RESPONSE BY IT FOR CHANGE

to the Consultation Paper on

PRIVACY, SECURITY AND OWNERSHIP OF THE DATA IN THE TELECOM SECTOR

by Telecom Authority of India

November 2017

IT *for* CHANGE
NGO in Special Consultative Status with United Nations' Economic and Social Council

Responses by IT for Change, Bengaluru,
to the Consultation Paper on
Privacy, Security and Ownership of the Data in the Telecom Sector
by Telecom Regulatory Authority of India

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 current data protection regimes in India as applicable to all the players in the ecosystem are very insufficient. Section 72 A of the IT Act only protects against sharing of personal data that is done without consent or in breach of lawful contract. It has become amply evident by now that individual users have no real protection under such laws because consent/ contract frameworks are written in very broad terms. They are also entirely unilateral, between very unequal parties, and with consumer having little or no choice in the matter. Privacy related safeguards in ISP licenses are also based on user consent, and therefore suffer from the same drawbacks.

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

#393, 17th Main, Jayanagar 4th 'T' Block, Bangalore – 560 041, India
Tel.: 91 80 2665 4134, 2653 6890, Fax: +91804146 1055
www.ITforChange.net

Personal data?

Definition of personal data as any such data which, whether by itself or in combination with other data, can identify a person, is appropriate for the purpose of privacy protection. But, even for this purpose, its implications requires greater elaboration as for instance provided by Opinion 4/ 2007 of EU's Data Protection Working Party.[1]

However, such personal data is not the only form of user-generated commercially valuable data, which aspect of data has been stressed in this consultation paper, as do many user data related documents nowadays. To the extent the intention is only to protect one's privacy then safeguarding only personal data, as defined above, is meaningful. But if we are exploring the issue of commercial value of data[2], and its ownership, we need to be concerned with a larger set of user-generated data. Personally-identifiable data has great commercial value, but even 'collective data' (or social data) about groups of data subjects has considerable value. A company providing an educational application, even if it does not collect personal data, will gather a lot of granular collective/social data about students, in a particular school, in a particular district, segregated minutely along demographic and behavioral types, and innumerable other indexes,[3] which provide most valuable educational insights about what kind of students learn what, in which manners, in what conditions. A question may be asked; who should own these data/ insights, the school, the district educational authorities, or the application provider? Such data/ insights will soon become indispensable for developing education policies, and if indeed the application provider becomes the absolute owner of the data/ insights, would the education authorities then need to pay it for data/ insights required for policy-making? And if the provider is a foreign company, and the sector involved of strategic value, questions about the the geo-political implications, such as paying for the data in in foreign currency arise. Such questions can be extrapolated to most data-collection situations and almost all sectors.

The user generated data that has commercial and other values, and whose ownership needs better clarification, is thus not just personal data but also collective or social data. We can call this larger set as user data, to mean such data to which a user can claim certain kinds of ownership rights, either exercised individually or collectively. In terms of

1 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

2 We use only the term "commercial value" here but the value of data could also be policy related or political, or social and cultural.

3 Or it could be rather less structured providing training data for Artificial Intelligence.

exploring ownership and commercial value, therefore, the appropriate term is user data and not just personal data.

Yes, user's consent should be taken before sharing his/her data for commercial purposes.[4] But as is generally recognized nowadays, and as also stressed in the consultation paper, consent is necessary but it does not provide an adequate protection to consumers, because of an unequal nature of relationship between service provider and consumer, the latter's often monopoly or near monopoly status, and complexity of information around such consent. We therefore need to go beyond consent based approach to privacy and user's control over her/ his data.

New capabilities that must be granted to users over personal (and other user data) are foremost of a legal kind. These consist in defining the ownership patterns over various kinds of user generated data, and defining what constitutes such data (and other categories like data that is further developed from/ over user generated data). In the same way as definitions of ownership of physical resources (property regimes) were key to construction of civilized large-scale physical spaces, cyberspace must also be constructed from defining access and ownership rights to its most important resource, data. Like in physical spaces, these rights can be individual or collective. To enforce such legal regimes we will require technology and other means.

