TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

iSPIRT Response

About iSPIRT

iSPIRT (Indian Software Product Industry Round Table) is a think tank for the Indian software Product Industry. Our mission is to build a healthy, globally-competitive and sustainable Indian Software product industry.

We welcome this move by TRAI to start a conversation on Privacy, Security and the Ownership of Data. We believe that India is at a unique tipping point where only a fraction of its users have gone online, and a majority are yet to do so. It is important we build the right set of protections for these users as they enter the digital world.

It is equally important not to limit our thinking to simply "protection" of data. We must also question how we can "empower" users, who will be data rich before they are economically rich, to use their data for their own benefit. iSPIRT has presented some of its views on how to Protect and Empower in response to the questions posted by TRAI below.

Detailed Responses to the Consultation Paper

Q.1 Are the data protection requirements currently applicable to all the players in the ecosystem 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?

Given the changed technology environment and the changing regulations around the world, it is time to update the norms and rules around data protection. The current data protection requirements are insufficient. For instance, there is no requirement to notify the user in the event of a breach or there doesn't exist an efficient grievance redressal mechanism for users whose data may have been compromised in a breach. Therefore, a nation-wide regulatory framework for data protection is required. The Justice Srikrishna Committee is tasked with putting it in place for India, and TRAI should consider aligning itself with recommendations of that committee.

Pertaining to the telecom sector, telecommunication-related data (like CDRs, recordings, SMS, etc) is often insecure during its transmission and open to potential leakage during its storage. Insecure protocols for signalling and forwarding are being used[1] [2] [3] and the current measures are not sufficient to protect the interests of telecom subscribers[4]. Therefore, we recommend to TRAI to mandate better encryption standards, create a clear framework on the applicability of Deep Packet Inspection (it may be used for network management and QoS, security, but not for advertising or malicious purposes), and adoption of international privacy and security standards by all service providers. This would form a core part of data protection and should be followed up with regular audits.

Q. 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?

Personal Data should be defined as any data linked to a specific user through any of the identifiers associated with that user. Informed user consent for collection of data should be a mandatory requirement for collecting data from users and there must be a mechanism for users to opt-in or opt-out of the data collection. We believe that stronger acceptable-use agreements must be introduced that dictate what the data collector or the eventual recipient of the data can and cannot do with it.

Further, it is also important to consider empowerment of customers to get access to their own telecommunications data. In February 2017, the Ministry of Electronics and Information Technology (MeitY) put forward the Digital Locker Framework (Digital Locker Technology Framework - Version 1.1[5]) as a national standard for aggregation and federated storage of information. Along with it, an Electronic Consent Framework (Electronic Consent Framework - Technology Specifications Version 1.1[6]) for enabling consent for sharing of data has also been released. Informed user consent, prior to sharing of personal data, should be made mandatory.

These open standards for consented data sharing should be considered, as the allow a user to get access to their own data, in the following ways:

[1] https://spectrum.ieee.org/tech-talk/telecom/security/alarming-security-defects-in-ss7-the-global-cellular-networkand-how-to-fix-them

[2] https://www.sans.org/reading-room/whitepapers/critical/fall-ss7--critical-security-controls-help-36225

[3] https://www.ernw.de/download/TSD2016_Known_Unknowns_of_SS7.pdf

[4] https://scroll.in/article/810148/how-easy-is-it-to-tap-someones-phone

[5] http://dla.gov.in/sites/default/files/pdf/DigitalLockerTechnologyFramework%20v1.1.pdf

[6] http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

- Make the user's telecom data (as defined by TRAI) available to users (in a digitally signed and machine readable format with ability for the users to view/print in human friendly format) via email or a telecom company's website
    - In case of multiple users linked to data, each user is permitted to share that data further with only their individual consent. Some fields may be protected to eliminate privacy of the other party.
- In accordance with the Digital Locker System, put the user's data into their Digital Locker on a periodic basis
- In accordance with the Electronic Consent Framework, put the user in control of their data by making it accessible for safe and secure consented data sharing with other service providers as determined by the user.

Also, an immutable and auditable record must be implemented for data being accessed in the interest of national security, based on a lawful process, and such access must be reported publicly at a monthly interval by each service provider. Appropriate privacy controls must also be built when enabling access to a user's records to the public.

