

Bit by byte protecting her privacy

The Srikrishna committee draft law on data protection is days away. Here's a bucket list of issues that will matter

Last Published: Thu, Jul 26 2018. 10 10 PM IST

✉ Mihir Dalal | ✉ Anirban Sen



India doesn't have a comprehensive, up-to-date privacy law.

Bengaluru: In an era dominated by “free” platforms such as Google, Facebook and Amazon, among others, data privacy had largely been considered an academic matter. However, in the past one year that notion has changed forever, bringing data privacy to the fore, as one of the defining issues of the internet, both in India and abroad.

Last August, the Supreme Court ruled that privacy was a fundamental right under the Constitution of India. Concomitantly, the debate over Aadhaar and its potential misuse picked up steam on the back of reports about data breaches in the biometric ID system though these reports were denied by the Unique Identification Authority of India, which built Aadhaar. (The apex Court will deliver its verdict on petitions that have challenged the constitutional validity of Aadhaar and its legal framework)

Globally, Facebook came under severe criticism after it was revealed that the social media giant had compromised user data in the run up to the US elections. Finally, in May, Europe introduced its landmark data privacy law, General Data Protection Regulation (GDPR), which has put users in control of their data through various measures.

The stage is now set for the much-delayed draft law on data protection, which is expected to be submitted soon by the 10-member panel headed by former Supreme Court justice B.N. Srikrishna.

The committee, which had been set up last July, has attracted criticism from some quarters. Earlier this month, more than 150 lawyers, activists and journalists, among others, wrote to the Srikrishna committee, complaining about the lack of transparency in its process, the lack of diversity in the views held by members of the committee, besides other issues. In an earlier letter in November last, activists, lawyers and others had alleged that too many members of the committee held pro-Aadhaar views. Some experts believe that the mandate of the committee was flawed to begin with. “Given that personal information is omnipresent in so many different sectors, it is better to have a light touch legislation that deals mostly with key principles of data privacy and empowers a data commissioner to frame more detailed regulations,” said Stephen Mathias, partner, Kochhar and Co.

Last week, the Telecom Regulatory Authority of India (Trai) released a set of recommendations on data privacy that favour giving users control of their data and personal information, while severely restricting the ways in which telecom and internet companies can use customer data. Here are the major issues to watch out for in the draft data protection law.

Users vs. collectors

This broad umbrella includes mandatory consent of users for data collection, data portability, the right to be forgotten and the right to erasure. Last week, Trai gave its recommendations on some of these issues in what were considered pro-privacy and progressive suggestions. Those recommendations tracked GDPR measures. The Srikrishna committee is also expected to suggest pro-privacy measures, though the details will be all-important. The committee is also expected to define what is ‘sensitive’ or ‘critical’ data. “In India, government agencies, private entities and others collect various forms of data on individuals,” said Chetan Nagendra, partner, AZB Partners. “The committee will have to clarify what category of data is allowed to be collected and whether this should be standardized across different entities. It will also have to standardize rules on how long is it okay to store such user-collected data.”

The flip side of user rights is the role of data repositories that collect and process user data. The committee will be required to clarify what data firms and government

agencies can gather on users and what will be their responsibilities toward the usage of that data. This includes the principle of privacy by design, that is, companies must ensure by default that their platforms are designed to protect rather than exploit user data and privacy.

IndusLaw partner Namita Viswanath said that in terms of data repositories, there was a need to distinguish between a data controller and a data processor. A data controller is the user-facing platform that gathers data, whereas a data processor is often a third-party firm that provides infrastructure for the platform. “Responsibilities of user personal data should be shared between a data controller and processor. The nature and extent of liability should depend on the nature of data, the party responsible for handling data and the measures adopted, but ultimately, the data controller should most responsibility,” Viswanath said.

Regulation vs. Self-control

Given that data is such a broad-ranging topic, the Srikrishna committee will be expected to recommend who should have oversight of data-related matters. Will there be a new data protection authority? If so, what will be its scope, given that regulators, such as the RBI, Sebi and Trai, will all be affected by a privacy framework in their respective areas? And what will be the punitive measures and fines for offenders on data matters?

Some experts said the government should appoint a data protection authority. As the recent travails at Facebook show, relying solely on self-regulation of internet platforms, is a disastrous policy. But it’s unlikely that the entire burden of regulation will fall on one authority.

“Logistical problems are likely, especially in the early days, with having a top-down regulatory approach,” said Kriti Trehan, partner, Panag and Babu. “The process of training, requirement of funding and access to skilled human resources will necessitate organisational and administrative inputs. With this in mind, I believe that a co-regulatory framework for data protection will be efficient. With this approach, established parameters may guide escalation in specific instances.”

Data localisation

In April, the RBI had issued norms on the storage of payments system data, which requires digital payment providers to store data in India. That has sparked another debate over the possible stance of the Srikrishna committee. Many start-ups and firms use data servers located in overseas locations because of several reasons, including economies of scale and tax planning. “Data protection should not be confused with data access,” said Kartik Maheshwari, leader, Nishith Desai Associates. “For instance, if a firm is storing user data abroad, that should be fine as long as it is secure and

access in India is provided, whenever required. Storing data locally is not necessarily the best solution from the perspective of data security as better infrastructure may be available abroad. However, the government may, in exceptional cases of sensitivity, legitimately require local storage of very narrowly defined streams of data.”

Surveillance is key

The law will also need to clearly define the contours of the contentious issue of surveillance and how to ensure that India does not end up replicating the policies in place in countries such as China, which are notorious for mass surveillance practices. Surveillance that has been legally sanctioned is part of the exceptions to regular privacy practices. The committee will have to define the parameters of these exceptions. In the case of surveillance, some experts, including Amber Sinha of Centre for Internet and Society, said that while it needs to be allowed in specific instances such as issues related to national security, a judicial system needs to be in place to protect the rights of the parties that are being put under surveillance. This, in many ways, is the heart of a very important matter.

The Aadhaar factor

The most hot-button of all issues for the committee is, of course, Aadhaar. Former UIDAI chairman Nandan Nilekani told *Mint* this week that “if something needs to be modified in the Aadhaar law, it will be done” by the Srikrishna committee. The changes that the committee will suggest to the Aadhaar law will go a long way in determining whether its draft law is truly pro-privacy.

First Published: Thu, Jul 26 2018. 10 09 PM IST