SUBMISSION OF COMMENTS ON TRAI CONSULTATION PAPER

Privacy, Security and Ownership of the Data in the Telecom Sector

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?

The applicable data protection requirements as currently defined by the policymakers and regulators in India are insufficient to protect the interests of telecom subscribers. This is evident from the fact that 'unlike other developed countries, India does not have a separate/dedicated data protection law. Though the Government had brought the 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011'[1] – the same seems to be inadequate for data and privacy protection in the wake of recent cyber challenges.'[2]

Further, it is important to note that a sound data protection regime protects consumer data not just from private digital platforms, but also from the Government. 'Increasing data leakages through the websites of Central and State Government departments has become worrisome.'[3] Consequently, 'the Government has constituted a ten-member committee to make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India, and suggest a draft Data Protection Bill.'[4]

Periodic sensitisation workshops to build awareness on data protection must be organised by appropriate regulators and policymakers with subscribers and other critical stakeholders. These workshops can be organised using ready network of registered Civic Action Groups (CAGs) and academia to ensure strong penetration among subscribers. Consumers need to be empowered through granting them more control (in terms of sharing, porting, refusing, pull out etc.) over their data. The fog covering the question of who owns the data must be cleared.

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 the 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?

[1] Information Technology Rules, 2011 is accessible at: http://meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

[2] Mondaq Article – Data Protection Laws in India: The Road Ahead – published on July 1, 2015 is accessible at: http://www.mondaq.com/india/x/408602/data+protection/DATA+PROTECTION+LAWS+IN+INDIA+THE+ROAD+AHEAD

[3] The Wire Article – 130 Million Aadhaar Numbers were made public, says new report – published on May 01, 2017 is accessible at: https://thewire.in/130948/aadhaar-card-details-leaked/

[4] Economic Times Article – Justice B N Srikrishna to head committee to draft data protection framework – published on August 2, 2017 is accessible at: http://tech.economictimes.indiatimes.com/news/corporate/justice-bn-srikrishna-to-head-committee-to-draft-data-protection-framework/59870627

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India ◆ Ph: +91(0)141-228 2821 ◆ Fx: 228 2485 ◆ Email: cuts@cuts.org ◆ Website: www.cuts-international.org
Also at Calcutta, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); and Geneva (Switzerland).

Personal data has not been explicitly defined under Indian laws.[5] Reliance has been placed on the definition of data [as defined under Section 2(1)(o)[6] of The Information Technology Act, 2000] and personal information [as defined under Section 2(1)(i)[7] of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011], though The Information Technology Act, 2000 has defined information separately under Section 2(1)(v).[8]

The Data (Privacy and Protection) Bill, 2017 (Bill No. 100 of 2017), as introduced by the Member of Parliament (MP) Jay Panda in the Lok Sabha defines 'personal data' in S.2(l) as following:

"Personal data means any data or information, which relates to a person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data". This definition is similar to the one under recently adopted General Data Protection Regulation (GDPR) by European Union (EU), which will come into force in May 2018.

In light of the rising economic value of data, it becomes imperative that the definition of 'personal data' be wide enough to include consumers' passive data.[9] This raises the important question of adequately defining/classifying various kinds of consumer data, such as: qualitative data, descriptive data, preferential data, quantitative data, identity data, anonymous data etc.[10] All of these must be optimally protected, through different consumer consent mechanisms and legal protective regimes.

User consent MUST be taken before sharing their personal data, or any of the above-mentioned data with a third party, for commercial, as well as non-commercial purposes, such as processing, analytics, storage etc.

Both regulatory and technological modes should be used to establish control/ownership over one's 'personal data', including the right of portability of such data. Further, consumers might also be empowered through a defined information disclosure mechanism so as to understand how their data is being used by data controllers, and for what reasons. Such disclosure in a simple and standard format, with multi-lingual accessibility, will allow such consumers to report any misrepresentation or violation grievances and hold the Data Controller accountable. A consumer awareness generation programme should also be launched simultaneously with a strong intent to strengthen the consumer grievance redressal mechanism.

---

[5] http://www.livelaw.in/data-protection-india/ accessed on 03.11.2017

[6] 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

[7] 'Personal information' means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

[8] 'information' includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

[9] Passive data collection is the gathering of consumer data through their behaviour and interaction without actively notifying or asking the consumer's permission. In fact, most consumers don't even realise how much data is actually being captured, nor how it's being used or shared. https://martech.zone/what-is-passive-data-collection/ accessed on 03.11.2017

[10] https://www.smartinsights.com/customer-relationship-management/customer-privacy/types-customer-data/ accessed on 03.11.2017

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India ◆ Ph: +91(0)141-228 2821 ◆ Fx: 228 2485 ◆ Email: cuts@cuts.org ◆ Website: www.cuts-international.org
Also at Calcutta, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); and Geneva (Switzerland).

