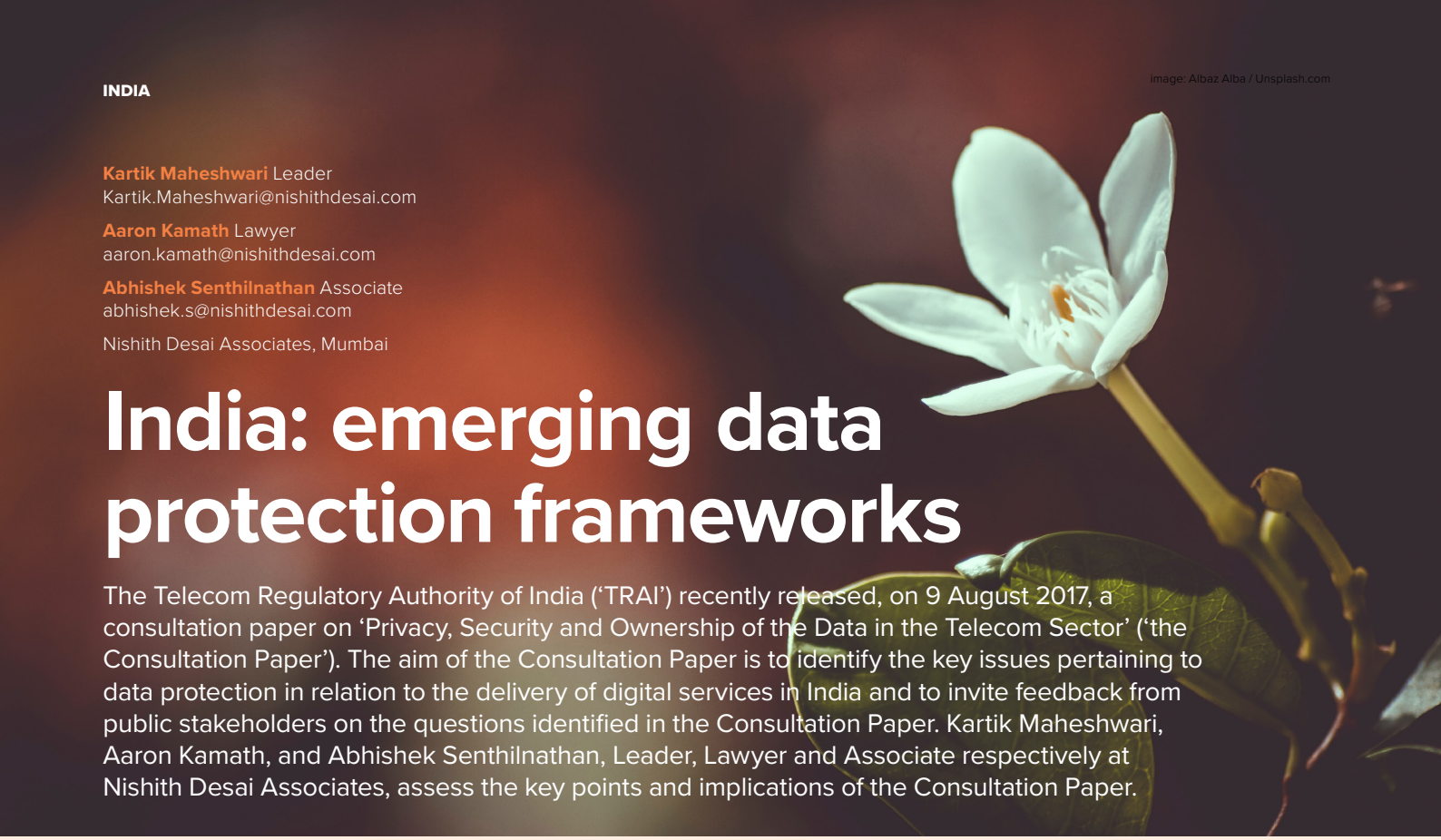

image: Albaz Alba / Unsplash.com

Kartik Maheshwari Leader
Kartik.Maheshwari@nishithdesai.com

Aaron Kamath Lawyer
aaron.kamath@nishithdesai.com

Abhishek Senthilnathan Associate
abhishek.s@nishithdesai.com

Nishith Desai Associates, Mumbai

India: emerging data protection frameworks

The Telecom Regulatory Authority of India ('TRAI') recently released, on 9 August 2017, a consultation paper on 'Privacy, Security and Ownership of the Data in the Telecom Sector' ('the Consultation Paper'). The aim of the Consultation Paper is to identify the key issues pertaining to data protection in relation to the delivery of digital services in India and to invite feedback from public stakeholders on the questions identified in the Consultation Paper. Kartik Maheshwari, Aaron Kamath, and Abhishek Senthilnathan, Leader, Lawyer and Associate respectively at Nishith Desai Associates, assess the key points and implications of the Consultation Paper.

