Digital Economy Kit

Switch your economy on for all

CASE STUDY

India: Drafting data protection laws

Policy and regulation

With digital technologies playing an integral part of everyday life for many Indians today, a strong personal data law is needed to protect citizens from privacy and data breaches. Current laws covering data protection and privacy lack a coherent regulatory framework and only impose obligations on private companies, and not government organisations holding large amounts of citizen data. So, in response to a Supreme Court ruling, the Indian government drafted the Personal Data Protection (PDP) bill based on the European Union's General Data Protection Regulation (GDPR). The draft bill sets out regulations on consent, collection, processing and storage of citizen data by individuals, private firms and public organisations. It lays a much-needed foundation to transition to a digital economy, but concerns remain over its provisions on data localisation, surveillance safeguards and independence of the regulator. As the Indian government works through the controversial issues before passing it into law, its example provides useful lessons for other countries.

The problem

Public interest and concern about data privacy and protection in India has increased in recent years. India has 1.2 billion mobile subscribers, 560 million internet users and 310 million social media users, and the government holds data on more than 1.2 billion citizens on its digital identity and authentication platform Aadhaar.[1, 2] But India's current laws on data protection and privacy are inadequate. The Information Technology Act 2000 and Contract Act 1872 provide guidelines on penalties in cases for data misuse but only cover private companies. They don't cover government organisations holding large amounts of citizen data on Aadhaar. The laws also fall short on recourse for citizen complaints, fine enforcement, surveillance protection and data misuse. All these came to a head in August 2017, with Supreme Court declaring the 'right to privacy' to be a fundamental part of the 'right to life and personal liberty' under the Indian constitution and ordered the government to draft a new data protection law.[3]

Solution

The Ministry of Electronics and Information Technology set up a committee to draft the new data protection law. Th committee published a white paper setting out key data protection and privacy issues in India and principles underpinning the new data protection law. After four rounds of public and private consultations on the paper, in July 2018 the committee published a draft Personal Data Protection Bill.[4]

Digital Economy Kit case study 10
November 2019

Pathways for Prosperity Commission
Technology & Inclusive Development

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

The draft bill aims to protect citizens from privacy and data breaches and push digital economy growth in India.[5] The law sets out regulations and procedures on consent, collection, processing and storage of citizen data by individuals, private firms and public organisations. It also sets out citizen rights on data purpose notice, data consent, data access, the right to be forgotten, data portability and data minimization. The draft bill also gives clear definitions of key terms including 'personal data', 'sensitive personal data' and 'data processing' to help citizens and businesses understand the law and make better decisions. Many of the key principles and procedures in the draft bill are inspired from the European Union's flagship GDPR law. One notable omission, however, is the citizens' right to erasure of personal data that GDPR guarantees. The draft bill also calls for the establishment of a national Data Protection Authority (DPA) and Adjudication Officer Body to regulate compliance, deal with violations and enforce penalties. The draft bill covers government institutions and private firms incorporated in India, and firms incorporated overseas that process data of citizens living on Indian territory (regardless of where the processing happens).[6]

Impact and risks

The draft bill provides welcome protection for citizens, however civil society and private companies hold concerns over its provisions on data localisation, surveillance safeguards and regulator independence. It requires firms to store copies of personal data on servers in India and permits the government to identify and declare that certain types of data may only be stored on servers located in India. The government justified this provision by maintaining that this will create local jobs in data management. But foreign firms have strongly resisted data localisation claiming it will restrict data flows between global firms and thus limit innovation and overseas investment.[7]

There are also concerns in the civil society, particularly among the technology policy experts who say that the risk of unrestricted law enforcement access cannot be ruled out as India lacks surveillance reform laws. Under the current laws the government has the power to order surveillance – eg accessing data and data trails – without court orders or third-party review. In the draft bill, the government has the legislative means to process data – without seeking citizen consent – for purposes different from those originally intended in the interests of state security, for legal proceedings or for journalistic purposes. While the exact nature of these provisions is still being worked through, there are critics in civil society, NGOs and the private sector who say it will give the government unrestrained access to citizen data and perverse incentives to use personal data as a resource.[8] A recent move by the Ministry of Road, Transport & Highways, India to sell citizen license and vehicle registration data to 87 private firms has only intensified the calls for stronger regulatory safeguards.[9]

Another contentious provision regards the independence of the law's regulators. The draft bill gives government significant influence over the composition of the DPA. Members of the DPA are appointed and removed by a committee (which does include the Chief Justice and the Cabinet Secretary), but the technical expert candidates for the committee may only be considered from a shortlist of data protection experts maintained by the Central Government.

