Personal Data Protection Bill, 2019: Considering data localisation and its effects on payments

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the third article in the series. Read our extensive coverage of the Bill here.

By Nikhil Sud

This article has been written considering this scenario in light of the Personal Data Protection Bill, 2019:

An OTT platform offers services in India but uses an international payment gateway to process payments. Does the OTT platform need to be a part of a DPA-approved intra-group scheme? What about the payment gateway? How does the intra-group scheme requirement interact with the RBI's data localisation mandate?

Considering the scenario — a few impressions

(The following does not constitute legal advice.)

This scenario involves two types of data:

1. The payments data noted in the scenario and
2. Any other data that the OTT platform processes as part of its service offering.

However, this article — like the scenario — focuses on type (1). The Personal Data Protection (PDP) Bill's localisation provisions likely apply to this data for multiple reasons.

First, this data likely comprises "personal data" per the Bill's definition of "personal data". The definition, given its concerning breadth, would likely apply despite measures that the OTT platform or payment gateway may take to make it difficult to identify individuals from this data.

Note: If, however, this data is anonymised (per the Bill's definition of "anonymisation" which requires, arguably impractically, "irreversible" anonymisation), then the Bill would consider the data "non-personal data," potentially allowing the government to demand access to that data to help the government improve the delivery of government services. Complying with this demand may require some form of localisation, depending on the additional guidance the government is expected to release on non-personal data. Policymakers should have reserved the matter of "non-personal data" entirely for a separate proposal and consultation, in line with the separate committee established by MEITY to explore "non-personal data". This is because non-personal data, by definition, does not

pertain to privacy (the core and impetus of the PDP Bill), and because its exact meaning and how exactly it should (and whether it can) be used without hampering innovation and competition are highly complex issues, meriting deep, thoughtful analysis and consultation before any legislative activity. Illustratively, India's draft e-commerce policy, published early last year, addressed non-personal data without thorough consultation, resulting in language that was confusing, inconsistent, and potentially detrimental to competition and innovation.

Second, this data likely comprises "sensitive personal data" under the Bill's controversially broad definitions of "sensitive personal data" and "financial data."

Note: Of course, the fact that (per the scenario) much of this data's processing is likely conducted abroad by the international payment gateway likely does not protect that processing from the Bill's localisation provisions. This is because that data was likely collected in India and had to be transferred abroad (which seems the sort of data for which the Bill's localisation provisions are designed — Section 34, which articulates these provisions, is framed as discussing the "transfer" of data outside India), and because the non-Indian nature of the gateway likely does not shield it from the Bill's obligations (see, for example, Section (2)(A)(c)(i)). If, however, this data was not collected in India (which seems unlikely), then it is unclear if any localisation requirements would exist. Section 2(A)(c)(i) suggests that the Bill would apply, implying that its localisation requirements would exist; however, the Bill's localisation requirements appear to assume that the data (to which they apply) was collected in India (as noted above, the Bill – when addressing localisation – prescribes requirements for the "transfer" of data abroad).

Transferring this data abroad

Setting aside the aforementioned complexity and proceeding on the basis that this data was collected in India (and, as discussed above, this data comprises "sensitive personal data"), this data "may be transferred outside India, but … shall continue to be stored in India" per the Bill. Policymakers should clarify the meaning of this language. It could mean that though the data can be transferred abroad temporarily for processing, it must be brought back to India and stored in India after the processing. It could alternatively mean (among potentially other things) that even if this data is transferred abroad, a copy of it must remain in India.

Either way, for the data to move abroad, the data principal must provide explicit consent, and certain other requirements must also be met per Section 34, which deals with the transfer of data abroad.

Using an intra-group scheme

One option, per Section 34, is for the transfer to occur through an intra-group scheme between the OTT platform and the payment gateway.

Note: Assuming that the OTT platform "determines [alone or in conjunction

with the payment gateway] the purpose and means of processing" the data, the OTT platform is likely the "data fiduciary" and the payment gateway is likely a "data processor" per the Bill. Both parties are thus subject to obligations in the Bill, but per Section 10 of the Bill, the data fiduciary is responsible for compliance with the Bill in relation to the processing it undertakes or the processing that others – such as data processors – undertake on its behalf.

The scheme between the OTT platform and the gateway would need approval from the Data Protection Authority (DPA). For approval, the DPA will likely require (among other things) that the scheme contain "effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person." Policymakers should provide guidance on the precise meaning of this language. For example, what exactly constitutes "effective protection"? More fundamentally, requiring DPA-approved schemes is not ideal; it can strain the resources of the DPA, the data fiduciary, and the data processor, and foster uncertainty, potentially chilling data flow, investment, and innovation. Policymakers could instead consider incorporating into the Bill the principles articulated in the voluntary and widely embraced APEC Privacy framework and the APEC Cross Border Privacy Rules (CBPR) which seek to balance innovation with privacy.

Besides using an intra-group scheme, the platform has other options

It could attempt invoking the Bill's Sections 34(1)(b) or 34(1)(c). Both would likely require engaging with the government and the DPA.

