On the TRAI's recommendations on Privacy

The talk of the tech policy circles in Delhi these days is about the delays in the release of the Srikrishna Committee report on Privacy: Will they release a law, or will it just be recommendations? Have the recommendations been delayed because the committee is indecisive now about data localisation, given the reaction to the RBI's seemingly "out of the blue" diktat regarding localisation of financial transaction data? Is the iSpirt/UIDAI/"Nandan-Nilekani-friendly" faction in the Srikrishna Committee digging its heels in about data localisation? Or is it that they don't want it to affect Aadhaar and Justice Srikrishna does? Is there a point to the Srikrishna Committee, since the bill may never get tabled: the opposition may not let the Monsoon session to run in Parliament, and there's very little chance of any work in the winter session?

In that context, the TRAI's recommendations are very important, especially given that the TRAI Chairman is the former CEO of the UIDAI, the fact that the TRAI took on this consultation suo moto, and there's talk of him possibly becoming head of India's first data protection authority after his term finishes at the TRAI. These recommendations are being seen as a signal for what's to come from the Srikrishna Committee.

Issues that the TRAI has avoided

Before we get into what the TRAI has recommended, I think it's worth looking at what the TRAI has avoided talking about:

- Data Localisation,
- Cross-border data flows,
- Legitimate Exceptions to privacy,
- Lawful interception,
- responsibilities of data controllers and technology-based audits.

These are all contentious topics and there, from what we've heard, is a lot of pressure from law enforcement agencies, for access to user data. This TRAI, which has been especially focused on consumer interest, has avoided stepping into some potential minefields.

Most importantly, it hasn't gone into issues of mass surveillance and its prevention, offered no conclusive comments on exceptions to the privacy law, saying that because the privacy framework is under development, "the Authority has decided not to make any recommendations."

Uhh... pretty much everything that the TRAI has covered in this paper is a part of the privacy framework under development, and this isn't a sufficient reason for the TRAI to opt out from commenting, while commenting on everything else. Somewhere in the paper, it does say that "Since the data is collected by private as well as government entities, the data protection framework should be equally applicable to both the Government as well as private entities", which is

a welcome development, given that there would have been push-back regarding this from the Home ministry.

That said, the TRAI has done a fairly decent analysis of issues pertaining to cross-border data flows and data localisation, without taking a stand on it.

TRAI Recommendations on privacy and data protection

1. Ownership of personal data:

> **Each user owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem. The entities, controlling and processing such data, are mere custodians and do not have primary rights over this data.**
>
> The TRAI says that data isn't just a property and "...it would appear illogical/ inequitable to permit complete transfer of rights over an individual's personal data. This would imply that, the personal data can no longer be used/ accessed by the data owners – a situation which is quite clearly untenable. In the circumstances, there must be a recognition that while data controllers may indeed collect and process personal data, this must be subject to various conditions and obligations – including importantly, securing explicit consent of the individual, using the personal data only for identified purposes, etc. The entity that has control over personal data would be responsible for compliance with data protection norms."

The TRAI has recommended a study to formulate standards for anonymisation and de-identification of personal data. In addition, it has said that

> All entities in the digital eco-system, which control or process the data, **should be restrained from using metadata to identify the individual users.**

How exactly does the TRAI expect all entities in the digital ecosystem to be restrained from using metadata from identifying individual users?

2. Jurisdiction of TRAI's recommendations:

> Two aspects of the TRAI's recommendations appear to go beyond its remit. It says:
>
> - Till such time a general data protection law is notified by the Government, **the existing Rules/ License conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem.** For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers, and Applications.

These recommendations, coupled with the recommendations regarding devices – of allowing users to delete pre-installed apps, and previous comments from the TRAI Chairman regarding devices being a part of the telecom ecosystem, appear to be seeking to extend the TRAI's jurisdiction beyond telecom. Remember that when this paper came out, it appeared to be more about the Internet than telecom, and we had pointed out that the TRAI does not have jurisdiction over the Internet. No doubt that these recommendations are well-meaning, but privacy isn't really a part of the TRAI's or the DoT's remit. That should be with MEITY, in the absence of a Data Protection Authority.

