Vaibhav Parikh Leader and Head of the TMT and Corporate Law Practice Group
vaibhav.parikh@nishithdesai.com

Aaron Kamath Lawyer
aaron.kamath@nishithdesai.com

Abhishek Senthilnathan Lawyer
Nishith Desai Associates, Bangalore

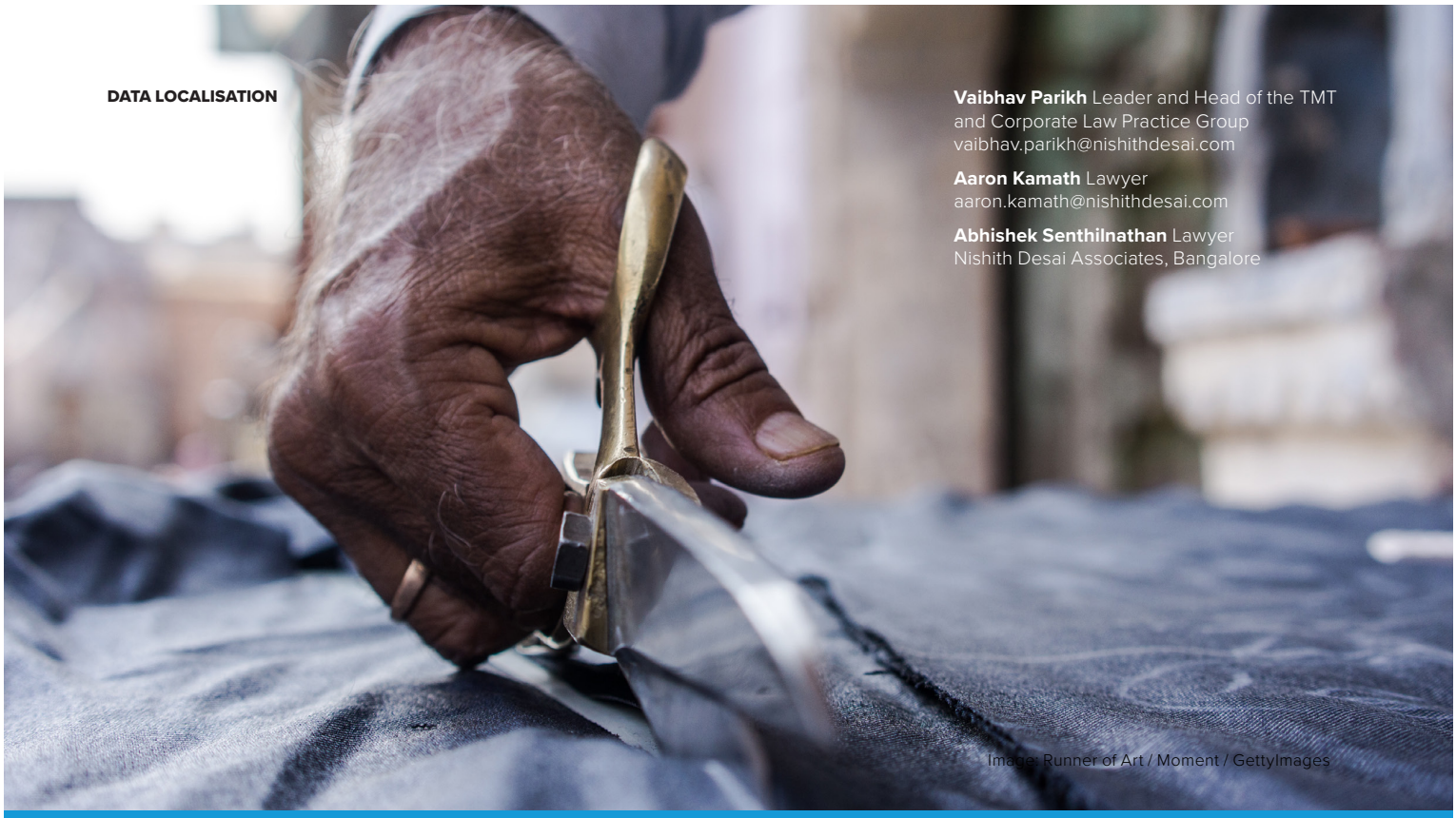

Image: Runner of Art / Moment / GettyImages

India steps towards localisation of payment systems data

The Reserve Bank of India ('RBI') issued on 6 April 2018 a Notification on the Storage of Payment System Data, which requires amongst other things that all payment system providers ensure that all of the data relating to payment systems operated by them are only stored in a system in India. For the 'foreign leg of the transaction,' the data can also be stored in the foreign country, if required. Vaibhav Parikh, Aaron Kamath and Abhishek Senthilnathan of Nishith Desai Associates, discuss the new data localisation requirements in India relating to payment systems and the areas of ambiguity.

The digital payments sector in India has undergone a massive surge and experienced major growth in both rural and urban areas in recent years. The Indian digital payments industry is expected to reach USD 700 billion by 2022 in terms of the value of transactions and is further expected to contribute to 15% of gross domestic product ('GDP') in India by 2020[1]. In addition, the industry is expected to witness a compound annual growth rate of 59% during the period 2017-2023[2].

Recognising the growth and the promise of the digital payments sector in India and corresponding security related issues and risks, the RBI, India's central bank, recently issued a Notification directing all payment system providers operating in India to ensure that the data relating to the payment system operated by them is only stored in a system in India. The Notification has been issued to address growing concerns with regard to the security standards/measures in place in the digital payments sector and to provide for 'unfettered' access by the RBI to such data. The Notification has also been introduced at a time when India is on the brink of adopting a new general data protection law.

Highlights of the Notification

1. The Notification directs all digital payment system providers to ensure that all the data relating to payment systems operated by them are only stored in a system in India.

