Government invites public comments on Srikrishna data protection bill

The IT Ministry has invited comments on the Srikrishna committee's data protection bill. Comments can be posted here. till the 5th of September 2018, that is 20 days from now. This further consultation takes special significance due to the contentious nature of the draft bill — there were voices of dissent from within the committee that found place on its official report. The data protection bill's provisions on maintaining a copy of personal data in India and its stiff criminal penalties for breaches have also drawn criticism.

Read: All roads of data sovereignty lead to a dystopia

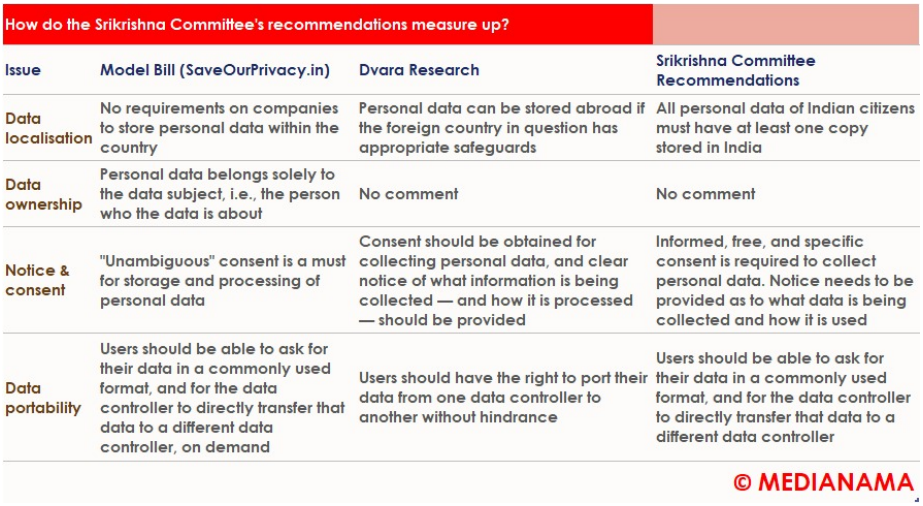
It's unclear if the comments to the draft bill collected by MeitY will be made public. Public comments solicited by the Srikrishna Committee prior to the bill's drafting stage were not made public. In fact, MeitY declined multiple RTI requests to publish stakeholder comments. It's also unclear if MeitY will hold a counter-comment stage of consultation, where stakeholders will be able to comment on each other's responses. This two-stage process is typical of TRAI consultations, where comments are made public and commented on in a counter-comment stage as a matter of process.

How the bill measures up

While comments to the Srikrishna Committee were not published, some organisations made their filings public voluntarily. Here's a comparison of the Srikrishna Committee's bill with the expectations of i) Dvara Research, which prepared a skeletal draft bill of its own, and ii) SaveOurPrivacy.in, a volunteers' collective spearheaded by the Internet Freedom Foundation (*Note: MediaNama editor and publisher Nikhil Pahwa is IFF co-founder and chairman*).

Ownership, consent, portability and localisation

Localisation is probably the most glaring departure from both business' and civil society's expectations. The committee's bill requires all entities to store a copy of an individual's personal data in India, which will have huge associated costs. Data ownership is not asserted as the sole domain of the data subject, which somewhat weakens the foundations of a data protection bill. Consent requirements are still stringent, though, with multiple requirements needed to be satisfied for the consent to be regarded as explicit. Portability is required as it is in the SaveOurPrivacy.in privacy code.

