ISACA
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008-3105, USA
Web Site: *www.isaca.org*

Telephone: +1.847.253.1545
Facsimile: +1.847.253.1443
E-mail: *info@isaca.org*

Q.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?

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?

In response to both Q.1 and Q.2:

While the consultation addresses a number of data protection requirements, there are additional considerations for citizens that merit consideration and potential inclusion:

- **Right to access:** Individuals should be able to request confirmation as to whether or not personal data concerning them is being processed, where it is being processed, and for what purpose. India's government might also want to consider how it wishes to address those requests from citizens. In response to those requests from individuals, data controllers should provide a copy of the personal data, in a widely-supported electronic format (i.e., Word, PDF, etc.). These requests could either be free of charge to citizens, or could require a modest fee, thereby creating an additional revenue stream for government.
- **Right to information:** This has to be the basic tenet of all data collected. TSPs must inform individuals about all information that is collected and also information that is being derived from their data. At present, telecom subscribers do not know what information is being collected, for what purposes, with whom the data is shared and in what format, and with what end use. It is imperative that TSPs disclose data being collected to their subscribers and the purpose for which such data is being collected. A unified definition of such data may also be required as some of the provisions of existing legislation may need to be re-examined with the Personal Identifiable Information provisions of the IT Act in mind.
- **Right to forget:** Individuals must be afforded the right to be forgotten.
- **Data portability:** Simply put—the data protections afforded to India's citizens travels with them, regardless of where in the world their travels take them.
- **Data should only be used for the purpose that it was collected for:** If a data controller wants to use the data for other purposes (e.g. for marketing by the data controller's organization, or

passing on the data to another organization for marketing purposes, etc.), then consent should be obtained from the data subject.

- There also needs to be a right of the data subject to make a Subject Access Request, and to request that the data controller provide the data they hold on the data subject. The data subject's rights should also include the right to have erroneous data corrected or deleted.

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.

First and foremost, Data Controllers should only use data for the purpose that it was collected for, and data should be kept for only as long as the purpose it was collected for.

Responsibilities for Data Controllers should include adherence to and expert knowledge of all applicable data protection laws, regulations and practices affecting the organization in question. In addition, Data Controllers must always maintain a direct reporting access to the highest level(s) of an organization; issues like information and data security are enterprise-level concerns, and those responsible for their safeguarding should liaise directly with the decision makers at the pinnacle of the organization. Creating a Data Control Authority as a mechanism for governing, regulating and educating Data Controllers might be a concept worth considering. Centralizing this function enables streamlined two-way communications, enabling better information dissemination to all involved.

The rights of an individual over his or her personal data should remain paramount at all times. In issues of national emergency or security, the rights of a Data Controller might be required to supersede the rights of an individual. However, it is not ISACA's place to suggest this as a course of action. This is a determination best made by each respective government, taking into consideration the rights of their citizens, and balancing that against the safety and security of their nation. Fundamental rights to privacy, as well as personal liberties, are matters of grave importance, as India's recent Supreme Court ruling noted[1]; the Court's decision must be considered as well in any deliberations regarding the rights of Data Controllers superseding the rights of individuals.

In addition to these concerns, consideration must be given to requiring TSPs to provide opportunities for individuals to report issues. This could be very much akin to the current ombudsman structure that is currently in place for reporting complaints.

[1] V. Doshi; *India's Supreme Court Says Privacy is a Fundamental Right in Blow to Government*; Washington Post, August 24, 2017

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?

ISACA believes that it is advisable to create a technology-enabled architecture to audit the use of personal data and associated consent; such a mechanism would be of benefit to India's government while simultaneously protecting its citizenry. Though India's audit workforce has become increasingly robust in recent years, enhancement and expansion of that workforce—to best address the added responsibilities the creation of this new architecture would bring with it—is an advisable course of action. However, whenever and wherever possible, technological solutions should be explored as well. Ideally, such solutions should be evolutionary in intent; the solutions should be designed so that they meet today's needs, but are able to be adapted and improved upon to meet future challenges. This two-pronged approach—augmenting both the human and technological aspects—would be of great value to both India's government and its citizens. An additional consideration, one which would complement this two-pronged approach, would be the creation of a central register containing information for each data controller. The register's information should include, but need not be limited to: the name of the data controller and their organization, the nature of the information collected, and the purpose for which the data was collected.