Background and context

The Consultation Paper has been prepared and released by the TRAI in light of the extensive debate on privacy and data protection in general and the need to formulate and put in place a legislative framework for the protection of data in India.

Data protection was first addressed by the Government under the Information Technology Act, 2000 ('IT Act'). The IT Act contained certain provisions which provided for the protection of data stored in computer systems. However, there was no explicit framework in place which dealt with the protection of personal or sensitive data, or information that was collected or processed by entities in India. The Government took steps in 2008 to resolve this by amending the IT Act to specify that 'a body corporate which is in possession of sensitive personal data, is negligent in maintaining reasonable security practises and as a result causes wrongful loss or gain to any person, shall be liable to pay damages by way of compensation, not exceeding five crore rupees [approx. €650,000], to the person so affected[1].' However, the Government failed to specifically define the phrase 'sensitive personal data' and therefore there was no clarity as to which data was specifically protected under the IT Act.

The Government took cognizance of the absence of a specific definition of 'sensitive personal data' under the IT Act and enacted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules) 2011 ('Data Protection Rules'), wherein a specific definition was provided for 'sensitive personal data or information' ('SPDI') to include 'passwords, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, and biometric information[2].' In addition, a list of requirements were set out which were to be adhered to by any body corporate in India collecting, storing, processing or transferring SPDI. However, there have been several questions that have arisen with regard to the effectiveness of the Data Protection Rules, due to the fact that the requirements set out under them were restricted only to certain kinds of information and because there is no protection as such for information that does not fall under the definition of SPDI.

These concerns have been brought to the forefront as a result of two suits before courts in India, namely:

- *K.S Puttaswamy & Anr. v Union of India & Ors.*[3] wherein the manner of collection and processing of data by the Government under the Aadhaar scheme[4] was challenged on the grounds of being in violation of Articles 19(1) of the Constitution of India, which protects certain rights regarding free speech, and Article 21, which protects life and personal liberty. The Supreme Court held privacy to be a fundamental right guaranteed under the Constitution and also highlighted the need for a comprehensive data protection law to be introduced by the Government, which should apply to non-state actors; and
- *Karmanya Singh Sareen & Anr. v. Union of India & Ors.*[5], wherein the manner in which consent for the collection and sharing of sensitive data of consumers by WhatsApp Inc. with Facebook Inc. was also challenged on the grounds of being in violation of Articles 19(1) and 21 of the Constitution.

In light of the concerns raised with regard to the inadequacy of the existing data protection framework, the Ministry of Electronics and Information Technology ('MeitY') constituted a committee of experts in July 2017, under the chairmanship of Justice B.N Srikrishna, to identify key data protection issues in India, to recommend methods of addressing such issues and to prepare a draft data protection bill that may be introduced in Parliament.

In light of similar concerns in the telecom sector, the TRAI has also released this Consultation Paper to highlight the key issues pertaining to data protection in relation to the delivery of digital services and to invite feedback from public stakeholders with regard to these issues.

Key points from the Consultation Paper

Jurisdiction

From the Consultation Paper, it is evident that the TRAI is looking to address issues

While the title of the Consultation Paper appears to address issues in the telecom sector, it clearly raises a wider set of questions. Whilst these questions may be relevant and timely, the question as to whether the TRAI has over stepped its powers remains unanswered.

Image: Jayakumar Ananthan / Unsplash.com

1. Section 43A of the IT Act.
2. Rule 3 of the Data Protection Rules.
3. WP (Civil) No. 35071 of 2012, decided on 24 August 2017.
4. An Aadhaar number is a 12 digit unique-identity number issued to all Indian citizens by the Government, based on their biometric and demographic data. Indian citizens can use their Aadhaar numbers to avail of social welfare schemes instituted by the Government of India, as well as other purposes such as verification in filing tax returns.
5. WP (Civil) No. 7663 of 2016.
6. Chapter III, Paragraph 3.1 of the Consultation Paper.

continued

pertaining to data collection by licence service providers, but also by third party service providers such as software applications, app stores, over-the-top ('OTT') service providers, operating systems and advertising providers[6].

