23 Sep 2020

Safeguarding digitised India: everything you need to know about the Personal Data Protection Bill

The Indian government has banned more than 200 Chinese apps amid rising concerns over data privacy. In terms of legislation, it has also proposed the Indian Data Protection Bill 2019, which draws heavily on the EU General Data Protection Regulation (GDPR), albeit with some notable divergence. In this guest analysis, **Cyril Abrol**, partner at Remfry & Sagar, provides insight into the debate over privacy and data in India, the country's position in comparison with international efforts and what brands need to know about the ever-shifting environment.

Guest analysis

With more than half a billion internet subscribers, India is one of the largest and fastest-growing markets for digital consumers. The path to digitisation has involved a synergy between private entrepreneurs bringing the latest technological tools and e-commerce solutions to the market and the government, whose 'Digital India' campaign has facilitated 'digital' ways of transacting business. Prominent examples of the latter include the launch of the world's largest biometric system towards issuing unique identification numbers named as 'Aadhaar' to all residents of India, boosting e-governance and creating platforms for e-payment systems, as well as the implementation of a single goods and sales tax for the entire country.

The benefit of online platforms came into sharp focus once again in the wake of the covid-19 lockdown in India, with the e-commerce sector posting rising volumes even in the midst of an overall economic slowdown. Another segment that has witnessed soaring popularity during this time is that of social networking apps – scores of new users have come online to create networks and share content. The importance of going digital has never been clearer. However, when data belonging to more than 1.3 billion Indian citizens is stored online, concerns also arise over data security and safeguards for individual privacy.

Exactly these issues have led to the recent ban of several popular Chinese apps including TikTok, WeChat and PUBG Mobile in India. Many of these apps have also met with data privacy and security concerns in other jurisdictions including the United States, and this provides an opportune moment to analyse how data protection is managed in India and how it compares with international trends.

How a new Personal Data Protection Bill came to be proposed

The Supreme Court of India declared the right to privacy as a fundamental right in its 2017 *Puttaswamy* judgment. This decision arose from a constitutional challenge to the 'Aadhar' scheme (mentioned above) regarding concerns surrounding the collection of sensitive biometric data, the mechanisms of disclosure to third (public and private) parties and the compulsory linking of 'Aadhaar' for governmental benefits delivery. Issues of digital privacy received detailed attention and the ruling set the ball rolling for the formulation of a data protection legislation for the country.

A committee was appointed to propose a framework and its report, while emphasising the responsibilities of the state towards protecting citizen interests, also underscored another point made in the aforesaid judgment – that of the proportionate benefit or risk when balancing interests of privacy with other concerns (eg, trade and national security).

Thereafter, the **Personal Data Protection Bill** was introduced in Indian Parliament in December 2019, which sets rules for how personal data should be processed and stored, and lists people's rights with respect to their personal information. The creation of an independent regulatory authority, the Data Protection Authority, to carry out this law was also proposed. Further, the bill sets out grounds for exemption which have invited criticism. Currently, the bill is being analysed by a joint parliamentary committee and amendments are likely before the text of the new statute is finalised by the legislature.

Mobile apps at the centre of controversy

In the absence of a specific data protection law, the recent ban imposed by the Indian government on 224 Chinese apps is rooted in Section 69A of the Information Technology Act 2000, read with relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009. These provisions confer power on the government to issue directions for blocking public access to information through any computer resource to prevent activities prejudicial to the sovereignty, integrity and defence of India, security of the state and public order.

Such steps were taken based on complaints of misuse of mobile apps available on Android and iOS platforms with respect to stealing and surreptitiously transmitting user data in an unauthorised manner to servers located outside India. The government claimed that the compilation of such data, its mining and profiling by elements hostile to national security and the defence of India infringed upon the sovereignty and integrity of the country and required emergency measures.

In a parallel development, the Clean Network programme – a comprehensive effort to address long-term threats to data privacy, security and human rights posed to the 'free world' from 'authoritarian malign actors' was introduced in the United States in August. Rooted in internationally accepted digital trust standards, it is a path to an open, interoperable and secure global Internet based on shared democratic values and respect for human rights. The initiative includes removing untrusted Chinese apps such as TikTok and WeChat from US app marketplaces. US authorities claim that TikTok and WeChat capture vast swathes of data and private information from users which they are compelled to share with the Chinese government upon request. The network's five-pronged approach aims at reducing Chinese access to US data and includes programmes such as:

- Clean Carrier – to keep out untrusted Chinese telecommunication companies connecting US and foreign destinations;
- Clean Store – to remove untrusted Chinese apps from US app stores;
- Clean Apps – to prevent Chinese companies such as Huawei from pre-installing or making available for download trusted US apps on Chinese-made devices;
- Clean Cloud – to prevent Chinese cloud service providers from accessing sensitive personal information and proprietary data of businesses in the United States, including information relating to covid-19 vaccine research; and
- Clean Cable – to ensure that the Chinese government cannot subvert information carried through undersea cables.