User education will also be required to make the users aware about the risks and benefits of sharing their data. The regulator must strive to ensure that consent being given is truly informed and not a cognitive burden on the user, leading to over-consenting.

List of Telecom Information

A partial list of telecom information that must be made available to the subscriber is provided here.

- Customer Master Record
- Call Records
- Billing information (postpaid/prepaid, bills, payments, methods of payment)
- Connectivity with towers
- Browsing History
- Device information from the user's device (SIM number, IMEI number, IMSI number, etc)
- IP Traffic from the user device
- Any other information as specified by TRAI may be added to this list.

The above information may vary with the type of license - for instance, ISPs regulated by TRAI may have different user data. Details like the purpose of collection and duration of storage must also be shared with the subscriber.

If the data is appropriately anonymised using modern anonymisation technologies, such that the individual cannot be re-identified from the anonymised dataset, consent may not be required in the process of data sharing. In this regard, we also need a national standard for data anonymization techniques so that insecure and ad-hoc techniques for anonymization are not used.

Q.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.

Rights of the Individual must exist in harmony with rights of the Data Controller. In addition to some of the user rights suggested in response to Q2, here are rights and responsibilities for data controllers.

Rights of Data Controllers :

- Data Controllers may co-create data with users and can retain a copy of such generated data
- Anonymised data sets created from merging user data that is held by the Data Controller can be shared without user consent
- Data Controllers may demand for data that is proportional to the feature they are enabling. For example, a map-based application may request access to your location, to show you a route. They have the right to refuse service or offer a limited service, if a user does not consent to sharing data demanded, if it is a proportional demand. For example, a map-based application may not show you route, if you do not share location details with it.

Responsibilities of Data Controllers:

- Data controllers are responsible for the safe and secure storage of data, and face liability for unwanted access or sharing of data
- Data controllers must notify the purpose of personal data collected and collect only data proportional to the purpose. This would include collecting data for potential anonymization in the future.
- Data controllers must allow a user complete access to their data in a human-readable and machine-readable format.
- Data controllers must allow a user to share their data with other service providers in a safe and secure manner
- Data Controllers must notify the users in the case of a Data Breach
- There must be a mechanism for a subscriber to correct or amend a record of identifiable information about that subscriber
- There must be no personal data record-keeping systems whose very existence is secret to the subscriber

Suggested Mechanism for Regulating and Governing Data Controllers :

- Data controllers must publish regular statements that are easy to understand by the users about their practices.
- TRAI should monitor these statements for abusive practices, or proportionality.
- Complaints about not following these practices should be managed by TRAI through a customer grievance cell.
- TRAI should allow / facilitate the sharing of anonymised / aggregated data to enable innovation in this space.
- Periodic Privacy Impact Assessments and Security Impact Assessments must be conducted

Q. 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 authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

Yes, it is advisable to create a technology enabled architecture to audit the use of personal data and associated consent. That being said, the audit based mechanism will provide some visibility, but is not entirely sufficient to prevent harm. We recommend that such an audit mechanism be created, but at the same time a regulatory sandbox be created for testing out new innovations, that allow for rapid evolution of regulations.

Yes, a skilled workforce of data auditors will be required. However, since the data auditors would be dealing with large troves of machine-readable data, it may be possible and desirable to automate large parts of the auditing process using technological solutions.

Q.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?

It's important to give users control of their data such that they may then share it in a safe and seamless manner with various service providers to receive better services. The Reserve Bank of India has taken a major step forward in this regard by creating a new entity – the NBFC Account Aggregator (NBFC-AA) in its Master Direction DNBR.PD.009/03.10.119/2016-17[7]. As per the regulation, an account aggregator is a specialized entity meant to serve as an intermediary between a customer and different financial service providers providing Banking, Insurance, Securities, Pension and other such services and responsible for consolidating, organizing and presenting such financial information to the customer or any other financial information user. A similar approach,

[7] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598&Mode=0

like the Account Aggregator, would be a huge leap forward for empowering the individual subscribers in the telecommunications sector.

Given the rapid pace of technological changes, the regulator must provide for a mechanism whereby startups can experiment with new data-based businesses in a slightly modified or relaxed regulatory environment. Such an arrangement has been known as a Regulatory Sandbox. The scope of this sandbox should be restricted to a small fraction of the larger population to contain exposure to risk.