However, from a reading of the Telecom Regulatory Authority of India Act, 1997 ('TRAI Act'), it appears that that the ambit of the TRAI should only extend to licensed telecommunications services and licensed services providers and not to non-telecommunication service providers. Furthermore, given that the TRAI is not entitled to amend licence conditions for licensed telecommunications service providers, it may make suggestions to the Department of Telecom ('DoT') to carry out data protection amendments. However, it may not be possible for the DoT to enact a general data protection regime, which extends beyond telecom licensees, since the Government of India (Allocation of Business) Rules, 1961 ('Allocation Rules') provide that MeitY would be the nodal body responsible for enacting all matters related to the internet (other than licensing) on this subject. It appears that the TRAI has recognised this limitation and news reports suggest that the Chairman of the TRAI has clarified that the scope of the Consultation Paper is limited to the telecom sector and that recommendations of this consultation process could also be shared with MeitY to take into consideration when framing the new data privacy law in the country.

Cross-border transfer of information

The TRAI has also sought to address the issue of cross-border transfers of information. The TRAI has observed that the Data Protection Rules and the IT Act do not expressly provide any authority in India with the jurisdiction to regulate service providers who do not have a physical presence in India. Resultantly, such service providers may freely transfer any information collected in India to their data centres outside India for processing. However, as mentioned above, the TRAI's jurisdiction may not extend to parties who are not licensed telecom service providers. Issues such as cross-border transfers of information could therefore be addressed in the new data protection framework being formulated by MeitY.

Government audit and compliance

The TRAI has also observed that one manner of ensuring that entities that are collecting and processing information in India comply with the applicable data protection standards, is placing an obligation on such entities to carry out compliance audits to ensure that their data security measures are in compliance with the standards as prescribed under applicable law.

The TRAI has suggested that an audit mechanism with the oversight of the Government be put in place to ensure compliance with the new data protection framework. However, it may be beneficial for the industry as a whole if an auditing regime based on self-regulation driven by an industry best practices regime is put in place with minimal or no intervention from the Government.

Categorisation of data

It seems that the TRAI has placed all the information collected and processed in India in a single bracket of personal information in the Consultation Paper and has suggested a single standard of protection for such information in India. It would be advisable for it to segregate data on the basis of the sensitivity of the data and specify that different categories of data should have different levels of protection such as opt-in/out, consent requirements, purposes for collection and use, data sharing, and transfers.

Such segregation is already in place under the IT Act and the Data Protection Rules, wherein SPDI and personal information have already been categorised separately as provided above. Adequate revisions may be made to such definitions and the data protection framework for each category may be strengthened as required.

Data analytics and Big Data

From the Consultation Paper, it appears that one of the objectives of the TRAI is to put in place a data protection regime that is more suited to specifically regulate the data analytics industry in India. However, it should be noted that information that is processed by the data analytics industry is mostly anonymised and to that extent may not be capable of identifying individuals. In light of the above, regulation of the data analytics industry in India may restrict growth in the industry as well as form a barrier to entry for new industry players. Therefore, we believe that it is important that the aforementioned distinction on categorisation of data should be clearly made.

Data monopoly

Another issue identified by the TRAI in the Consultation Paper is the issue of data monopolies and the creation of data sandboxes to encourage innovation in India. However, it may be preferable if there is minimal or no Governmental intervention in requiring private parties who are collecting and processing customer data, to share such data with the Government or with other third parties.

The Government may, however, consider encouraging private parties to set up data sandboxes and implement measures to foster the growth of such data sandboxes in India, wherein private parties are encouraged to voluntarily share information to foster innovation and growth of new services and business in India whilst being mindful of applicable competition and anti-trust laws.

Conclusion

While the title of the Consultation Paper appears to address issues in the telecom sector, it clearly raises a wider set of questions. Whilst these questions may be relevant and timely, the question as to whether the TRAI has overstepped its powers remains unanswered. MeitY, which is provided with the clear mandate to formulate legislation with regard to the internet has constituted a committee of experts to deliberate and formulate a comprehensive and robust data protection framework in India. Given that such a committee has been established, the TRAI should provide the comments received from the public stakeholders to MeitY to serve as guidance for the comprehensive data protection framework that it is formulating.