Harvard Business Review

Digital Article

Regulation

How India Plans to Protect Consumer Data

by Vijay Govindarajan, Anup Srivastava, and Luminita Enache

How India Plans to Protect Consumer Data

by Vijay Govindarajan, Anup Srivastava, and Luminita Enache
Published on HBR.org / December 18, 2019 / Reprint H05C04

PM Images/Getty Images

The Indian government looks set to legislate a Personal Data Protection Bill (DPB), which would control the collection, processing, storage, usage, transfer, protection, and disclosure of personal data of Indian residents. Despite its regional nature, DPB is an important development for global managers. The digital economy in India is expected to reach a valuation of $1 trillion dollars by 2022 — and it will attract numerous global players who must comply with DPB.

India has followed the EU's General Data Protection Regulation (GDPR) in allowing global digital companies to conduct business under certain

conditions, instead of following the isolationist framework of Chinese regulation that prevents global players like Facebook and Google from operating within its borders. Yet, Indian DPB carries additional provisions beyond the EU regulation. Because India is a nation state, it would treat the data generated by its citizens as a *national* asset, store and guard it within national boundaries, and reserve the right to use that data to safeguard its defense and strategic interests.

There are a number of features of the DPB that will require companies to change their business models, practices, and principles. Many others will add operational costs and complexity. The issues we raise here serve as a primer for what businesses need to keep in mind about India's new regulation and the increase in data protection regulation around the world. Understanding these issues will help digital companies plan ahead, address future regulations, and decide whether to enter or exit certain markets.

Privacy as a fundamental right: In 2017, the Supreme Court of India ruled that privacy is a constitutional right of Indian citizens. Every citizen, however, leaves a visible trail of private data while navigating in the digital world. DPB intends to protect and safeguard citizen's privacy rights by controlling the collection, security, storage, sale, and exploitation of these data. New regulation would affect the cost-benefit analysis for many digital firms that often lose money in offering free services, but aim to earn profits from the sale and exploitation of customers' personal data. Many of those digital firms would have to rethink their business models if they can no longer collect, exploit, retain, and sell user data as profitably as before.

User consent: DPB requires that a digital company must obtain explicit permission from a user before collecting their personal data. In doing so, it must explain the extent and the purpose of data collection. Explicit permission must also be obtained at each stage of subsequent data processing. Compliance with this provision could be tricky, because digital companies not only collect personal data, they also process that data to create new information that does not belong to the original user. For

example, Uber ascertains traffic patterns and Amazon analyzes feedbacks from individual transactions. Furthermore, raw data could be transferred to a third-party data processor for analysis, creating new information in conjunction with the data received from other data collectors. Companies will have to rethink their operating procedures for data tracking and security as well as ascertain whether, when, and how to obtain user permissions. Digital companies now become "data fiduciaries" as defined in the DPB, instead of being mere data collectors, when they assume responsibility for obtaining user permission for both initial collection and subsequent processing of user data.

Ownership of personal data: In principle, DPB proposes that the data provider is the owner of their own personal data. While simple in idea, this notion could impose an enormous implementation burden for digital companies. In the physical world, a property owner can ask for return of their property. Companies in the digital world would have to figure out how to comply with this requirement when the user demands erasure or recall of their personal data from a digital company — for example, when a person requests deletion of all of their information after they cease to be a Facebook member. Digital companies would also have to think beyond their own data storage and usage, because they might have sold the data to a third party.

Three classes of data: DPB has identified three categories of data from which a principal can be identified: *Sensitive* data includes information on financials, health, sexual orientation, genetics, transgender status, caste, and religious belief. *Critical* data includes information that the government stipulates from time to time as extraordinarily important, such as military or national security data. The third is a *general* category, which is not defined but contains the remaining data. DPB prescribes specific requirements that data fiduciaries must follow for the storage and processing for each data class.

All sensitive and critical data must be stored in servers located in India. Sensitive data may be processed outside but must be brought back to India for storage. Critical data cannot be taken out of the country at all. There are no restrictions for general data. Digital companies currently operate in a seamless cyber world, where they mostly store and process their data wherever is economically most efficient. This locational divide proposed by DPB would impose additional costs on digital companies, might lead to subeconomic storage and processing capacities, and might result in what some refer to as "splinternet"or the fragmentation of global digital supply chains.

