ALBRIGHT STONEBRIDGE GROUP

INDIA'S NEW APPROACH TO DATA PROTECTION

MAY 21, 2018

OVERVIEW

With consumers increasingly providing data regarding themselves to companies (particularly technology and internet companies) and several recent large-scale breeches of consumer data, regulators around the world are turning their attention to data protection. The most high-profile among these regulatory efforts is the European Union's General Data Protection Regulation (GDPR), which becomes effective May 25, 2018. The GDPR impacts companies that collect and process the data of customers residing in the EU, requiring robust data protection measures, and imposing significant penalties for non-compliance. While companies focus on complying with this far-reaching new law, they should not lose sight of developments in India. India is crafting a new cross-sector data regime, which could significantly affect companies around the world collecting and processing the data of customers residing in India. Below is an overview of recent developments in India's efforts, followed by a discussion of key issues that Indian policymakers, regulators, and companies serving Indian customers, will need to consider.

SIGNIFICANT DEVELOPMENTS

- Late last year, after the Indian Supreme Court declared privacy a fundamental right, India's Ministry of Electronics & Information Technology (MeitY) formed a committee to develop a comprehensive cross-sector data protection law. The committee collected public input in January this year, and is expected to submit its draft of the law to MeitY by the end of June.

- The Cambridge Analytica incident, which unfolded in March of this year, triggered a spike in commentary globally on the need for urgent and stringent data protection measures. Since then, other sections of the Indian government have undertaken data protection efforts, including: the Reserve Bank of India's recent data localization mandate for the payments ecosystem; the Ministry of Health and Family Welfare's new draft law focused on the protection of health-related data; and the Ministry of Commerce's think tank that will contemplate, among other things, data protection in the e-commerce context.

- Because each of these efforts is separate from MeitY's cross-sector initiative, a fragmented landscape may emerge with conflicting and unclear data protection obligations. If this happens,

increased compliance costs are likely to follow. Alternatively, assuming policymakers seek to vary data protection measures slightly between different sectors, tailoring MeitY's cross-sector law to incorporate those variations would likely lead to a more cohesive and predictable regulatory landscape.

ISSUES

As MeitY develops the law, it will grapple with the fundamental challenge in crafting data protection measures: strengthening privacy without stifling innovation. The Indian government has been championing innovation and investment, particularly in the technology and internet space, through multiple initiatives including Digital India. Such innovation and investment promise significant socio-economic benefits across India, but often rely heavily on the flow of data. MeitY will need to consider multiple issues as it addresses the difficult challenge of balancing privacy with innovation, as discussed below.

- *Consent.* MeitY is considering whether companies should be allowed to collect and process data on grounds other than consent. Limiting the grounds to consent can be a tempting way to give individuals control. However, requiring consent each time data is collected can burden the company and the individual. One outcome is often "consent fatigue," whereby consumers bombarded with consent prompts simply click "accept" without reviewing the terms of the consent form. Furthermore, emerging technologies may need to regularly collect and process different types of data to provide beneficial services, such as smart home devices; requiring consent each time can undermine these benefits. One solution in certain circumstances could be to permit data collection and processing if consent can be reasonably inferred, based on the context of the transaction or on the user's relationship with the organization. This approach can be supplemented with allowing users to "opt-out" of providing particular types of data or data for particular uses.

- *Data localization.* MeitY is considering whether to require data localization, which would require the personal data of Indian individuals to be stored within India. Proponents of localization argue, among other things, that storing data within the country's borders makes it easier for the government to keep the data safe. However, the potential downsides of localization include significant costs on businesses (including the costs to reorganize and relocate data, and identify or establish new data centers), and diminished quality of service as local operations may lack the efficiency of global cross-border networks. One approach policymakers may consider – that might balance some of these concerns – is localizing only data from particularly sensitive sectors, rather than data across all sectors.

- *Individual participation rights.* Individuals' "participation" rights include, among others, the right to confirm what data about them has been collected and how it is being used, the right to rectify collected data, the right to access the logic behind automated decisions (e.g., decisions based on algorithms), and the right to data portability (requiring the organization processing the data to maintain it in a format portable to other platforms). These rights may help provide individuals greater control over the use of their data. However, they may also impose substantial costs on businesses, which could divert resources away from innovation. Further, disclosing details behind algorithmic decisions can be impractical given algorithms' complexity and may result in revealing proprietary technology to competitors, thereby harming competition and innovation.

- *Liability standards.* MeitY is contemplating standards of liability. Under the strict liability standard, the company collecting and processing the data would be liable for any harm an individual suffers due to a security breach even if the company had taken all reasonable measures under the law to prevent that breach. This could significantly stymie innovation in India. A negligence standard, which imposes liability only if the company did not act reasonably, may strike a better balance between privacy and innovation.

- *Role of industry in framing regulations.* MeitY is considering how much say industry should have in framing data protection regulations. Options include:

  - a "command and control" model in which the government prescribes clear and specific rules, and industry has little or no role;
  - a "co-regulatory" model in which the government provides a broad statute which is supplemented by codes of conduct framed by industry (and approved by the government); and
  - a "self-regulation" framework in which market forces drive industry to frame and adhere to their own codes of conduct, with little to no role for the government.

  Industry could offer critical insights into the services consumers find beneficial, including how they like their data collected and processed; the risks associated with data collection and processing; and the technical challenges surrounding data protection. Therefore, providing industry a substantial role in framing regulations may help strike a healthy balance between privacy and innovation.

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