telenor

Telenor (India) Communications Pvt. Ltd.
(Erstwhile Telewings Communications Services Pvt. Ltd.)
The Masterpiece, Plot No. 10, Golf Course Road, Sector 54,
DLF Phase-V, Gurgaon, Haryana-122002.
www.telenor.in

T: +91-124-3329000
F: +91-124-3329996

06 November, 2017

Shri Arvind Gupta
Advisor (Broadband and Policy Analysis)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi 110002

Subject: Consultation Paper on "Privacy, Security and Ownership of the Data in the Telecom Sector"

Dear Sir,

This is with reference to the above referred TRAI consultation paper No. 09/2017 dated 09.08.2017. In this regard, please find enclosed our response to the consultation paper as an annexure to this letter.

We hope that the TRAI will find our response useful and consider our inputs while finalising the recommendations on this subject.

Thanking you,

Yours sincerely,
For **Telenor (India) Communications Pvt. Limited**
(Erstwhile Telewings Communications Services Private Limited)

(Pankaj Sharma)
Chief Corporate Affairs Officer

Encl: a.a.

Telenor (India) Response to TRAI Consultation Paper on Privacy, Security and Ownership of Data in the Telecom sector (No 09/2017 dated 9th August 2017)

Preamble

Indian telecom consumer usage is moving towards higher data consumption. From streaming videos to using social media or chat-driven apps, data is expected to be the key driver for the telecommunications industry growth in the years to come. As per the *Ericsson Mobility report'17*, between 2016 and 2022, total mobile data traffic is expected to grow at a CAGR of around 40 percent, reaching almost 8 EB[1] of data per month compared to around 1 EB of data consumption by the end of 2016. Factors driving growing data consumption include: fast-paced smart phone adoption, changing user behavior and disruptive pricing strategies. Today, application services, devices and access combined are growing into a utility i.e. inelastic need for all government services, commerce, health and education apart from simple person to person communications. The Government ambitious program - Digital India, has further fuelled the data growth and acts as an enabler for creating a country wide digital eco system. The data generated over all ICT platforms have taken the center-stage to better the delivery of each of these services. Thus, in the data driven market dynamics, privacy, ownership and security of data couldn't have come in for an extensive debate at a better time. The very foundation of Digital India resides on the privacy and security of users data.

While we are mindful of the limitations of the applicability of current set of data protection laws and regulations on the entire digital eco-system, nevertheless, this new start in the direction of a healthy consultation on the pillars of Digital India i.e. privacy and security of personal data is well timed.

The Supreme Court judgment on Right to Privacy – In the recent judgment of Hon'ble Supreme Court dated 24 Aug'17, in the case of *Justice K.S. Puttaswamy (Retd.) AND ANR. Vs Union of India AND ORS.*, it has been held that the inalienable fundamental right to privacy resides in the Article 21 fundamental freedom contained in Part III of the Constitution of India. In the judgment the right to privacy has been declared as a "guaranteed fundamental right". Thus, it is pertinent to mention that any statute on the privacy or any framework around that should satisfy the test as needs to be satisfied by the other Statues governing any part of Part III of the Constitution of India.

Consumer Data Protection Framework should be encompassing all stakeholders in the Internet value chain – The digital ecosystem comprises several e-services related to health, education, e-governance (taxes, passport, driving license, national

---

[1] An Exabyte (EB) is a unit of digital information storage used to denote the size of data. It is equivalent to 1 billion gigabytes (GB), 1,000 petabytes (PB) or 1,000,000,000,000,000,000 bytes (B)

identity etc), e-commerce, digital payments etc and telecommunications as an infrastructure service. Consumers, while using data services generate enormous amount of data as well as browse various websites / applications indicating their preferences and usage pattern which is an important tool for digital market place. In the entire internet value chain, several stakeholders get the benefit of consumer generated data. These stakeholders include – device manufacturers, App owners & developers, operating platforms & browser owners, content providers, network service providers etc. and protection of consumer data is of a paramount importance and equally applicable to all the stakeholders. However, the prevailing regulations pertaining to data privacy and protection are mostly applicable to telecom service providers and while the rest of the stakeholders in the digital market place have a greater control and flexibility to collect and use, user generated data to get consumer insights to the benefit of their own business growth. Telecom Service providers being one of the stakeholders should not be alone seen as data controller and responsible for implementing a monitorable privacy and confidentiality standard while offering communication services.

