ALBRIGHT STONEBRIDGE GROUP

UPDATE ON INDIA'S NEW DATA PROTECTION BILL: SOME BALANCE, MANY RISKS

AUGUST 2, 2018

OVERVIEW

Last year, India's Ministry of Electronics & Information Technology (MeitY) established a committee to craft a cross-sector data protection law. On July 27, 2018, the committee submitted a draft bill and an explanatory report to MeitY. MeitY is expected to study the bill and report, consult other ministries and stakeholders, edit the bill if it chooses, and send it to Parliament. The timeline is uncertain, but the bill may be tabled at Parliament's winter session this year. The key challenge in designing this data protection law is bolstering privacy without hindering innovation, a critical balance for India's socio-economic growth. As discussed below, while certain aspects of the bill could achieve this balance, others risk stifling innovation.

POTENTIALLY BALANCED ASPECTS

- *Several obligations incorporate a "reasonableness" standard.* For example:
    - The bill recognizes that always requiring consent can impede cutting-edge technologies and is unnecessary because consent can sometimes reasonably be inferred. The bill permits data processing, even without consent, if the purpose of processing is "reasonable." It articulates factors determining reasonableness, including the interest of the data fiduciary (the entity processing the data) and the expectations of the data principal (the individual whose data is being processed).
    - The data fiduciary must take *reasonable* steps to ensure that personal data is accurate, and retain personal data only till it is *reasonably* necessary to fulfil the purpose for which it was collected.
- *Tailored rights for data principals.* The bill provides data principals substantial control over their data through the rights to confirm whether their data is being processed, to access a summary of the data being processed and of the processing activities, to correct data, to restrict its disclosure, and to port it. However, overly broad rights could raise fiduciaries' costs and hamper innovation. The bill helps mitigate these risks. For example, data principals may access only a summary of their data (as noted above), rather than all of it; they may demand portability only if it is technically feasible and would not reveal the fiduciary's trade secrets; and free speech concerns limit the right to restrict disclosure. Additionally, the fiduciary may charge a reasonable fee for some of these rights. Further, the right to access the logic behind automated decisions – which risked revealing proprietary algorithms to the detriment of competition and innovation – is missing from the bill.

ABOUT ASG

Albright Stonebridge Group (ASG) is the premier global strategy and commercial diplomacy firm. We help clients understand and successfully navigate the intersection of public, private, and social sectors in international markets. ASG's worldwide team has served clients in more than 110 countries.

ALBRIGHTSTONEBRIDGE.COM

- *Transition times and no retrospective application.* The bill provides transition times to help fiduciaries comply, as several provisions may require significant organizational changes. Additionally, the law will apply only to activities undertaken after it comes into force. The alternative – i.e. retrospective application – could be impractical, raise costs substantially, and divert resources away from innovation.

KEY RISKS TO INNOVATION

- *Extraterritorial application.* The law will apply not just to data processed in India, but also to data processed abroad, including if the processing relates to certain broadly defined activities (any business carried on in India, any systematic activity of offering goods or services to data principals in India, or any activity involving profiling data principals in India). This extraterritorial application can lead to conflicting obligations from different jurisdictions, raising costs and discouraging innovation.

- *Data localization.* The bill requires that every data fiduciary store at least one copy of data in India. Further, it directs the government to identify categories of "critical" data, which must be stored only in India. These obligations, coupled with potentially restrictive cross-border data-flow requirements, risk significantly impairing innovation by raising costs (potentially prohibitively for small and medium enterprises) and undermining highly beneficial emerging technologies that rely significantly on global networks, like cloud computing. Notably, the bill in a different context categorizes financial data as sensitive, raising the likelihood that the government will classify payments data as critical in the localization context. This would affirm the Reserve Bank of India's highly contentious mandate to store payments data exclusively in India. Tellingly, two members of the bill's drafting committee issued forceful dissents against its localization requirements, labelling them "not only regressive but against the fundamental tenets of [India's] liberal economy" and opposed to "the basic philosophy of the [i]nternet."

- *State surveillance.* The bill provides broad powers to the government to access and use personal data. For example, it permits non-consensual processing for "state functions." It also exempts the government from several obligations in the interest of preventing, investigating, or prosecuting illegal activity. Such provisions – especially combined with the aforementioned localization requirements – risk creating an environment where citizens fear sharing data even with non-government entities (in exchange for innovative services), due to concerns that the government may easily access and use that data. Surprisingly, the bill expressly recognizes the need for judicial oversight of government use of personal data but does not require it.

- *Onerous "accountability" requirements.* The bill requires that data fiduciaries be able to demonstrate compliance. To this end, it imposes several potentially onerous obligations, including impact assessments, audits, record-keeping, and appointing a data protection officer. Several such requirements apply only to "significant" data fiduciaries, i.e. those that can cause significantly greater harm given factors like the amount and nature of data they process. However, many fiduciaries may qualify as "significant" based on how these factors are interpreted.

- *Criminal liability.* The bill imposes criminal liability for certain acts including obtaining, disclosing, transferring, selling, or offering to sell personal data in contravention of the law. The harshness of criminal liability risks chilling investment and innovation, even if liability is limited to intentional, reckless, or knowing acts. Notably, one member of the bill's drafting committee dissented against criminal liability, calling it draconian and unnecessary, especially given the significant civil penalties the bill also imposes.

- *Uncertainty regarding precise requirements.* The bill establishes the Data Protection Authority (DPA), an autonomous regulatory body, to enforce the law. The DPA's responsibilities include developing specific requirements ("codes of practice") to supplement the law's many broad articulations, including for notice and consent requirements; obligations relating to the quality and retention of data; processing of sensitive personal data (i.e. particularly sensitive types of data); processing for "reasonable" purposes as discussed above; data principals' rights; accountability obligations; methods for de-identification and anonymization (the law applies to de-identified data but not to anonymized data); cross-border data transfer; and any other matter the DPA chooses. Until the DPA issues these codes, data fiduciaries' precise obligations remain uncertain, and there is a risk that they may be so stringent that they hamper innovation. Consulting industry when developing these codes can help balance privacy and innovation, given the insights industry can offer. While the bill requires that the DPA consult stakeholders before issuing codes, the extent and nature of that consultation remains to be seen. Relatedly, industry should consider proactively engaging with the DPA on the issuance of these codes.

- *Fragmented landscape.* While this bill applies across sectors, other sections of the government have undertaken data protection initiatives in parallel, risking a fragmented landscape with unclear if not conflicting requirements. MeitY is expected to consult other ministries before bringing the law to Parliament, and the bill requires the DPA to consult across sectors before issuing codes of practice. These consultations could mitigate fragmentation but, as above, that will depend on the extent and nature of these consultations.

In May 2018, ASG published this analysis on India's evolving data protection regime and this op-ed on unique risks this regime poses.

ASG's South Asia Practice has extensive experience helping clients navigate markets across South Asia. Please contact Nikhil Sud with questions or to arrange a follow-up conversation.