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?

ISACA believes that encouraging the creation of new data-based businesses (within an overall data protection framework) is only part of the puzzle. It is imperative that privacy by design occurs. Products, services and solutions should include data protection and security as core elements of design and development. This applies to both data-based and non-data-based businesses equally.

To support such an approach, building a data protection framework that keeps privacy by design as a central focus is critical. India—and the world—is already seeing the dangers inherent in not incorporating adequate privacy and security elements at the design and development levels; this is a negative trend that must be reversed. Creating frameworks that include privacy by design can do so.

As part of these data protection frameworks, the governing body should retain the right to access any organisation to review their data privacy processes to assess if they are appropriate and effective.

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

This is an approach most recently undertaken by Singapore, and it is already meeting with some initial success. While the Singapore sandbox is still in its inaugural year, it bears close examination by India's government. Early indications are that this could become a valued tool for Singapore in its efforts to develop new services, and foster startup companies within the FinTech sector. This could have a similar effect within India, albeit on a much larger and more impactful scale. India's government, or an authorized authority, should absolutely explore the creation of a data sandbox, but do so with a close eye on the ongoing work in Singapore, to better enrich India's own efforts in this area.

Q. 7 How can the government or its authorized 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?

ISACA, in its earlier response to ***Q.4***, noted that a combined focus on enhancing both the human and technological aspects of the workforce would be of value to India and its citizens. The advances we have already begun to see with artificial intelligence, machine learning, and process automation bode well for technological solutions that will enable compliance monitoring at an ecosystem level. It is difficult to describe what exactly this should look like; the best solution should meet all the needs of today, yet retain enough flexibility and adaptability that it is able to address the needs of the future as well. One element which must be included, however, is the right of access to audit; the governing body should retain the right to access any organisation to review their data privacy processes to assess if they are appropriate and effective

Ensuring that regulations keep pace with a changing technology ecosystem, however, is another matter. We have already seen that the regulatory environment does not always keep pace with the advancement of technology. Going forward, it is in India's best interests to keep pace as best as possible; indeed, it is in all nations' best interests to do so. This will require all stakeholders, acting in concert, to explore the best possible path(s) forward, and do so in a manner that is thorough, comprehensive, and rapidly iterative.

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?

ISACA believes that a combination of many of the elements it has already mentioned—improvements and enhancements to the professional workforce and the technologies that augment their work, as well as public policy and regulatory efforts that are organic and iterative—are the best tools for strengthening and preserving the safety and security of telecommunications infrastructure, and India's digital ecosystem.

There is a need, as well, to consider the people, processes and technology controls required to appropriately and adequately protect data, and to focus on the protection of data both 'in transit' and 'at rest'.

As for specific measures, it would be beneficial to explore measures that combine some or all of these aforementioned elements; for example, putting forth public policies that support worker retraining, while also incentivizing companies to invest in technologies that will augment and enhance the efforts of their newly-retrained professional workforce. Other approaches could include adherence to standardized frameworks and benchmarks for performance, security, and capability, among other areas. Cyber security frameworks and models focusing on maturity enhancement of the ecosystem should be constructed with flexibility and evolution in mind, so that the systems keep pace with shifts within the ecosystem and are more readily able to scale up to meet increased requirements.

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?

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?

In response to both Q.9 and Q.10:

There is a need to consider the responsibilities and requirements of both data controllers and data processes. The focus for data processes is on security measures and deleting data held in backups, beyond the length of time required to keep the information for the purpose that it was collected. Another of the key issues in data protection, ISACA believes, is the 'right to be forgotten' by stakeholders within the digital ecosystem. Individuals should have the final say over their data, and be able to cease its dissemination to other stakeholders[2]. Likewise, individuals should retain the right to know where and when their data is being shared with third-party stakeholders. In light of India's recent Supreme Court decision[3], there is likely to be discussion and debate about issues such as this. It would be beneficial if these debates and discussions produced legislative and regulatory measures that were well-considered, and organic enough to evolve with shifts within the ecosystem. For the stakeholders that become possessors of third-party data, it is critical that mandatory breach notification be in place, and that the community is held to the strictest of standards.

