TAKSHASHILA
INSTITUTION

POLICY ADVISORY
OCTOBER, 2017

Privacy, Security and Ownership of Data in the Telecom Sector

In response to comments sought by the Telecom Regulatory Authority of India

Rahul Matthan, Manasa Venkataraman and Ajay Patri[1]

Executive Summary

There is an urgent need to bring forth effective data protection norms in India. However, these norms must be introduced and regulated by the appropriate regulator. The questions posed by the Telecom Regulatory Authority of India (**TRAI**) in this Consultation Paper are pertinent, but some of them are beyond its remit. To this end, while our comments to this consultation paper span the entire subject of data protection, it is respectfully submitted that TRAI take steps to effect norms for the stakeholders falling within its jurisdiction.

Without prejudice to the above, we are of the opinion that a rights based approach to data protection is the proper way forward. The law should extend certain basic data rights to every individual, as well as prescribe certain harms. Service providers collecting data (**Data Controllers**) for the purposes of providing their services should be liable if it is proven that their actions have caused harm to individuals by violating data rights. The law should also provide that data processes be audited periodically to rectify errors in processing. This framework shifts the burden of evaluating the privacy risk to personal data away from the data subject and onto the data controller. This will also ensure that data controllers are mindful of complying with data processing standards.

Responses to TRAI's Consultation Paper on Data Privacy, Security and Ownership

At the outset, it is necessary to understand the scope of TRAI's mandate as the telecom regulator. While TRAI is fully authorised to regulate the conduct of business by telecom service providers and internet service providers, codifying data protection standards for the entire digital ecosystem is beyond TRAI's ambit. Per the Information Technology Act, 2000 (**IT Act**), several of the questions TRAI has put forth in this Consultation Paper should fall for consideration before the Ministry of Electronics and Information Technology (**MeitY**).

The object of the TRAI Act, 1997 (**TRAI Act**) is to regulate telecom service providers for better provision of telecom services. While TRAI's initiation of a discourse on this subject is healthy, it might be problematic if regulatory boundaries are blurred. Separately, it must be noted that an Expert Committee under Justice B. N. Srikrishna has already been constituted to set out the details of a data protection framework.

Nevertheless, our comments to each question are set out below:

1. **Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard?**

   No, the current standards of data protection do not adequately protect the interests of telecom subscribers. Although the Unified License contains many covenants for protecting subscriber data, it is still insufficient in comparison to the desired level of data protection.

   At the outset, the risk of profiling is not sufficiently mitigated against. From a subscriber's perspective, there is no compelling regulation stopping the service provider from constantly monitoring the subscriber's online and communications activity. While the rules framed under the Indian Telegraph Act, 1885 state that individual messages will only be intercepted by the State under compelling circumstances, there is no law restricting the circumstances in which private entities can monitor data pertaining to personal communications. This leaves the subscriber vulnerable to being monitored and even profiled by a data controller.

Secondly, service providers who collect data for providing services are not accountable for a lot of wrongs caused due to insufficient data protection regulation. As everything is hinged on consent and on the inevitably onerous terms that data controllers present to individual consumers, they are able to limit their liability to a large extent. Additionally, interoperability and increasing transfers of data only make it more difficult to attribute liability to a data controller. The regime must shift so that larger stress is laid on a data controller's accountability. This will result in the data controllers being responsible for any harmful consequences arising from improper handling of data.

Further, individual privacy is not holistically protected in the telecom sector. For instance, there is no equivalent of the "Do Not Call" provision for emails and instant messages. Therefore, although individual subscribers are spared calls and to a certain extent call tracking, they are still subject to intrusive emails and messages that are clearly based on tracking their ambient activity.

2. **In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?**

   Presently, the definition of personal data refers only to information that enables identification. However, data layering can allow even anonymised aggregate data to be converted to personal data. The definition of personal data should, therefore, not only cover information that allows easy identification of a natural person, it should also encompass anonymised aggregate data which can become personal information through the addition of one or more filters.

   A consent based model will prove to be increasingly inadequate, the more we start relying on data. More reliance on consent causes consent fatigue. Instead, a new data protection framework must focus on certain inherent rights that people have over their data.

Even if user consent is sought for certain services, they should not be designed as "take it or leave it" clauses. The user should have the ability to view the granular aspects of his consent, so that even if he does not agree to providing some data, he should be able to avail of the services of the data controller to the extent applicable.

3. What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

Although the data controller's primary duty is the processing of data such that no harm is caused to the data subject, the law should provide protection to the data controller if it proves that due diligence was exercised in processing data. If the controller fails to prove this, then it will be held liable. While this is not exactly a right, it is a protection. In this sense, the data controller's rights will not prevail over the rights that an individual has over his personal data. Similarly, just as the data controller does not have rights over the personal data of the subject, the data subject cannot sue the data controller over anonymised data if the data is not capable of being attributed to a specific person.

The regulatory mechanism governing data processing by controllers should be based on three principles:

A. ***Accountability***

A data controller must be held accountable for all the harm resulting from violations of data rights.