A positive development is the TRAI's suggestion from the TRAI:

> Since the data is collected by private as well as government entities, the data protection framework should be **equally applicable to both the Government as well as private entities.**

3. Data minimisation & Privacy by Design:

> Privacy by design principle should be made applicable to all the entities in the digital ecosystem viz, Service providers, Devices, Browsers, Operating Systems, Applications etc. The concept of "Data Minimisation" should be inherent to the Privacy by Design principle implementation. Here "Data Minimisation" denotes the concept of collection of bare minimum data which is essential for providing that particular service to the consumers.

4. Data portability and deletion

> The Right to Data Portability and Right to be Forgotten are restricted rights, and the same should be subjected to applicable restrictions due to prevalent laws in this regard.

The TRAI here appears to conflate the Right to be Forgotten, which refers to removal from search engine index with data deletion. That said, empowering users to delete telecom data, and port their data (and not just from their numbers), is a welcome move.

5. Notice and Consent

This is a big one. As we've discussed, consent is broken, and the TRAI has recommended that for telecom users,

5.a Consent mechanism on the basis of the Electronic Consent Framework from MEITY

> "In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers." Apart from that, the TRAI has recommended that a framework, "on the basis of the Electronic Consent Framework developed by MeitY and the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be

notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users."

5b: Multilingual agreements: The TRAI has recommended that agreement/terms and conditions be "Multilingual, easy to understand, unbiased, short templates" for "all the entities in the digital eco-system"

5c. No pre-ticked boxes:

Data Controllers should be prohibited from using "preticked boxes" to gain users consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.

5d. Devices and consent:

(g) Devices should disclose the terms and conditions of use in advance, before sale of the device.

(h) It should be made mandatory for the devices to incorporate provisions so that user can delete such pre-installed applications, which are not part of the basic functionality of the device, if he/she so decides.

Also, the user should be able to download the certified applications at his/ her own will and the devices should in no manner restrict such actions by the users.

6. Improvement in Encryption standards

This is one of the issues that we had raised at the open house on privacy: That data sent over telecom networks is not secure, and we need strong privacy recommendations to enable security of that data. The TRAI recommends that:

- To ensure the privacy of users, National Policy for encryption of personal data, generated and collected in the digital eco-system, should be notified by the Government at the earliest.
- For ensuring the security of the personal data and privacy of telecommunication consumers, **personal data of telecommunication consumers should be encrypted during the motion as well as during the storage in the digital ecosystem.**
- Decryption should be permitted on a need basis by authorized entities in accordance to consent of the consumer or as per requirement of the law.

This is a very welcome suggestion from the TRAI, and it's about time that this issue got addressed. That said given the mess that the last (now withdrawn) Draft Encryption Policy was, this needs to be looked at carefully.

7. Breach and notification

> All entities in the digital ecosystem including Telecom Service Providers should be encouraged to share the information relating to vulnerabilities, threats etc in the digital ecosystem/ networks to mitigate the losses and prevent recurrence of such events.
>
> All entities in the digital ecosystem including Telecom Service Providers should transparently disclose the information about the privacy breaches on their websites along with the actions taken for mitigation, and preventing such breaches in future.
>
> A common platform should be created for sharing of information relating to data security breach incidences by all entities in the digital ecosystem including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem including all such service providers to be a part of this platform.
>
> Data security breaches may take place in-spite of adoption of best practices/ necessary measures taken by the data controllers and processors. Sharing of information concerning to data security breaches should be encouraged and incentivized to prevent/ mitigate such occurrences in future.

This is a measured approach: one issue with breach notifications is that companies that get breached are afraid of harassment from law enforcement agencies. It's a tricky thing to deal with: at one level, it is important to ensure that companies try and protect user data, and hence penalties are a means of ensuring that they behave responsibly. At another level, the fear of penalties (and loss of business) prevent companies from disclosing breaches to law enforcement and customers.

All in all, these are welcome recommendations from the TRAI. Download your copy here.