

# Untangle The Privacy Law

**BW** [www.businessworld.in/article/untangle-the-privacy-law-157103](http://www.businessworld.in/article/untangle-the-privacy-law-157103)

[Smitha Krishna Prasad](#) Aug 08, 2018



Over the last week of July, the right to privacy and data protection has once again made headlines in India. On 29 July, reports stated that the proprietors of three small IT companies were arrested in connection with the leak of personal information of over 8 lakh students.

A day before that, on 28 July, the chairman of the Telecom Regulatory Authority of India (TRAI), published his Aadhaar number, challenging security researchers to show what harm could be done to him using this number. There has been much debate on the Aadhaar project and its impact on privacy over the past few years. This “challenge” was apparently issued to show that “Aadhaar does not contribute to increasing any of your other digital vulnerabilities”.

Researchers were able to find several pieces of personal information about the TRAI chairman, while pointing out that availability of such information may not harm him, but could be harmful to others.

On 27 July, the long-awaited draft data protection bill and an accompanying report were submitted to the Ministry of Electronics and Information Technology (MEITY) by a committee of experts.

The incidences of data leaks, and the “challenge” issued by a senior member of government go to show the state of disarray that we see in the general discourse on the value of technology and data. On the other hand, the data protection bill brought with it hope that we could soon be in the leagues of countries that actively work towards protecting the privacy of their people – an important objective at a time when the constant emphasis for rapid ‘innovation’ seems to disregard the need to plan for the long term protection of individuals and their rights.

## **Right to privacy and data protection**

The disparity seen above is reflected in the state of legal protections currently afforded to privacy and data protection in India.

The most comprehensive data protection rules we have currently fall under the Information Technology Act, 2000. The rules, applicable since 2011, are, in many instances, inconsistent, and are difficult to enforce. In addition, we also have specific provisions applicable to certain sectors, for instance, the financial sector and the telecom sectors.

In August 2017, the Supreme Court affirmed that the right to privacy is a fundamental right in its judgement in the Puttaswamy case. The Court rejected the Indian government's argument that privacy is not a fundamental right. It also recommended that the government put into place a statutory framework to protect this right as it relates to personal information.

## **Committee of experts**

In the meantime, MEITY set up a committee of experts chaired by former Supreme Court Judge B.N. Srikrishna. The committee was asked to recommend principles to be considered for data protection in India and suggest a draft data protection bill.

In the wake of criticism regarding the Constitution, as well as lack of transparency on the functioning of the committee, a white paper with the committee's provisional views was published in late November 2017. Public comments were called for, and consultations were held to discuss issues raised in the white paper in January 2018. The committee has not provided any information regarding the number or nature of comments received.

With privacy issues such as the Facebook-Cambridge Analytica scandal dominating the news cycle over the past few months, the committee's reports have been waited on with much anticipation.

## **The personal data protection Bill, 2018**

The bill as recommended by the committee, is applicable to the collection and processing of personal data by the State and the private sector.

It adopts an approach similar in structure to the European Union's General Data Protection Regulation (GDPR). The GDPR, which came into effect May, found its final form after several years of debate, and is largely considered to be one of the most comprehensive data protection laws in effect today.

Several countries have adopted laws that take guidance from the GDPR, and it is fast becoming the standard for data protection laws across the world.

In this context, the structure of the bill is a welcome move, since it aims to use high benchmarks to protect the data of individuals in India, while also adopting international standards that most data processors who work across borders are subject to.

The bill protects a wide range of information that can be used to identify individuals, calling for a higher standard of protection where information is sensitive, and can be potentially used to cause greater harm. Individuals must be notified of the collection and processing of their personal data, in detail, and consent must be obtained for the processing of data for specific purposes. Individuals have the right to withdraw their consent, access and correct / update personal data held by processors. The bill also proposes transparency, and accountability measures to be adopted by data processors.

However, while the bill ostensibly enables individuals to exercise their right to privacy against the State and the private sector, there are several concerns in this regard.

It grants broad exceptions to the State, in some cases in the context of specific obligations such as the requirement for individuals' consent. In other cases, State action is almost entirely exempted from obligations under the law. In the context of the private sector, while the obligations in relation to data processing have been articulated in detail, several provisions allow for the possibility of making compliance with these obligations difficult to assess or enforce.

### **Sectoral regulators and data protection**

The Justice Srikrishna Committee's work with MEITY is one of several government processes that are now addressing issues relevant to personal data, among other things.

Some of the other important processes are the TRAI's recommendations on privacy, security and ownership of data in the telecom sector, and the Ministry of Health & Family welfare's draft Digital Information Security in Healthcare Act (DISHA). The RBI's recent rules mandating data localisation are relevant. Reports also suggest that the upcoming national e-commerce policy framework will follow in this direction.

The TRAI's recommendations touch upon a wide range of data protection issues, as relevant to the telecom sector. Interestingly, the TRAI has chosen to address telecom service providers and all actors in the digital ecosystem for instance, providers of devices, browsers, operating systems, and over the top services. Many of these service providers are outside the reach of the TRAI, or even the Department of Telecommunication's powers.

DISHA aims to regulate the processes related to digital health data, and 'reliability, data privacy, confidentiality and security of digital health data'. This is to be done by the national and state e-health authorities to be set up under this act.

The TRAI recommendations and DISHA touch upon a wide range of data protection issues, while providing little detail on actual compliance.

It is not clear whether the Justice Srikrishna committee has taken these processes into account – there is no mention of the TRAI recommendations in the report. DISHA, is only once referred to as an example of a sector specific law that imposes a higher standard – without any analysis regarding the difference in the two laws. There does not seem to be

any mention of the RBI's data localisation directive either. However, many of the issues touched upon in these frameworks are reflected in the committee's report, some such as data localisation by their controversial presence, and others such as the idea of ownership of personal data, by intentional absence.

In the days following the its submission, it has become apparent that although the direction that the bill takes in terms of protection of personal data is deserving of some praise, there is much work to be done. Several issues – ranging from typographical errors, and inconsistencies in drafting, to conceptual problems affecting constitutionally guaranteed fundamental rights – need to be addressed.

At the press conference held during the submission of the report and bill, the IT Minister has stated that extensive consultations will be held. It is important that these consultations be as inclusive as possible. While many issues have been raised by different stakeholders, finding the right solutions will require collaboration.

The final form that this bill takes could very well define the way we, as individuals, interact with companies and government agencies, across the board. It is important for each of us, that we get this right.



---

## Also Read

---



[Vodafone Idea Shares In Focus As SC Set To Rule On Rs 9,450 Cr AGR Dues Plea Today](#)

---

2 min(s) read



[Canara Robeco AMC Sets IPO Price Band At Rs 253-Rs 266; Issue To Open On 9 Oct](#)

---

2 min(s) read



[Next Week's IPO Bonanza: Tata Capital, LG Electronics India Open For Subscription](#)

---

2 min(s) read



**HINDUSTAN ZINC**

**Zinc & Silver of India**

[Hindustan Zinc Q2: Mixed Operational Show, Profit Beats Estimates But Dips 4.7%](#)

## YoY

---

1 min(s) read



### [Tata Steel Gets Rs 2,411 Cr Demand Notice Over Sukinda Chrome Ore Dispatch Shortfall](#)

---

1 min(s) read



### [Kotak Mahindra Bank Reports 14% Growth In Deposits, Advances In Q2](#)

---

2 min(s) read