The biggest drawback of the prevailing privacy norm is the lack of accountability. By relying on consent, the data controller can, and often does, limit the extent of its liability for any harm caused to the data subject. The ideal data protection model must enable a data subject to hold the data controller accountable for any security breach or mishandling of the data. If the data controller, on the other hand, proves that it exercised due care and diligence while processing the individual's data, then it will not be liable.

B. ***Autonomy***

Each individual must have the power to determine how much data he is willing to

share with a data controller.

The data subject should have the autonomy to decide how much data the data controller can collect, process, disclose, or transfer.

C. ***Security***

The data controller should be responsible for ensuring the security of the data that it has collected.

Any breach of such security, even if it results in no harm, will render the data controller liable.

The definition of data controller should include the Department of Telecommunications, TRAI, and other security agencies of the government that have access to personal data or issue telecommunications licenses.

On the other hand, a data subject is anyone who provides his data to a data controller for the purpose of availing some services.

Mechanism for regulating and governing data controllers

A. ***Auditing and interception of data by "Learned Intermediaries"***

Harm to a data subject can be caused in a variety of ways. At the most basic instance, data collected could be misused for purposes that have no relevance to the business of the data controller or purposes for which the data was collected. Harm could arise from an unauthorised disclosure of personal information or as a result of the transfer of data to third parties without legitimate reason. When data is processed through algorithms for the purpose of automating decision-making processes, harm could result due to biases inherent in the algorithms used to process data. In all these circumstances, it is beyond the ability of the data subject to identify the cause for the harm that he suffered.

Hence, the regulatory framework must incorporate a mechanism through which such investigations can be carried out by entities who are capable of evaluating the output of algorithms used by data controllers and detecting bias (**Learned Intermediaries**).

These Learned Intermediaries, or auditors, could be drawn from the private sector and could be persons who understand processing of personal data and are skilled in the art and science of data-driven decision making. Their role will be to help identify instances where data rights are violated as well as suggest remedial measures to data controllers for correcting the biases in their algorithms.

B. ***Regulation and primary adjudication through a Data Commissioner***

A Data Commissioner must be appointed to function as a regulatory and adjudicatory entity. The Data Commissioner's regulatory duties will include: (i) setting appropriate standards for data controllers to adhere to; and (ii) performing periodic updates of these standards to account for advancements in technology.

The Data Commissioner will also have the power to investigate cases of improper processing, determine whether harm was caused, and accordingly pass appropriate orders of redressal.

4. **Given the fears related to abuse of this data, is it advisable to create a technology-enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorised authority to prevent harm? Can the industry create a sufficiently capable work force of auditors who can take on these responsibilities?**

Yes, the audit architecture must be technologically enabled to evaluate the use of personal data. This will allow efficient identification of unwanted queries and indicate whether the data is being accessed for the stated purpose or not. As the desired regulatory model will assure certain rights to the data subjects irrespective of their consent, there will be no need to audit consent.

Yes, audits will provide visibility to rectify or prevent harmful consequences.

In the context of processing through machine learning algorithms, harm to the data subject could take place over an extended period of time and, consequently, there is a risk that it could remain undiscovered unless the actions of the data controller are actively monitored. Harms caused by machine learning algorithms are often the result of inherent algorithmic bias. This bias is often extremely difficult to detect and puts the very process of

determining a breach of fiduciary obligations beyond the technical capabilities of most people.

Auditors should be capable of evaluating the output of machine learning algorithms and detect bias on the margin. They should conduct periodic reviews of the data controller's algorithms with the objective of making them stronger and more privacy protective, and not just point out problems in their functioning or punish the data controllers. They should be capable of indicating appropriate remedial measures if they detect bias in an algorithm. For instance, a data auditor can introduce an appropriate amount of noise into the processing so that any bias caused over time due to a set pattern is fuzzed out.

Auditors could adopt the following staged approach to review the operations of the data controller:

A. ***Publication of Queries to Databases***

The law must mandate all data controllers to publish the queries they make on databases containing information about the data subjects. As disclosure of this information will not detrimentally affect the data controllers' proprietary rights over their algorithms, it is easily realisable. In fact, enabling auditors to review the disclosed queries will help detect bad actors who are querying the database for information outside the purpose for which data has been collected. For instance, in the context of loan processing, a query on a bank's database relating to the caste of loan applicants is clearly irrelevant to the purpose for which the data was processed.

B. ***Black Box Audit***

In a black box audit, the actual algorithms of the data controllers are not reviewed. Instead, the audit compares the input algorithm to the resulting output to verify that the algorithm is in fact performing in a manner that preserves privacy. This mechanism is designed to strike the balance between the auditability of the algorithm on one hand and the need to preserve proprietary advantage of the data controller on the other. Data controllers should be mandated to make themselves and their algorithms accessible to the auditors for a black box audit.

C. *Access to Algorithms*

Should the data controller's algorithms appear to operate in a manner detrimental to the data subjects' rights, the data controller can be required to provide the auditor with access to its algorithms. Where possible, open source algorithms could be used for providing such access, so that their workings are visible for inspection while at the same time the data controller's proprietary details of the algorithms are protected.