1. Under Section 34(1)(b), the government — in consultation with the DPA — could allow transferring this data abroad if it concludes that the data will be adequately protected in the destination country. However, it is unclear how the government will assess adequacy; policymakers should make this clear and consult all stakeholders when deciding how the government will assess adequacy. Section 34(1)(b) also requires that the transfer "shall not prejudicially affect the enforcement of relevant laws". This language too calls for clarity, and risks a broad interpretation that could stifle data flow, given the strikingly wide powers the bill elsewhere provides the government to collect and process personal data.
2. Under Section 34(1)(c) of the Bill, the DPA could allow the "transfer of any sensitive personal data…for any specific purpose." The seemingly welcoming language of this provision — signaling an openness to data flow — is at least partly offset by the lack of clarity on how the DPA will make this assessment. The assessment should be conducted reasonably and transparently, and all stakeholders including industry should be consulted when policymakers decide how the DPA will conduct this assessment.

Interplay between RBI's localisation mandate and PDP Bill

The interplay creates the risk of a fragmented landscape with potentially unclear and conflicting obligations, stunting innovation and investment. This risk is

exacerbated by the confusion surrounding the RBI's mandate, alleviated only partially by the guidance (FAQs) that the RBI released in June 2019, more than a year after it issued the mandate in April 2018.

Broadly, while all of the payments data mentioned in the scenario likely falls under the scope of the Bill, some of that data (though not necessarily all of it) may *also* fall under the scope of the RBI's mandate, depending on the exact nature of the data processed by the gateway, and on the categories of data articulated in the RBI's localisation guidance. For the data to which both sets of rules apply, it is unclear which set trumps the other. The PDP Bill, designed as a cross-sector bill, should arguably trump the RBI's rules (especially given Section 96 of the Bill, discussing the overriding effect of the Bill).

However, the PDP Bill frequently recognizes the importance of sectoral regulators in shaping data protection rules, potentially signaling deference to them. Additionally, policymakers in their public comments have generally signaled some deference to sectoral regulators. Further, in situations where the RBI's rules exceed the PDP Bill's rules, policymakers may construe the two sets of rules not as inconsistent but as complementary – they may interpret the PDP Bill as setting the baseline, and the RBI as adding requirements beyond the baseline, thereby allowing the RBI's rules to apply.

Separately, at least three additional sources of uncertainty and complexity exist:

First, the PDP Bill requires "critical personal data" to be processed only in India (subject to certain exceptions) but does not define "critical personal data." It defers to the government for the definition. If the government defines "critical personal data" to include some forms of financial data, that could alter the assessment above, and impose heightened obligations. Relatedly, if the government defines "critical personal data" in consultation with sectoral regulators such as the RBI, the definition could support the RBI's localisation goals (which appear to exceed the PDP Bill's localisation goals), impacting the assessment above regarding the interplay between the PDP Bill and the RBI's mandate.

Second, the PDP Bill empowers the DPA and the government to issue substantial additional guidance on a variety of matters including localisation. Until this guidance is issued, uncertainty will persist. There is also a risk that this guidance is overly stringent. Though the Bill commendably requires every rule and regulation made under it to be tabled in Parliament, the government and the DPA should consult all stakeholders, including industry, before developing any such additional guidance.

Third, policymakers' views on these issues frequently evolve and this evolution is not always reflected — or reflected in a timely manner — in the written materials produced by policymakers. Further, and relatedly, some policymakers sometimes signal one view on the meaning of a policy, while others signal a different view on the same policy, neither of which is reflected in written materials.

This all perhaps stems from the complexity of these issues, but policymakers should react to that complexity differently: they should adopt thorough, transparent, well-organized, collaborative, and numerous wide-ranging consultations, fueling a coherent and clearly articulated policy. Otherwise, industry is forced to make critically important investment decisions based on information that is sparse, ambiguous, and unreliable (as it may not reflect policymakers' latest thinking, or it may reflect one policymaker's thinking but not another's). This all risks deterring investment and innovation, and ultimately hurting consumers.

In conclusion

The Bill's data localisation requirements would likely apply to the data in this scenario. Complying with these requirements can prove challenging, forcing the platform to navigate complex and onerous rules. Additionally, the platform faces significant uncertainty, stemming from the Bill's ambiguous language, the unclear interplay between the Bill and the RBI's localisation mandate, and the wide rule-making powers the Bill provides to the government and the DPA. These challenges could hinder the platform's ability to invest in India and innovate for Indian consumers. This is particularly concerning because the Bill's and the RBI's data localisation requirements may not materially bolster data security; are unnecessary for law enforcement; and risk creating a starkly uneven playing field between Indian and international players (though likely hurting Indian players much more than policymakers may anticipate).

*

Nikhil Sud *serves as Regulatory Affairs Specialist at the Albright Stonebridge Group. He is a lawyer by training and specialises in legal and policy issues relating to technology.*

Edited by Trisha Jalan