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 Data Controller might only supersede an individual's right over personal data only in situations, where there is a strong case and evidence for compromise of national security and/or sensitive law and order situation. This would help in plugging out anti-social elements, while providing rightful access to responsible consumers.

As consumers can get empowered through a defined information disclosure mechanism so as to understand how their data is being used by data controllers, and for what reasons. Data Controllers should be duty-bound to make such disclosure in a simple and standard format, with multi-lingual accessibility, will allow such consumers to report any misrepresentation or violation grievances and hold the data controller accountable.

A Data Controller firm might have the rights to commercially use a user's personal data provided that the firm has informed consent of the user. However, it need not have the 'exclusive' right to such usage data. Therefore, it should be the duty of such Data Controllers to make available usage data (in a requisite format) to consumers, so that the latter can use their Right to Portability.

Moreover, it is to be noted that to put the data protection regime in place, private and Government Data Controllers must be treated alike. Further, the Data Controllers must continue to be held accountable for any data breaches that might occur at the data processor's end, in case the task of processing the data collected by the controller is being outsourced to a third party for processing/analysis. The distinction between a Data Controller and a Data Processor becomes important to remember in this regard.

A suitable tech-framework coupled with futuristic and non-restrictive regulatory framework should regulate and govern Data Controllers. There is need to ensure that such frameworks should be optimal and promotes competition, and at the same time, does not pose hurdles for future innovation.

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

Just like the algorithms used for distance and fare calculation, by taxi aggregator mobile apps are checked and validated for accuracy, by Standardisation Testing and Quality Certification(STQC) or any other agency authorised by Ministry of Electronic and Information Technology (MEITY), on a one-time basis,[11] a similar mechanism can be put in place for auditing data collection and processing by digital technology platforms to prevent any harm to consumers *viz-a-viz* data privacy and protection.

[11] http://morth.nic.in/showfile.asp?lid=2525 accessed on 03.11.2017

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India ◆ Ph: +91(0)141-228 2821 ◆ Fx: 228 2485 ◆ Email: cuts@cuts.org ◆ Website: www.cuts-international.org
Also at Calcutta, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); and Geneva (Switzerland).

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

Viewing the possibility of a dominant/monopolistic market situation (winner-takes-all-scenario), 'data portability'[12] can be an *ex ante* tool to promote competition. Non-access to consumer data should not become an entry barrier or a cause for ousting of competitors. However, any regime for data privacy and protection must be optimal – while being pro-competition it must not hamper innovation.

The importance of classifying the various kinds of user data is once again highlighted through the question of data portability, since the distinction made between the different types of data will be instrumental in determining the scope of 'data portability', i.e. what data should/should not be ported.

Further, viewing the rising fears of data colonisation, it is imperative for India to frame optimal laws pertaining to data export so as to ensure the availability of domestic data to domestic start-ups, who might not be able to compete with large foreign multi-nationals, given the increasing dependencies on data-driven business models.

Situations giving rise to concentration of power in the hands of a few foreign data controllers should be avoided, and room must be made for Medium, Small and Micro Enterprises (MSMEs) to capitalise on the large pool of data available within the country. Therefore, the data protection regime being pondered over must take into account the Start-up India initiative of the Government.

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

Such data sandbox is an encouraging initiative to drive research and innovation activities among regulated companies. In order to understand the use cases of newer data services and risks to consumers better, the Government could adopt a regulatory sandbox approach,[13] i.e. permitting use of data sets in controlled environment (within specified consumer base – with informed consent, for specific time and purposes).[14] This would help understand consumer protection concerns relating to such new services and facilitate the self-regulatory forums to design appropriate disclosure and grievance redress standards.

---

[12] The right to data portability allows a user to receive their data back in a format that is conducive to reuse with another service. The purpose of data portability is to promote interoperability between systems and to give greater choice and control to the user with respect to their data held by other entities. The aim is also to create a level playing field for newly established service providers that wish to take on incumbents, but are unable to do so because of the significant barriers posed by lock-in and network effects. https://www.legallyindia.com/views/entry/my-data-my-rules-the-right-to-data-portability accessed on 03.11.2017

[13] Schan Duff (2017) - Modernizing Digital Financial Regulation: The Evolving Role of RegLabs in the Regulatory Stack – is accessible at https://www.aspeninstitute.org/publications/modernizing-digital-financial-regulation-evolving-role-reglabs-regulatory-stack/

[14] The Reserve Bank of India's research arm Institute of Development and Research in Banking Technology had issued a whitepaper on applications of blockchain technology for banking and financial sector in India (see, http://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf). Similar approach could be adopted in case of designing newer services.