[2] Only for data held by consent; data may need to be kept and not deleted for legal purposes and for business reasons related to the purpose that the data was collected.

[3] *ibid*

Various stakeholders must be required or should consider mapping the data being collected from individuals and what the aggregation of such data might mean within the ecosystem. Efforts must be taken to drive all actions based on the unified intent of protecting customer privacy and the prevention of unintentional aggregation (especially in the context of the digital ecosystem and the various types of tracking/data collection it allows such as digital fingerprinting, cookies etc.), which allows the breach of any of the seven types of privacy which are to be afforded to the individual**.**
TSPs and other service providers should be required to carry out privacy impact assessments and ensure the transparency of such assessments and outcomes to regulators and other stakeholders.

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?

In ISACA's earlier response to Q.3, we noted that the rights of an individual over his or her personal data should remain paramount at all times. This includes those times when their personal data is in the hands of TSPs and other providers in the digital ecosystem.

However, in issues of national emergency or security (and with a valid, documented justification), the rights of an individual might be superseded—but this is a choice a nation must make; it is not ISACA's place to suggest a course of action. India, like all nations, must take into consideration the rights of their citizens, and balance that against national safety and security. Fundamental rights to privacy, as well as personal liberties, are matters of grave importance. India's recent Supreme Court ruling on privacy must be considered in any deliberations regarding the superseding of the rights of individuals to data protection, particularly in matters of law enforcement and lawful surveillance.
Other than in matters of national security, the individual must be afforded the right to be informed/made aware of the information that has been shared by TSPs to government/regulatory agencies or any other parties without their express consent.

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?

As was mentioned earlier, data portability is paramount. Simply put—the data protections afforded to India's citizens should travel with them, regardless of where in the world their travels take them, or where their data flows to or from. Possible measures that focus on the cross-border flow of information and merit further examination could include the U.S government's "Privacy Shield" and the EU government's "General Data Protection Regulation".

Some additional measures that can be considered include:

1) Codify minimum requirements that need to be met.
2) Inform the individual what information is collected during the cross-border flows (especially in the light of the digital eco-system mentioned in the TRAI document) and the potential threats/risks to privacy.

Suggestions for

Privacy, Security & Ownership of data in the Telecom sector.

By
Zunzar Patil
M:- +91 9223173302
E:- zunzar.socialwork@gmail.com

Some suggestions

- As a part of Service provider license agreement Ts&Cs , Telcos should be made to agree to explicit Non Disclosure agreement to protect privacy of user data.
- During course of time Telcos are able to gather historic data of users on their location, movement patterns, online activity, purchase patterns, calling patterns etc. This data needs to be encrypted with private key which is available only with user. Telcos can retain the public keys for each user accounts.
- Along with Telcos all OTT application providers also need to agree to Non disclosure agreement towards protection of user data privacy.
- With integrated mobile computing ecosystem all mobile operating system providers (Google, Apple & Microsoft), Mobile manufacturers also need to be bound into Data protection guidelines.
- Integrated User data protection guidelines need to be designed for entire Mobile communication ecosystem (Telcos-> Mobile manufacturers-> Mobile application providers-> OTT application providers.), Each of these stake holders at different levels gather different level of personal user data which if not protected can compromise privacy, safety, security of mobile users.
- It should be made mandatory to all stake holders to issue popup notification to each user requesting for their concurrence before logging respective user data, incase user does not agree to logging of personal data , user data logging should not be initiated.
- There should be provision to profile users as per their preferences on personal data privacy, inline with “Do Not Disturb” profile, there should be “Do Not Capture” profile, for users opting for DNC there should be no user data logging by default.

Jai Hind