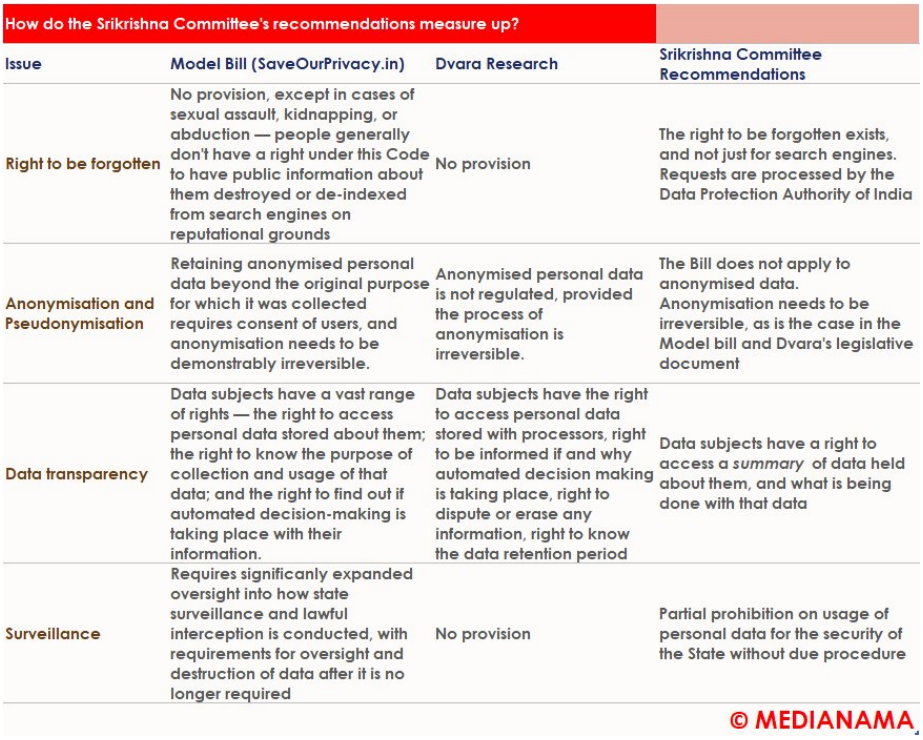


How do the Srikrishna Committee's recommendations measure up?

Issue	Model Bill (SaveOurPrivacy.in)	Dvara Research	Srikrishna Committee Recommendations
Data localisation	No requirements on companies to store personal data within the country	Personal data can be stored abroad if the foreign country in question has appropriate safeguards	All personal data of Indian citizens must have at least one copy stored in India
Data ownership	Personal data belongs solely to the data subject, i.e., the person who the data is about	No comment	No comment
Notice & consent	"Unambiguous" consent is a must for storage and processing of personal data	Consent should be obtained for collecting personal data, and clear notice of what information is being collected — and how it is processed — should be provided	Informed, free, and specific consent is required to collect personal data. Notice needs to be provided as to what data is being collected and how it is used
Data portability	Users should be able to ask for their data in a commonly used format, and for the data controller to directly transfer that data to a different data controller, on demand	Users should have the right to port their data from one data controller to another without hindrance	Users should be able to ask for their data in a commonly used format, and for the data controller to directly transfer that data to a different data controller

Right to be forgotten, transparency, and surveillance

The Srikrishna Committee's bill includes a right to be forgotten. The Adjudicating Officer, who is appointed under the data protection authority of India, will process applications based on sensitivity and necessity, among other factors. Anonymised data is not regulated by the bill, provided that the anonymisation is irreversible (the word anonymisation is itself defined as irreversible in all the bills). While the civil society bills allow users to access a copy of their information, the Srikrishna Bill only allows for a *summary* of that information to be accessed. On surveillance, the bill partially prohibits use of personal data for "security of the State" but doesn't go as far as SaveOurPrivacy hoped it would in mandating oversight.