The regulator must evaluate the results of the sandbox to see which of the modified regulations should 'graduate' into the larger regulatory framework to encourage more innovation.

Further, we also encourage the regulator to create a Data Sandbox, as outlined in the next question.

Q.6 Should government or its authorized authority set up a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

The creation of an open data sandbox containing anonymised datasets would be a very positive step in the enablement of new data-driven businesses as well as introduction of newer services that deliver better customer value. Also, the regulators and government have a significant amount of data that can be anonymised and included in the open data sandbox that would further improve transparency and development of newer services.

Q. 7 How can the government or its authorized authority set up 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 exchange of audit logs with the regulator must be done through a technology solution that is automated and standardised. This solution should mandatorily use formats, and interfaces which are openly available for public review, and preferably use open source. Also, automated auditing is a part of the Electronic Consent Framework by MeitY[8].

Since the landscape is changing rapidly, the solution must be reviewed periodically, for new requirements, and to manage newly discovered harms.

[8] http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

Regulatory Technology around the world is developing through the use of RegTech (Regulatory Technology) accelerators, and it may be useful for TRAI to participate and learn from the global experience and to pioneer the next generation of monitoring tools and techniques.

Q. 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?

As mentioned in our response to Q1, it's important that data is protected using the highest security standards and so the current security protocols need to be updated to reflect the same.

The TERM Cells must conduct regular security audits of the telecommunications infrastructure and security-related practices employed by the telecom providers. Also, information related to various incidents - network threats, breaches, malware, DOS attacks, etc - must be shared proactively with the relevant players in the ecosystem and telecom subscribers, and in a timely manner to reduce potential damage.

The sustainable solution to these problems is to encourage the White-Hat community to constantly monitor and proactively report possible threats to the appropriate authority. We encourage the use of bug-bounty programs, community building and other such measures to build a large base of volunteers/professionals who ensure that the security of critical systems is up-to-date.

Q. 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?

If data protections (through a national policy / law) are framed in terms of user rights, then they will apply uniformly to all entities that handle or process user data. TRAI may have complementary requirements, that align with these, to ensure that all TRAI-regulated players conform to these data protection requirements. However, TRAI may not be able to impose these requirements on Over The Top services, Operating Systems, Browser vendors easily. In these scenarios, they must evaluate the potential customer harm (For instance, if an OTT service interferes with the security of the SMS or a browser captures sensitive user data), and work with the appropriate authority to control it.

Q. 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?

Yes - it is important that there is no regulatory arbitrage with regard to data protection in favor of OTT services which are not regulated. The current challenge is that jurisdictions of regulators are typically defined by the underlying infrastructure, and not by function. For example, even though Instant Messaging and SMS serve the same purpose and expose customers to similar harms, they are not regulated in the same way, nor by the same entity.

This is best achieved by ensuring that the data protection laws are in a legal framework laid down by the parliament. The framework must lay emphasis on the function being regulated, and not its medium. It should ensure that the consumer is protected from harms, irrespective of the channel. Such a legal framework may also introduce new entities which safeguard and protect user interests (e.g., entities tasked with auditing data collection and sharing practices), and which function across different regulatory domains.

Q.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?

Surveillance and law enforcement requirements must be rooted in appropriate laws, which provide a clear framework for such requests to be made, enforced, and audited. An immutable record of lawful requests for surveillance must be maintained to ensure that the laws are being followed, and can be submitted for judicial oversight. It would also be useful to publish statistics for these requests, in the aggregate on a monthly basis, by each service provider.

Q.12 What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

India is a large enough market for all regulated players to operate their services from servers, and offices in India. However, for the provision of cross border services, global services, as well as for reasons (such as redundancy, high availability), it is possible that the data for Indian users may leave the jurisdiction. All regulated entities must submit to Indian jurisdiction for the provision of services. Hence, Indian rules and regulations must apply even when the data or servers are physically not present in India. Any data that leaves the jurisdiction, which belongs to an Indian user, must be reported to the authority (For the most part, this may not be on a per user basis, but the situations in which this data leaves, for instance, to provide international calling, SMS, and roaming services, etc)