At the time of writing, TikTok was in talks with Oracle to become its 'trusted technology provider' in the United States. Reportedly, the proposed deal, details of which have not been made publicly available, was expected to meet the needs of TikTok users, as well as satisfy US national security concerns.

One may place the ban on Chinese apps, in both India and the United States, in the wider context of resetting trade and diplomacy dynamics. From a pure data protection perspective, a long-term solution to address the misuse (or threat of misuse) of data may lie not in curtailing access to data within a particular geography via piecemeal bans, but rather in directing efforts towards creating a strong framework for the secure storage and transfer of data.

The GDPR and how India's bill differs

In July 2020 the Court of Justice of the European Union (CJEU) rendered its decision in the landmark case of *Data Protection Commissioner v Facebook Ireland*, commonly known as the *Schrems II* case. The background to this case is that the EU GDPR restricts transfer of personal data to third countries outside the European Union unless the transfer satisfies certain conditions, such as the transfer being to a country with data protection laws that the European Union deems to be adequate or transfers carried out under appropriate safeguards like the EU-approved standard data protection clauses (SCCs).

In *Schrems II*, which was filed against Facebook, Ireland challenged the use of SCCs and the EU-US Privacy Shield as a mechanism by Facebook to transfer personal data to Facebook Inc in the United States. The Irish High Court asked the CJEU to consider the validity of the SCCs as well as the EU-US Privacy Shield.

In its decision, the CJEU confirmed that, while SCCs might provide adequate data protection, the EU-US Privacy Shield did not and thus invalidated it. Consequently, personal data transfers on the basis of the EU-US Privacy Shield were held to be illegal. The CJEU declared that personal data may be transferred to the United States and other jurisdictions relying on the safeguards enshrined in the SCCs, provided that this is assessed on a case-by-case basis.

This would ensure that the recipient of the data is able to comply with the SCCs in a practical manner, particularly with regard to obligations under the laws applicable in the recipient's jurisdiction. If the recipient's domestic law conflicted with the obligations of the SCCs, the SCCs would be an invalid mechanism for transfer of data to such country. As is evident, the decision has a wider impact than purely in relation to transfers to the United States.

This decision came in the background of surveillance activity undertaken by US intelligence agencies that did not provide adequate protection to personal data transferred from the European Union to the United States. The US laws in question included provisions that permit surveillance of individuals located outside the United States, who are not US citizens, in order to gather foreign intelligence. According to the CJEU, such use of personal data by the US government in surveillance programmes was not proportionate since it was not limited to what was strictly necessary. The means to redress an objection against the US authorities was deemed insufficient and the ombudsperson mechanism provided in the EU-US Privacy Shield was also found to be lacking. Hence, the privacy shield framework was invalidated by the CJEU on the ground that EU personal data might be at risk of unauthorised access and processing by the US government in a manner incompatible with privacy rights guaranteed in European Union.

The Indian Data Protection Bill 2019 draws heavily from the EU GDPR and mirrors various concepts of data protection. Businesses must tell users about their data collection practices, seek consent explicitly and provide users the option of withdrawing consent. Consumers would also have the right to access, correct and erase their data, as well transfer their data, including any inferences made by businesses based on such data, to other businesses. Privacy would also become a key consideration in how entities are organised so as to ensure adequate data protection.

However, in a departure from GDPR standards, the Indian government retains power to exempt any government agency from requirements of the Data Protection Bill on grounds related to national security, national sovereignty and public order. While the GDPR offers EU member states similar escape clauses, they are tightly regulated by other EU directives – safeguards currently lacking in the Indian bill.

Additionally, unlike the GDPR, the Indian bill allows the government to direct an entity to share all non-personal data with the government. The stated objective behind this provision is the improvement of delivery of government services. But questions arise on how this non-personal data will be used, whether it will be shared with other private businesses, and whether any compensation will be paid for the use of this data. These are primary reasons why the bill has not received legislative sanction to date and is pending before a joint parliamentary committee for review.

The road ahead

Significantly, India's proposed data protection legislation also stipulates that all 'sensitive personal data' must be stored in India and that 'critical personal data' must not be transferred out of India. This will undoubtedly impact market-driven decisions of businesses to access the best data storage services.

Also, in conjunction with the two exemption provisions discussed above, this aspect will impact India's desire to be included in the list of countries which the European Union deems as having adequate data protection laws. Moreover, post-*Schrems II*, SCCs, which form the basis of data transfers at present, that conflict with Indian domestic law would also hinder data transfer.

Given the emergent primacy of data protection across jurisdictions, it will be interesting to see how the Indian government balances national prerogatives with international demands for a robust data privacy law in the days ahead.

Cyril Abrol

Partner | Remfry & Sagar
cyril.abrol@remfry.com

TAGS

Government/Policy, Online, Internet and Online, Technology, Asia-Pacific, India