Such definition and enforcement of data ownership is the best and the foremost way to empower users to own and take control of their data. Once this is done, appropriate institutional and technological means will need to be devised to implement such ownership.

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.

Data Controllers should act as trustees of user data (such data which is established as individually or collectively owned by users, under the aforesaid required new legal

4 Such consent should also be taken before sharing it for other purposes, other law provides for otherwise. However, we understand from the question that the accent here is commercial exploitation of personal or user data, and our responses will conform to such a focus.

regimes). They should be able to develop services based on such data but in strict trusteeship for users, demonstrating at all steps that (1) since such services are build over user contributed data, their commercial value accrues to the latter to a significant/ appropriate level, and (2) any value creation does not harm users as is assessed by the . Both, (1) and (2) are very difficult for individual users to assess much less enforce, and therefore this should be done through appropriate regulatory regimes.

For constructing ownership patterns for user-generated data within a country, it may be useful to *inter alia* consider the elaborations about national trusteeship based ownership of natural resources provided by the Supreme Court in the 2G spectrum auction case. It can be explored if collective user data (as nation's social resources) can be considered akin to a nation's natural resources, in this regard.

Data Controller rights begin after all user rights have been asserted and provided for, as being within and subservient to user rights.

We need to begin by developing the first principles of data ownership and value, as indicated above. Based on these principles elaborate law and regulation must be laid out. As data concerns both fundamental civil/political rights, as in privacy, and economic and social rights, as regarding right to commercial value of data generated by users, some such first principles may even need to be put into the Constitution, or read into it (as the Supreme Court recently did about privacy and will likely do regarding social/ governance value of data in the Aadhaar case).

For effective regulation, all data-based businesses above a certain (sufficiently large) threshold of users must be subject to close regulatory scrutiny, but in a manner that does not ham-shackle the growth of digital economy, which of course is fundamentally data-centric. This trade-off needs to be carefully negotiated, and will require much political, legal and regulatory deftness. But simple abdication of data regulation as largely is the situation today is not acceptable. As discussed below, it also favors foreign owned mega digital corporations over domestic digital industry.

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?

Such a technology enabled architecture could only be useful if there are appropriate laws and regulations in place, and should be used to enforce them. For instance, if it were designed to simply track consent under existing frameworks, while it will have some use, it will be a very limited one because consent is easily obtained in current frameworks for almost all and any kind of data. Having said so, employing such a technology enabled architecture for auditing the use of personal data can be beneficial. We do believe that in the current hyper technology-based social architecture, innovative use of technology will be required to effectively implement laws and regulation. Therefore, while we are unable to develop a good picture of the precise kind of technology based architecture that TRAI may have in mind in framing this question, we welcome such an exploration.

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?

Digital economy is centrally about developing granular intelligence about everything based on extensive data about the concerned thing, field or sector. Some such data may indeed be developed by a body corporate by its creative efforts and should belong to it, and it can legitimately build a competitive advantage on its private ownership. However, much of the data that contributes to building such granular digital intelligence about a thing/ field/ sector comes raw from the social, physical and natural environment outside the ownership realms of a body corporate. The latter's ownership over such data is questionable. It is either appropriately owned by individuals users or collectively as as groups, one form of which is the whole nation state.

Currently those who collect all such data assert their exclusive ownership over it, the legal basis of which is uncertain (often trade secret protections are employed). These data collectors then use exclusive access to this data as their central business model, data which more appropriately should be a 'commons'.

Legal and technical means should be developed so that this latter kind of data is

considered as a "data commons" for anyone to use, but with protections (like through APIs employed by IndiaStack[5] for a similar purpose) that ensures against harm to individuals and groups by indiscriminate use of such data. Businesses can combine insights from such commons data with those from their private data to provide the best possible range of digital services (or digitally intelligent services). Such a "mixed economy" model of commons plus private data will enable a much more vibrant and competitive digital economy than the current model of monopolistic private hoarding of personal and social data even when its private ownership is questionable. It will also ensure a level playing field for domestic digital businesses that is not available today. These domestic firms lack the immense capital needed to 'develop monopoly over data hoards first and make profits latter' – which is the way most digital big business is done today.