Data sovereignty: DPB reserves the right to access the locally stored data to protect national interests. This implies that DPB would treat citizens' data as a *national asset*, no different than control over citizens' physical properties. In this respect, DPB differs from GDPR, which imposes no locational storage requirements or preferential access to data for protecting national interests. Currently, digital companies practically own the data as long as they can address the privacy concerns and meet the user-acceptance requirements. One implication of the new policy is that when the government demands its citizens' data, in case of foreign attacks and surveillance, digital companies would have to abide and assist the Indian government's defense policy.

National interests: While placing a large emphasis on citizens' privacy, DPB disregards privacy rights in certain cases. It states: "All or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data..." That is, various public sector entities of the government of India will not require individuals' consent to obtain their personal data when responding to the security of the state, detection of any unlawful activity or fraud, and epidemic and medical emergencies. Those data could be demanded from digital companies. In addition, the government can direct a digital company to provide non-personal or anonymized data for research or planning purpose. Critics argue that these data can be potentially misused by the

government for unintended uses such as political surveillance. Others argue that anonymous data can be easily deanonymized. Digital companies may have to change their policies to comply with these requirements. Recall Apple's refusal to unlock an iPhone for an FBI investigation. It is debatable whether Apple would be able to decline that request under DPB.

Verification tag: DPB requires that all digital companies must identify their users and tag them into three categories to reduce trolling (e.g., an anonymous user or a bot trying to incite violence by posting incendiary comments): Users who have verified their registration and display real names; users who have a verified registration but have kept their names anonymous; and users that have not verified registration. This would be a first regulation of its kind in global social media. This implies that digital companies must put in place procedures for collecting and verifying the real identities of their users. Note that Facebook has more that 100 million fake accounts and faces the dilemma of continuing as is, attempt to verify them, or delete those accounts.

Compliance and enforcement: DPB proposes steep penalties for noncompliance. In case of a data breach or inaction by the fiduciary upon data breach or a minor violation, the penalties could reach $ 700,000 or 2% of a company's global revenues, whichever is higher. For major violations, such as data shared without consent, the penalties would double. These penalties, which are based on multinationals' *global* income, and potential jail sentences for officers of digital companies, imply that DPB regulations cannot be taken lightly. Its provisions must be complied with in order to do business in India.

Taxing digital companies: As we note in a previous article, multinational digital companies can easily transfer their income to tax havens and avoid paying taxes to local governments, with no fear of confiscation of their properties. Physical control over data and fear of enforcement penalties might give the Indian government additional leverage to collect taxes and dues from digital companies. This would lower the likelihood that digital

companies can get away with paying little or no taxes to the local governments.

Other issues: The DPB applies to all businesses that collect personal data, not just digital businesses. For example, John Deere collects and processes data obtained from its farm equipment. Whether DPB applies to tractors with sensors, whether the collected data belongs to the farmers, and how the benefits of farm data are shared becomes a debatable point.

In our view, there is an urgent need for data protection regulation in India, and it is better to have one, even if a bit flawed, than none. This bill is a good first step in providing broad principles for regulation, and the detailed laws and regulations will hopefully continue to be finetuned — as happened for automotive safety standards that have evolved since the beginning of the 19th century.

When DPB becomes effective, the principles of data protection regulations would be similar across the EU, California, Canada, and India. A company that learns to comply with the regulations of one jurisdiction can easily comply with the regulations of another. Uniform standards, similar to ISO 9000, would promote global commerce. An orderly digital market would be a win-win for citizens, nations, and multinational corporations.

Vijay Govindarajan is the Coxe Distinguished Professor at Dartmouth College's Tuck School of Business and faculty partner at the Silicon Valley incubator Mach 49. He is a *New York Times* and *Wall Street Journal* bestselling author. His latest book is *The Three Box Solution*. His Harvard Business Review articles "Engineering Reverse Innovations" and "Stop the Innovation Wars" won McKinsey Awards for best article published in HBR. His HBR articles "How GE Is Disrupting Itself" and "The CEO's Role in Business Model Reinvention" are HBR all-time top 50 bestsellers. Follow Vijay on Twitter and LinkedIn.

Anup Srivastava holds Canada Research Chair in Accounting, Decision Making, and Capital Markets and is an associate professor at Haskayne School of Business, University of Calgary. In a series of HBR articles, he examines the management implications of digital disruption. He specializes in the valuation and financial reporting challenges of digital companies. Follow Anup on LinkedIn.

Luminita Enache is an associate professor at Haskayne School of Business, University of Calgary. She investigates financial disclosures of new-economy firms. Follow Luminita on LinkedIn.

