) the specification of the controller or categories of controllers;
(vi) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(vii) the risks to the rights and freedoms of data subjects; and
(viii) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

4.6. Creation of new data based businesses / services

The Consultation Paper refers to actions that may be taken to encourage new data driven businesses and services. Specifically, there is discussion about creation of a data sandbox containing anonymised data sets that can be used by companies in the business.

Anonymised data is typically excluded from data protection regulations, which apply to data that is capable of identifying a person. However, over many years now, studies have increasingly shown that absolute anonymization of data may not be possible[55]. This means that the use of any anonymised data set will still include a risk of violation of the right to privacy of any individual whose data may have contributed to such a data set.

The GDPR continues to leave anonymised data out of the scope of regulation, but has incorporated a higher standard for the definition of anonymised data[56]. Some jurisdictions like the United Kingdom are even taking to criminalisation of any re-identification of anonymised data, whether intentional or not[57].

In this context, it is recommended that the TRAI (and MEITY) carefully consider regulation of the manner in which anonymization and re-identification of data in the private sector is carried out. Further, to the extent that the TRAI / government wishes to set up a 'data sandbox', the risk of re-identification may put such activities within the realm of a violation of the right to privacy.

[55] 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/ (last visited on November 5, 2017)
[56] Personal data, anonymization and pseudonymisation under the GDPR, available https://www.slaughterandmay.com/media/2535637/personal-data-anonymisation-and-pseudonymisation-under-the-gdpr.pdf (last visited on November 5, 2017)
[57] Natasha Lomas, UK to criminalize re-identifying anonymized personal data, available at https://techcrunch.com/2017/08/08/uk-to-criminalize-re-identifying-anonymized-personal-data/ (last visited on November 5, 2017)

As mentioned above, the right to privacy has been recognised as a fundamental right across Chapter III of the Constitution of India in *Puttaswamy v. Union of India*[58]. Any limitation or violation of such a right will need to meet the tests for restricting the rights granted under one or more fundamental rights under the Constitution. We have described in greater detail the considerations to be taken into account when such limitations or restrictions are imposed by law, in part 4.5 above. The TRAI will need to examine whether a broad function such as 'creation of new data based services' merits such a restriction.

4.7. Jurisdiction and powers of the TRAI

We note that the Consultation Paper makes several references to stakeholders / players in the digital / telecommunications eco-system that are not traditional telecommunication service providers. These include online content / application service providers, device manufacturers, and providers of online communication services, operating systems, browsers. The Consultation Paper poses several questions about the regulation of data use and processing by such stakeholders.

In this context, we have examined the role and responsibilities of the TRAI beyond the regulation of traditional telecommunication service providers.

The preamble to the Telecom Regulatory Authority of India Act, 1997 (TRAI Act) states that the law is meant to "*provide for the establishment of the Telecom Regulatory Authority of India and the Telecom Disputes Settlement and Appellate Tribunal to regulate the telecommunication services, adjudicate disputes, dispose of appeals and to protect the interests of service providers and consumers of the telecom sector, to promote and ensure orderly growth of the telecom sector and for matters connected therewith or incidental thereto".*

Telecommunication services have been defined to mean "service of any description (including electronic mail, voice mail, data services, audio tax services, video tax services, radio paging and cellular mobile telephone services) which is made available to users by means of any transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature, by wire, radio, visual or other electromagnetic means"[59]. Broadcasting services have been excluded from the definition of telecommunication services[60].

Service providers means either the government as a service provider, or a licensee[61] – which refers to any person licensed to provide telecommunication services under the Indian Telegraph Act, 1885[62].

[58] Puttaswamy v. Union of India, (2017)6MLJ267

[59] Section 2(1)(k) of the Telecom Regulatory Authority of India Act, 1997

[60] Section 2(1)(k) of the Telecom Regulatory Authority of India Act, 1997

[61] Section 2(1)(j) of the Telecom Regulatory Authority of India Act, 1997

[62] Section 2(1)(e) of the Telecom Regulatory Authority of India Act, 1997

Section 11 of the TRAI Act describes the functions of the TRAI. These functions are divided into two broad areas: (i) making recommendations of certain matters, and (ii) regulatory functions. The regulatory functions largely deal with monitoring compliance with the telecom licenses, and other functions of service providers.