Pathways for Prosperity Commission
Technology & Inclusive Development
BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD

Critics from the civil society say this gives the Executive the scope to influence the ostensibly independent DPA, and creates a risk that breaches are not investigated by the regulators.

Lessons

The government is planning further rounds of inter-ministerial consultations on these controversial issues before the draft bill passes into law. Although the draft PDP bill is not universally accepted, it is important to recognize that achieving a perfect balance of all the differing perspectives might not be possible. And whilst global consensus on analysis and solutions to data protection around is still emerging, there are several lessons other governments might learn from India's experience.

There are four main takeaways for the countries looking to implement a national data protection legislation to regulate the use of personal data. Firstly, the principles and procedures in the GDPR provide a strong basis for data protection laws (if they align with a country's goals), but they certainly don't provide all the answers. Governments must draft data protection laws that offer bespoke solutions to countries' specific data privacy and protection needs. Secondly, treating personal data as an asset to use as a tradable commodity should be avoided as it can create perverse incentives for public offices and complicate the process of drafting the legislation. Thirdly, the government must ensure that public awareness on data privacy and protection is high – which still isn't fully the case in India – to achieve public consensus and push for a strong national data protection law. Finally, governments need to recognize that while data localisation may seem attractive from a security point of view, it comes with other economic risks and can potentially lead to trade wars.

This case benefitted from inputs from a source close to the draft PDP Bill. The interviewee is a lawyer and a technology policy researcher based out of New Delhi, India, specialising in digital privacy, net neutrality, intermediary liability and open access to knowledge and the Internet.

Endnotes

1. McKinsey Global Institute (2019). *Digital India: Technology to transform a connected nation*, McKinsey.

2. MeitY (2019). [online] Ministry of Electronics and Information Technology's UIDAI database. Available at: https://uidai.gov.in/16-english-uk/aapka-aadhaar/994-state-wise-aadhaar-enrolment-ranking.html [Accessed 06 Sep 2019].

3. Privacy International (2018) *Initial Analysis of Indian Supreme Court Decision on Aadhaar.* [online] Privacy International. Available at: https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar [Accessed 06 Sep 2019].

4. EY (2018). *Personal Data Protection Bill-2018: An initiative to enforce privacy principles in India*, Ernst & Young.

5. PRS (2018), *Draft Personal Data Protection Bill*, [online] PRS Legislative Research. Available at: http://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018 [Accessed 06 Sep 2019]

6. Bird, R (2018). *India releases draft Personal Data Protection Bill* [online] Freshfields Bruckhaus Deringer LLP. Available at: https://www.lexology.com/library/detail.aspx?g=6828b80d-bd20-40a0-a25d-123c4b53d5ce [Accessed 06 Sep 2019].

7. Desai, R. (2019). *India's Data Localization Remains A Key Challenge For Foreign Companies.* [online] Forbes. Available at: https://www.forbes.com/sites/ronakdesai/2019/04/30/indias-data-localization-remains-a-key-challenge-for-foreign-companies/#5e44356ee0a3 [Accessed 06 Sep 2019].

8. MeitY (2018), "Draft Personal Data Protection Bill 2018," [online] Ministry of Electronics and Information Technology, Government of India. Available at: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf [Accessed 06 Sep 2019].

9. Mishra, S. (2019)."*Privacy Breach? Transport Ministry Selling Driving License, Vehicle Registration Data To Commercial Firms*." [online] The Outlook. Available at: https://www.outlookindia.com/website/story/india-news-legal-or-not-why-has-the-roads-ministry-sold-our-data/334278 [Accessed 26 Sep 2019].