Hindu Business Line
Imagining India\'s new data privacy law
Date: 17/08/2017 | Edition: Mumbai | Page: 8 | Source: SUPRATIM CHAKRABORTY SOUMYADRI CHATTOPADHYAYA | Cli
Clip: 1 of 1

Imagining India's new data privacy law

India is uniquely positioned to create a law that balances the right to privacy with harnessing the advantages of technology

SUPRATIM CHAKRABORTY
SOUMYADRI CHATTOPADHYAYA

"India has a unique opportunity to draft a very modern data protection and privacy Bill which can be superior to what is happening elsewhere in the world." — Nandan Nilekani

Data is the lifeblood of today's digital economy and is driving new businesses that challenge conventional wisdom about markets. With the proliferation of smartphones, every tap creates a digital footprint: valuable information that can be exploited by companies to generate everything, from customer preferences to consumption patterns.

Critically, the traditional notion of data being merely sensitive personal information is now being challenged as companies are also exploiting real-time data generated from daily activities such as one's route preference whilst booking cab rides using an app. Even the Government's drive to digitise India on the back of initiatives such as JAM (Jan Dhan-Aadhaar-Mobile) and the increased focus on digital payments is fuelled by data. As dependence on data continues to grow, so does the vulnerability of data subjects. Hence, any debate on data privacy must recognise the need for a comprehensive data privacy law, which not only contributes to and complements the constitutional right to privacy but also enables data subjects to harness the benevolence of technological advances.

Recent concern

India's existing data privacy framework dates only to the year 2009, introduced to address growing concern relating to 'data protection' and 'data privacy'. This framework was primarily introduced through Sections 43-A and 72-A of the Information Technology Act 2000. Subsequently, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 were issued. These regulate the collection, disclosure, transfer and storage of sensitive personal data and information.

Unfortunately, the above-mentioned legislative framework does not extend to government agencies, and also stops short of imposing an obligation upon the data collector to mandatorily report any data compromises to data subjects. Further, it imposes a stiff requirement to establish intent to cause wrongful gain or loss before an enforceable remedy against a data breach would be available to data subjects.

Setting the rules

A well-functioning data privacy regime should ideally set the rules of the game for all actors, cut out any regulatory uncertainty and strike a balance between protecting the right of privacy of data subjects with the business needs of data collectors.

In 2012, the AP Shah report studied global best practices with a view to rebooting the existing domestic framework; it identified transparency, consent, and accountability as the fundamental building blocks of the ideal data protection regime. The report also observed that any new data privacy framework must aim to harmonise principles such as the principle of notice, choice and consent, limitation on collection and purpose, disclosure, openness, security, and accountability. These would also be relevant today.

Key factor A chance to make privacy laws tough and up-to-date SDECORET/SHUTTERSTOCK.COM

Moreover, with technology constantly evolving, an approach based on standards would enable the law to keep pace with rapid changes in technology, as against objective rules that would fail to be relevant with constant technological developments.

Perhaps the biggest shift required from the existing regime is with respect to its applicability. It is imperative to bring government agencies within the ambit of the new framework. Although drafting a legislation that is applicable to both the private sector and the Government alike is a daunting task, it may be a streamlined method of ensuring that data subjects are adequately safeguarded.

Scan & share
https://goo.gl/78WUrF

Debatable

While 'consent' is the cornerstone of any data privacy regime, the adequacy of such consent from the data subjects is sometimes debatable, especially in the context of standard-form contracts such as click wrap agreements. Recent studies show that this problem has been exacerbated manifold; people are often forced to accept unfavourable terms of service since most apps are designed to quit immediately if one does not click on the 'I agree' button.

Behavioural research also points to the inability of data subjects to manage their own data. This is attributed to a combination of lack of understanding and general disinclination.

To counter this, researchers have argued that perhaps regulating only the collection of data may not be enough, its use by data collectors and data processors could also be regulated such that there is a prohibition on using certain data in a manner that is detrimental to data subjects. This could be a useful supplement to temper the current prior consent-based approach where data subjects often surrender their data without truly understanding the wider ramifications of exploitation of such data.

Several stops and starts and multiple draft privacy Bills later, the Government has now taken the step to constitute a committee under Justice (Retd) BN Srikrishna to suggest and draft a new data protection Bill. While the Supreme Court continues to deliberate whether the right to privacy should be elevated to a separate fundamental right, a robust and well-functioning data privacy legislation will go a long way in complementing the constitutional right to privacy in not only creating the right incentives for all stakeholders but also providing an efficient redress mechanism for data subjects.

Chakraborty is associate partner and Chattopadhyaya senior associate at Khaitan & Co