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India ◆ Ph: +91(0)141-228 2821 ◆ Fx: 228 2485 ◆ Email: cuts@cuts.org ◆ Website: www.cuts-international.org
Also at Calcutta, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); and Geneva (Switzerland).

Based on the findings of the regulatory sandbox, the Government can work with self-regulatory forums to ensure market-based solutions are available for consumers in form of adequate transparency, disclosures and insurances to deal with losses. In addition, the regulator must ensure a balanced risked-based approach wherein sophisticated informed consumers are not eligible for extra protections available for uninformed and retail consumers. Besides, the regulator should also keep a track of the data with respect to consumer concerns and must intervene through regulation and other means only when such concerns cross a predetermined threshold. It does not make sense for the regulator to intervene sans existence of market failure.

Q. 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?

No Comments.

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?

No Comments.

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 to address these issues?

Please see our response to Q. 2 and 3.

Q. 10 Is there a need for bringing about greater parity in the data protection norms applicable to Telecom Service Providers (TSPs) and other communication service providers offering comparable services (like Internet-based voice and messaging services). What are the various options that can be considered in this regard?

Yes, there should be parity in data protection norms applicable to TSPs and other communication service providers offering comparable services.

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?

To support lawmakers in such situations, Rights of Data Controller mighty only supersede an individual's right over personal data in such cases where there is a strong case and evidence for

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India ◆ Ph: +91(0)141-228 2821 ◆ Fx: 228 2485 ◆ Email: cuts@cuts.org ◆ Website: www.cuts-international.org
Also at Calcutta, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); and Geneva (Switzerland).

compromise of national security and/or sensitive law and order situation. This would help in plugging out anti-social elements, while providing rightful access to responsible consumers.

Consumers can also be empowered through a defined information disclosure mechanism so as to understand how their data is being used by Data Controllers and for what reasons. Such disclosure in a simple and standard format, with multi-lingual accessibility, will allow such consumers to report any misrepresentation or violation grievances, and hold the Data Controller accountable.

The exceptions laid under the recent landmark judgement[15] of the Supreme Court (SC) that establishes 'right to privacy' as a fundamental right might be taken into account. The SC stated, "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."[16]

This would necessarily mean that the State (read as Government) has a duty to safeguard citizen's right to privacy. It would also mean that any infringement of the 'right to privacy' can only occur by following the 'procedure established by law', withstanding the rigorous test of 'due process of law'. The leading example of Apple refusing to share consumer data of a mass shooting suspect with the FBI[17] is particularly useful in this regard. India must not walk on the evasive path, in which it is unable to regulate technology platforms in terms of providing exceptions to data privacy and protection.

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?

The advent of cloud computing raises important questions regarding the accountability of service providers who store a country's citizen data outside its boundaries, leading to a conflict of jurisdiction in case of any dispute. Moreover, having no or minimal control over crucial data due to the absence of localisation requirements could be detrimental to the national security of such countries in certain instances, since the data would be outside the purview of the country's cyber-security policy.

Many countries have enacted extensive data localisation laws, which require companies to process and store a copy of the data locally, apart from mandating Government/user consent for data transfers, or restricted access to certain websites, thus bouldering the cross-border flow of data.

In addition, the rising economic data value along with consumer data protection and data sovereignty issues have prompted many countries to enact such laws. Incubating and protecting domestic technology-driven companies, i.e. Start-ups, and MSMEs from High-tech Transnational Companies (TNCs) is another reason.

[15] Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012 – judgement delivered on 24.08.2017
[16] ibid
[17] https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple accessed on 03.11.2017

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India ◆ Ph: +91(0)141-228 2821 ◆ Fx: 228 2485 ◆ Email: cuts@cuts.org ◆ Website: www.cuts-international.org
Also at Calcutta, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); and Geneva (Switzerland).

However, free flow of data also enables MSMEs to reach their prospective global customers, along with participation in the global value chains (GVC). The key challenge is to find the right balance between protecting data privacy without restricting trade.

Therefore, enhanced inter-governmental cooperation is crucial to pave the way ahead for cross-border data flow to accelerate the growth of digital trade, without compromising on the data security and sovereignty, and ensuring fair competition in the market.

For queries and suggestions, please write to: Rahul Singh (ras@cuts.org) and Sidharth Narayan (sid@cuts.org)

****

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India ◆ Ph: +91(0)141-228 2821 ◆ Fx: 228 2485 ◆ Email: cuts@cuts.org ◆ Website: www.cuts-international.org
Also at Calcutta, Chittorgarh and New Delhi (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); and Geneva (Switzerland).