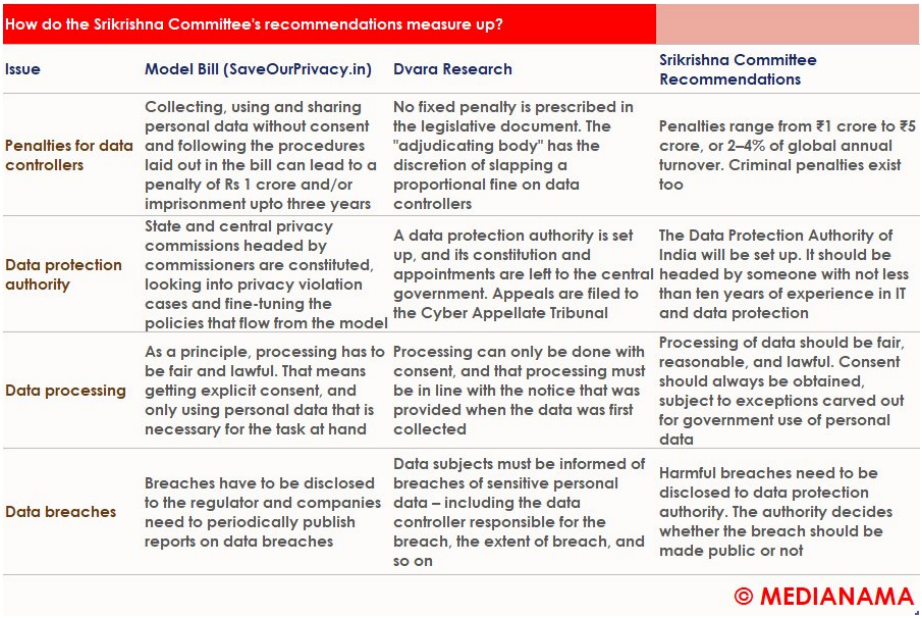


How do the Srikrishna Committee's recommendations measure up?

Issue	Model Bill (SaveOurPrivacy.in)	Dvara Research	Srikrishna Committee Recommendations
Right to be forgotten	No provision, except in cases of sexual assault, kidnapping, or abduction — people generally don't have a right under this Code to have public information about them destroyed or de-indexed from search engines on reputational grounds	No provision	The right to be forgotten exists, and not just for search engines. Requests are processed by the Data Protection Authority of India
Anonymisation and Pseudonymisation	Retaining anonymised personal data beyond the original purpose for which it was collected requires consent of users, and anonymisation needs to be demonstrably irreversible.	Anonymised personal data is not regulated, provided the process of anonymisation is irreversible.	The Bill does not apply to anonymised data. Anonymisation needs to be irreversible, as is the case in the Model bill and Dvara's legislative document
Data transparency	Data subjects have a vast range of rights — the right to access personal data stored about them; the right to know the purpose of collection and usage of that data; and the right to find out if automated decision-making is taking place with their information.	Data subjects have the right to access personal data stored with processors, right to be informed if and why automated decision making is taking place, right to dispute or erase any information, right to know the data retention period	Data subjects have a right to access a *summary* of data held about them, and what is being done with that data
Surveillance	Requires significanly expanded oversight into how state surveillance and lawful interception is conducted, with requirements for oversight and destruction of data after it is no longer required	No provision	Partial prohibition on usage of personal data for the security of the State without due procedure

Penalties, data protection authority, and breaches

The bill goes farther than civil society expectations here by not only having stiff civil penalties, but also *criminal* penalties that could involve jail time. The bill sets up a data protection authority, but only one — individual states don't get an authority of their own as the SaveOurPrivacy code hoped. Processing requirements are consistent with civil society attempts, but there exist carve-outs with fewer consent standards in the committee's bill. Importantly, breaches don't have to be disclosed to the public — only to the data protection authority.



How do the Srikrishna Committee's recommendations measure up?

Issue	Model Bill (SaveOurPrivacy.in)	Dvara Research	Srikrishna Committee Recommendations
Penalties for data controllers	Collecting, using and sharing personal data without consent and following the procedures laid out in the bill can lead to a penalty of Rs 1 crore and/or imprisonment upto three years	No fixed penalty is prescribed in the legislative document. The "adjudicating body" has the discretion of slapping a proportional fine on data controllers	Penalties range from ₹1 crore to ₹5 crore, or 2–4% of global annual turnover. Criminal penalties exist too
Data protection authority	State and central privacy commissions headed by commissioners are constituted, looking into privacy violation cases and fine-tuning the policies that flow from the model	A data protection authority is set up, and its constitution and appointments are left to the central government. Appeals are filed to the Cyber Appellate Tribunal	The Data Protection Authority of India will be set up. It should be headed by someone with not less than ten years of experience in IT and data protection
Data processing	As a principle, processing has to be fair and lawful. That means getting explicit consent, and only using personal data that is necessary for the task at hand	Processing can only be done with consent, and that processing must be in line with the notice that was provided when the data was first collected	Processing of data should be fair, reasonable, and lawful. Consent should always be obtained, subject to exceptions carved out for government use of personal data
Data breaches	Breaches have to be disclosed to the regulator and companies need to periodically publish reports on data breaches	Data subjects must be informed of breaches of sensitive personal data – including the data controller responsible for the breach, the extent of breach, and so on	Harmful breaches need to be disclosed to data protection authority. The authority decides whether the breach should be made public or not

Please note: MediaNama is also hosting discussions on the Srikrishna data protection bill in Delhi and Bangalore on August 23rd and 30th 2018 respectively. Click here to apply to attend.