2. The Notification clarifies that the 'data' to be stored in India includes 'full end-to-end transaction details/information collected/carried/processed as part of the message/payment instruction.'

3. Further, the Notification clarifies that with regard to a 'foreign leg of a transaction' (if any), the data could also be stored in the foreign country, if required.

4. Payment system providers in India will need to comply with the Notification by 15 October 2018.

5. An audit is also required to be carried out by payment system providers and a compliance report is to be submitted to the RBI by the end of 2018.

Analysis

No clear definition of 'data'

The term 'data' has not been specifically defined in the Notification. The Notification provides that 'data should include the full end-to-end transaction details/information collected/carried/processed as part of the message/payment instruction.' This definition is not exhaustive, which may lead to interpretation issues and ambiguity

Although the intent of the RBI behind issuing the Notification is clear, the RBI should have perhaps followed a more consultative process.

as to the types of data subject to the localisation requirement.

Data only to be stored in India

Another issue that may arise is the requirement of data having to be stored by payment system providers only in a system based in India. The Notification may imply that there is a prohibition on storing copies of such data overseas even if the data is stored in India. The RBI in introducing this particular requirement has provided neither reason nor rationale for doing so.

Exception to the data localisation requirement: 'foreign leg' of the transaction

The Notification provides for an exemption to the data localisation requirement, i.e. for a 'foreign leg of a transaction,' the data can be stored in the foreign country, if required. However, the meaning of the term 'foreign leg of a transaction' has not been clarified in the Notification. This may lead to ambiguity in the interpretation of what may actually constitute a 'foreign leg of a transaction' along with what data may be permitted to be stored overseas.

Concerns for MNCs operating in India

The new data localisation requirement may adversely impact multinational companies ('MNCs') operating in India as internal policies of the group companies of an Indian MNC may require inter-company transfers of data including to comply with the security policies of the group. MNCs, especially in the payments and financial services industry may also require customer transactional data for analytics purposes and for improving their own products and services. Data is a big asset for such companies and fluid data flows are key to global operations. Having said that, the data localisation requirement is applicable only to the payment system providers in India. Hence, if an Indian company engages a payment gateway to facilitate customer payments, the restriction is on the payment gateway, not on the Indian company, to share the data overseas. Hence, an argument may be made that a payment gateway engaged by an Indian company may share customer data with the concerned Indian company, which may then share/transfer such data to overseas entities.

Furthermore, the new data localisation requirement may also lead to MNCs incurring significant costs in setting up infrastructure to store data in India in order to comply with the data localisation requirement. Additionally, there may be technological and logistical hurdles involved.

Conclusion

Upcoming data protection law

Concerns pertaining to the protection of data in India have become more prominent following the judgment of the Supreme Court in *K.S Puttaswamy & Anr. v. Union of India & Ors*[3], wherein the right to privacy was held to be a fundamental right enforceable against the State. The Supreme Court also went on to comment that there is an immediate need for a comprehensive data protection framework to be enacted in India including for enforcement of rights against private and non-State parties.

Thereafter, the Ministry of Electronics and Information Technology constituted a committee of experts in July 2017, under the chairmanship of Justice B.N. Srikrishna (a former judge of the Supreme Court) to identify and analyse key data protection issues in India and to provide recommendations for the new data protection law to be enacted in India. The committee released a white paper[4] and requested input from the public and relevant stakeholders which were provided by the end of January 2018. Physical consultations were also held by the committee in major cities in India. The committee's recommendations are expected to be published in June[5] and a draft data protection bill is expected in the next couple of months.

In light of the above, the RBI may have considered waiting for the enactment of the new data protection framework prior to issuing the Notification, in order to ensure alignment with the new data protection framework. The new data protection law may seek to address widespread issues in India including the location of data across different industries.

The law making process

Although the intent of the RBI behind issuing the Notification is clear, the RBI should have perhaps followed a more consultative process by releasing a draft form of the law and inviting comments from the public and the relevant stakeholders in the digital payments ecosystem. A similar process was carried out earlier by the RBI when issuing the 'Master Directions on Issuance and Operation of Prepaid Payment Instruments[6]' in 2017. Of late, regulators such as the Telecom Regulatory Authority of India have followed such a consultative process whilst framing laws on sensitive aspects that may affect several stakeholders, such as net neutrality, data protection/privacy in the telecommunications sector etc. Such a consultative process may have adequately addressed the issues and ambiguities in the Notification that have been specifically detailed above as well as taken care of the concerns of industry players.

We understand that industry associations have been engaging in a dialogue with the RBI post issuance of the Notification, voicing their concerns on the localisation requirement as well as the ambiguities concerning compliance[7]. We understand that the RBI may also issue clarificatory notes or FAQs on the Notification in the coming weeks, which at this stage is much needed.

1. https://www.reuters.com/brandfeatures/venture-capital/article?id=21598, last accessed on 27 May 2018.
2. https://www.idc.com/getdoc.jsp?containerId=prAP43454117, last accessed on 27 May 2018.
3. Writ Petition (Civil) No. 494 of 2012, decided on 24 August 2017.
4. http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf, last accessed on 27 May 2018.
5. https://economictimes.indiatimes.com/tech/internet/expect-recommendations-of-the-srikrishna-committee-by-june-on-data-protection-law-ravi-shankar-prasad/articleshow/64098109.cms, last accessed on 27 May 2018.
6. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/58PPIS11102017A79E58CAEA28472A94596CFA79A1FA3F.PDF, last accessed on 27 May 2018.
7. https://economictimes.indiatimes.com/news/economy/policy/rbi-note-on-data-localisation-raises-hackles-in-the us/articleshow/63966786.cms, last accessed on 28 May 2018.