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?

Our response to the above question directly goes in the direction of exploring such a mechanism as posited in this question. Yes, governments as trustees of individual and social data must develop APIs based and such other mechanisms for date usage and protection, for which 'data sandbox; looks a good description. The consultation paper rightly observes the need "to create anonymized, public data sets, which can be used as a test bed by newer service providers". This is the single most important political economy assertion towards a digital economy which will be both the most robust, as well as fair and just.

The IndiaStack initiative of Government of India already provides some data infrastructures as "digital public goods". India needs to now take this initiative to the next level, of providing all the key data and insights about people, things/machinery, physical and natural environment that can be considered as "data commons" to be labeled as such and provided equitably to all through such 'data sandbox" like arrangements that this paper suggests. Data companies should be obligated to contribute data sets that are user generated/owned or data that is 'commons'; into such a 'data sandbox' from where they should be made available for development of newer digital services, with adequate protection.

5 http://indiastack.org/about/

However, it is important to realize thatthe designing and implementing a trusteeship framework of society's common data, including individual's data, is an enormous undertaking New roles under such a framework need to be entrenched, and relevant powers defined and circumscribed, at the constitutional level. This process has already begun, and is underway, at the Supreme Court (with its recent privacy judgment and the upcoming Aadhaar case). But there may be need for more direct constitutional level or other statutory changes, and institutional development. We believe that we will ultimately require a constitutionally defined 'Data Institution' of some kind, that is insulated from the executive branch.

But small steps in the right direction matter a lot, and TRAI must be congratulated for having made a very brave start towards addressing this most important of questions related to the digital society and economy- 'who owns society's data and digital intelligence?'.

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?

We understand that it should be an APIs based systems, building over the IndiaStack architecture. Its DigiLocker and e-consent framework elements are especially relevant in this regard.

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?

We will pass this question as our response focuses on issues of data ownership and management.

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 mechanismsneed to be put in place

in order to address these issues?

We will pass this one too, and expect many other respondents to provide exhaustive responses to 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?

There can be no distinction between TSPs and other large businesses that collect user data. These distinctions are anachronistic and no longer relevant. When the question is about regulating data use and abuse in public interest it should not matter what kind of technical history or legacy a business comes from. The issue here is solely about collection of user data and building business models from it in a manner which could (1) harm user's privacy, and/or (2) misappropriate commercial value that should legitimately belong to the user, individually or collectively. All actors that come in this ambit need to be treated similarly.

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?

Such legitimate exceptions, as well as the needed checks and balances, must be devised with the highest human rights standards in mind, as per the global best practices, and must pass the constitutional test. For the best economic appropriation of data value, it is important to develop new data institutions that give shape to the state's role of trusteeship for individual and social data. But this can be an extremly dangerous endeavor if done without due constitutional and other statutory protections, that are effectively and diligently enforced. In default, a country may move towards becoming a data-authoritarian state, like China with its "social credit" project .[6]

6 https://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian

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?

To consider data collected from individuals, social, physical and natural environment in India as a collective national resource, and operationalizing such ownership, is basic to solving the pernicious problem whereby data and thereby digital intelligence of every sector, from transportation and tourism, to finance and market transactions, to health, education and governance, is being hoarded in foreign centres by foreign corporates. This will enable not only economic control but also social, cultural and political control over the country by outside actors in the times to come.

Once India begins asserting its national rights over its data, it will be in a much better position to negotiate global agreements about data flows and corresponding jurisdictional challenges. Seeking new agreements based on national ownership of data does not necessarily mean that data systems become territorialised, and global data flows are checked. It just means a more just and fair global data economy and data flows/ systems.