It is anticipated that in time, data subjects will flock to those data controllers whose algorithms are consistently certified by auditors as being privacy neutral. This will incentivise the data controller to align with the accountability principle in the new framework.

As machine learning algorithms are tuned to be mathematically efficient instead of equitable, they may not necessarily be aware of the discrimination that takes place against the principles of equity and equality when they make a decision. On the other hand, these principles are keyed into the fundamental rights in our Constitution. So, biases in machine learnt data processes have the potential to be inconsistent with fundamental rights. As technology evolves rapidly, it would be counter-productive to define strict limits within which an algorithm functions. Rather, it would be best to define broad principles and develop specific restrictions on a case-by-case basis.

5. What, if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection?

Big data must be capable of being used to provide societal benefits, provided no harm is caused to individual data subjects from its usage. As elaborated earlier, it is important that the regulatory and audit mechanism is not merely punitive – but allows for rectification of errors and biases. The big data framework must only use aggregates of data and not personal (especially sensitive personal) information. Big data can also be processed by anonymising the underlying data, so that data controllers can process personal information without revealing the identity of the individual to whom it pertains. Similarly, for data that cannot be effectively anonymised, the method of "pseudonymisation" may prove effective.

The process of pseudonymisation, proposed as a secure data processing technique under the European Union's General Data Protection Regulations, allows the controller to process personal information such that it cannot be linked to a specific individual without adding some special attribute to it.

6. **Should government or its authorised authority setup a data sandbox, which allows the regulated companies to create anonymised data sets which can be used for the development of newer services?**

   We reserve our comments to the implementation of data sandboxes for want of more clarity on how they are intended to be deployed.

7. **How can the government or its authorised authority setup a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?**

   The government should not take on the responsibility of creating a technology solution to aid in monitoring. This role can be performed by market based entities such as auditors. These auditors would be technical personnel who would evaluate the algorithms used by data controllers to ensure that the outputs do not violate the rights of data subjects. The government's role in this would revolve around creating a mechanism by which such auditors can be suitably certified, supervised and monitored.

   The focus of the government's efforts, on the other hand, must be on regulation and primary adjudication of matters arising in the ecosystem. This can be achieved through the setting up of an authority, such as the Data Commissioner mentioned before. This authority will be tasked with redressal of grievances as well as the development of technology responsive standards of accountability and transparency.

8. **What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?**

   Insofar as safeguarding privacy is concerned, there are no further measures required to strengthen and preserve the existing telecom infrastructure. The need of the hour is a statute that addresses data protection in the country.

9. **What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues?**

   It is impractical to envisage all the issues that might concern the stakeholders listed in the question. Further, given the pace at which technology develops, it is possible that more key issues will arise or the existing ones might undergo a change. It is also possible that new stakeholders might crop up with the evolution of the underlying technology.

   Given this, it would be prudent to create a broad data security framework that addresses the safety of data at rest and data in transit. This framework can be based on certain fundamental principles, such as accountability, security, and autonomy. It must also be cognizant of the Supreme Court's recent ruling on privacy as a fundamental right under the Constitution. Once these foundations are in place, the jurisprudence around data protection can be developed on a case by case basis.

10. **Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?**

    As discussed earlier, the scope of some of the questions in this Consultation Paper are beyond the jurisdiction of TRAI. This is particularly true in the context of this specific question. The decisions around data protection norms will be determined by a data protection law, one that is expected to be enacted in the near future. It would be unnecessary for TRAI to explore the options to bring about greater parity in data protection norms in the country.

11. **What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?**

The legitimate exceptions to data protection requirements must be narrowly construed, expressly spelt out and be accompanied by adequate procedural safeguards.

Taking this as the yardstick, if the State is to engage in lawful surveillance in the interest of national security, it should only do so with clearance from a special body comprising members of the Executive and the Judiciary. This special body would have the power to authorise surveillance that is likely to affect data protection. It can also look at whether the data sought to be collected is necessary and that the collection is only for a specified purpose. Further, it can place restrictions on which other agencies of the State and third parties might have access to the collected data.

12. Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

The following measures can be considered for addressing issues arising from cross-border flow of information and jurisdictional challenges:

A. The data protection framework can be made applicable to the data pertaining to any Indian citizen. This will ensure that an Indian citizen whose rights have been violated will have a cause of action within the Indian jurisdiction.

B. This will also ensure that data controllers with an Indian presence will be answerable for the data rights violation. This is likely to result in such data controllers entering into agreements with their counterparts based abroad around the sharing of any liability that might arise due to their individual or collective actions.

[1] Rahul Matthan is a partner at Trilegal and a Fellow at the Takshashila Institution's Technology and Policy Program. Manasa Venkataraman and Ajay Patri are both lawyers and researchers at the Takshashila Institution. The Takshashila Institution is an independent think tank on strategic affairs and public policy contributing towards building the intellectual foundations of an India that has global interests. To contact us about the research write to research@takshashila.org.in or visit takshashila.org.in.

This document is the authors' formal submission to the Telecom Regulatory Authority of India (TRAI). TRAI floated a Consultation Paper on Privacy, Security and Ownership of Data in the Telecom Sector in August, 2017 to elicit views from stakeholders and the general public.