The TRAI's powers to make recommendations extend to the following matters:

(i) need and timing for introduction of new service provider;
(ii) terms and conditions of licence to a service provider;
(iii) revocation of licence for non-compliance of terms and conditions of licence;
(iv) measures to facilitate competition and promote efficiency in the operation of telecommunication services so as to facilitate growth in such services;
(v) technological improvements in the services provided by the service providers;
(vi) type of equipment to be used by the service providers after inspection of equipment used in the network;
(vii) measures for the development of telecommunication technology and any other matter relatable to telecommunication industry in general;
(viii) efficient management of available spectrum

We note that most of the above matters deal specifically with functions of service providers. However, as mentioned above, telecommunication services do include some services beyond those provided by traditional telecommunication service providers – such as electronic mail and voice mail among others.

In this context, we would argue that the functions and powers of the TRAI would not extend to making recommendations regarding, or regulating online content and application providers, device manufacturers or other businesses that do not provide communication services.

At best, the TRAI may derive powers to make recommendations regarding based on questions posed in the Consultation Paper, under sub-section (iv) which provides the TRAI with the authority to make recommendations on improving efficiency of telecommunication services.

5. Responses to Questions in the Consultation Paper

Q.1 Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard?

Response: For the reasons detailed in part 3 above, we do not find the current data protection rules sufficient to protect the interests of any data subjects, including telecom subscribers.

We recommend the adoption of new data protection principles such as those mentioned in part 4.1 above. We recommend cross-sectoral regulation to this effect, and if it is found that there

is still a need to address protection of data specific to telecom subscribers, additional sector specific law and regulations may be put in place accordingly.

We also note the reference to 'all the players in the eco-system', in this question, and through the Consultation Paper. In this regard, we would like to reiterate our comments from part 4.7 above: under the TRAI Act, the TRAI's powers are limited to making recommendations and regulating telecommunication services and service providers. In this context, any regulation on data protection implemented by the TRAI may not be applicable to many of the 'players in the eco-system' referred to in the Consultation Paper. Accordingly, we recommend that the TRAI and MEITY consider the nature of businesses and service provider who act as collectors, controllers and processors of data, and move towards the framing and implementation of suitable and comprehensive laws and regulations.

Q. 2 In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

Response: As mentioned in part 4.2, new technology allows for easier identification of persons using data that is not traditionally considered to be 'identifying data'. Accordingly, a wide definition of 'personal data' should be adopted in order to accommodate the changing nature of data that is capable of identifying an individual whether directly or indirectly.

With regard to the need for obtaining the consent of data subjects, we note that there is some discussion today about whether the notice and consent model adopted by earlier data protection regulation is still relevant.

However, as mentioned in part 4.3, even if consent is no longer sufficient by itself, the concepts of notice and consent do play a role in informing the data subject of the collection and use of their data.

We recommend that in order to protect personal data, and empower users to a greater extent, collectors and processors be required to undertake additional transparency and accountability measures. Some examples of such measures have been described further in part 4.3 above. Further, adequate due process procedures should be put in place in order to allow users an opportunity to question and address any concerns they may have with the use and processing of data related to them. We have described some such recommended processes in part 4.3 above, the same are summarised below:

(i) Opt-in and opt-out mechanisms, including complete or partial opt-out or withdrawal of consent
(ii) Data breach notification requirements
(iii) Accessible redressal and dispute resolution mechanisms

(iv) Right to access, review and correct data
(v) Right to data portability
(vi) Regular privacy impact assessments and audits
(vii) Implementation of data due process procedures

Q.3 What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

Response: We believe that the role and responsibilities of data controllers should be informed by the data protection principles described in part 4.1 above.

A data controller may be allowed to collect and use personal data of an individual. However, such activities must be undertaken in compliance with the law, and keeping in mind the protection of the data subject's right to privacy and protection of their personal data.

The business and other activities of data controllers should be regulated by data protection laws informed by sound data protection principles, as discussed in our comments to Question 1 above. It is advisable that the broader framework should use different regulatory strategies from self-regulation and co-regulation, to command and control regulation, as is appropriate for different contexts. However we wish to note that there are circumstances in which the data controller must not permit the sharing of data, even if the data subject is inclined to share it. This would be consistent with the reading of the right to privacy into the right to life[63], and with the principle that individuals cannot voluntarily give up this right[64].

We recommend that a data protection authority is be established to monitor and administer compliance with such laws and regulations. We have further discussed the establishment and role of such data protection authorities in part 4.4 above.

Q. 4 Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

Response: As mentioned in part 4.3, we believe that regular privacy audits, and privacy impact assessments will help increase a data subject's trust in data collectors and processors. These mechanisms will also help data protection authorities monitor the activities of data controllers and processors better.

[63] Puttaswamy v. Union of India, (2017)6MLJ267
[64] Basheshar Nath v. The Commissioner of Income Tax Delhi, [1959] Supp. 1 S.C.R. 528; and Olga Tellis & Ors v. Bombay Municipal Council & Ors, 1986 AIR 180

We do not have any comments on the technology and resources required to create such mechanisms except to recommend that any such architecture should be vetted and reviewed thoroughly, ideally with a separate detailed consultation, to ensure that it does not enable infringement of the right to privacy. The incentives in this case are likely to veer away from data protection and privacy, and it will be important to create strong norms and oversight mechanisms wherever industry is involved.

Q. 5 What, if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection?

Response: We do not have any comments on the measures that may be taken to encourage the creation of new data based businesses, or the need for any such measures.

However, we do note that any such measures should ensure compliance with the data protection principles specified in part 4.1 above. Further, to the extent that the State itself undertakes any measures that may require or regulate the use of personal data, or limit the rights of data subjects, we reiterate that such measures should fall within the acceptable limitations and restrictions on fundamental rights. The question of how such limitations and restrictions may be identified is addressed in greater detail in part 4.5 above.

We also recommend that the standards set out in the GDPR may be adopted as the base on which any new measures or regulations are built. This would ensure that India has greater chances of being recognised as having 'adequate' data protection frameworks by the EU, and improve our trade relations with the EU and other countries that adopt similar standards. The adoption of principles that are considered best practices across jurisdictions would also assist in increasing interoperability for businesses that operate across borders.

Q.6 Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

Response: As mentioned in part 4.6 above, we note that over many years now, studies have increasingly shown that absolute anonymization of data may not be possible[65]. This means that the use of any anonymised data set will still include a risk of violation of the right to privacy of any individual whose data may have contributed to such a data set.

In this context, we would argue that the risk of re-identification may put any initiative by the TRAI to set up a publicly available data sandbox consisting of anonymised data sets within the

[65] 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/ (last visited on November 5, 2017)

realm of a violation of the fundamental right to privacy. We note also that incentivising the development of new data driven services is unlikely to fall within the realm of legitimate exceptions, limitations or restrictions to such a fundamental right.

Q. 7 How can the government or its authorized authority setup a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

Response: We do not have any comments in response to this question, except what we have already stated in response to question 4. Any such solution will need to be discussed in detail separately.

Q. 8 What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?

Response: We do not have any comments in response to this question. However, we do recommend that any requirements that are put in place for ensuring such safety and security, such as security standards are documented and updated on a regular basis.

Q. 9 What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues?

Q. 10 Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

Response to Q. 9 and Q. 10: As mentioned above, we recommend that a horizontal data protection law which takes into cognizance the data protection principles mentioned in part 4.1 above, and is applicable to all stakeholders should be put in place.

However, we would again like to highlight the concerns expressed in part 4.7 above. Under the TRAI Act, the TRAI's powers are limited to making recommendations and regulating telecommunication services and service providers. In this context, any regulation on data protection implemented by the TRAI may not be applicable to many of the other stakeholders referred to in this question. Accordingly, we recommend that the TRAI and MEITY consider the nature of businesses and service providers who act as collectors, controllers and processors of data, and move towards implementation of suitable and comprehensive laws and regulations.

Q. 11 What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

Response: We refer to the discussion in part 4.5 and note that some of the internationally accepted purposes for which data protection obligations may be limited or restricted are:

(a) National security and defence
(b) Public security
(c) Law enforcement
(d) Important objectives of public interest such as economic or financial interest (tax collection and exchange control), or scientific research
(e) Protection of the data subject, or rights and freedoms of others

The manner in which these limitations and restrictions are applied will need to be considered on a case to case basis. However, we recommend that as discussed above, the internationally accepted parameters for such decisions should be applied in each such case. Some of these parameters are:

(i) Any limitations and restrictions should not be arbitrary or unlawful (the concepts of arbitrariness and unlawfulness are discussed in greater detail in part 4.5 above)
(ii) Any limitations and restrictions must be necessary and proportionate to the purpose they are intended to achieve
(iii) Any limitations and restrictions must respect fundamental rights and freedoms guaranteed under the Constitution (and international law).

We also recommend that the additional parameters set out in the GDPR (discussed in part 4.5 are adopted.