The telecom sector is currently heavily regulated with onerous obligations vide their licenses in the form of network security, confidentiality of data etc. with heavy pecuniary damages and sanctions for non-compliances. In comparison the rest of the players in the digital market place enjoy a regulatory oversight. Privacy & Security of data though has a large-scale impact across all the digital players in terms of their obligations towards their users and customers. In our view the obligations with respect to privacy and security of user data across the entire eco-system should be kept the same. This would be a key to modernizing regulations. Thus, it is important that **TRAI may consider recommending the need for a balanced consumer data protection framework, equally applicable to all the stakeholders ensuring level playing field.**

Need for common and comprehensive Data Protection legislation and establishment of the independent National Data Privacy & Security Regulator –

Privacy and security of data is a vast subject and touches all lives and therefore its protection should also apply equally across all players across various sectors in the space of collecting sensitive personal data of users in India. A national legislation is a route that many nations have adopted globally. India being the largest democracy with potentially one of the largest digital user base, would benefit through adoption of a national legislation for privacy of data as a common law replacing sector specific regulations. This becomes more important post the Supreme Court judgment on privacy wherein privacy is held as a fundamental right under Part III of the Constitution of India.

At this stage in India, there is an immense need to establish a separate legislative body to regulate privacy of data encompassing all the stakeholders. Artificial Intelligence, virtual reality, M2M & IOT are the newer technology adoptions elsewhere in the globe. Moreover, the sharp rise in mobile data adoption has exposed users to a series of frauds. With the increasing internet penetration, cyber crimes / frauds have also

increased in last few years[2]. As India progresses to a fully digitized platform the risks will increase exponentially. Privacy as an etiquette needs to be developed enabling a self regulating culture backed by the mandate of a national legislation. Awareness levels of the ills of sharing personal data, maybe proportionately low. Awareness levels of data privacy need to be increased in tandem with the exponential growth in mobile data usage and corresponding potential vulnerabilities. Privacy and security of personal data should be treated with utmost seriousness across the eco-system not only by the user (providers of data) but, even by the data collectors and /or data controllers. Both should be made aware of the risks, intent and purpose of the data provided/collected. Transparency in a declaration that the data is being collected for a specified purpose, after due consent, should be in a clear language and the inherent risks to all users.

The implementation of these proposals in an effective manner could only be made possible under an independent Privacy Regulator and enforcement of common privacy legislation equally applicable to the stakeholders of digital eco-system.

Question wise comments

Question 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?

Response:

- Presently, the data protection requirements applicable to the licensed TSPs are much stringent and wider in compare to other players in the digital eco-system on the premise of protection of consumer interest of telecom subscribers. TSPs being one of the stakeholders are having limited control over the data / content generated by the user in compare to other stakeholders while using the data services.
- The existing law – Information Technology Act 2000 (as Amended) and IT Rules[3] 2011 thereof are legally binding on all the sectors and stakeholders across India. However, additional penal provisions are exercised over TSP/ISPs vide their respective service licenses in addition to these laws. This has created an imbalance and unequal treatment for licensed TSPs/ISPs vis-à-vis other non licensed communication service providers.
- All related obligations in the Unified Licenses should be brought in tandem with the provisions of the IT Act / New Privacy legislation allowing for the same benefits and costs to apply to all other players of the digital eco-system.

[2] http://www.livemint.com/Technology/Rpy8mDxQVKMLs1BxN59dHJ/One-cybercrime-in-every-10-minutes-in-first-six-months-of-20.html

[3] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

- The impact of privacy of data stretches beyond only the ITES and Telecommunications sectors. As suggested in the preamble, we may consider having a common and comprehensive legislation at national level to protect the privacy of data of the users residing in India under the independent National Privacy Regulator. Such legislation on data security and privacy should be equally applicable across all sectors and all existing laws / licensing conditions to be subsumed into the common legislation. However, under this common legislation, the treatment of violation should be done basis the classification and sensitivity of the data.

- GSMA has done a considerable work on data protection and privacy framework. It is suggested that TRAI while framing the recommendations should also refer the GSMA documents on this subject ensuring international reflections and alignment at global stage.

Question 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?

Response:

- The definition of Personal Data outlined in the paper already aligns with international standards for the same. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organizations collect information about people. For instance, the GDPR's[4] definition is more detailed and makes it clear that information such as an online identifier – eg. an IP address – can be a personal data.

- The obligation of data collector to obtain user's consent should be purely depends upon the category and sensitivity of the information to be collected and the purpose for which the personal information will be used. In case, the personal sensitive information to be used for commercial purposes, we are of the view that the user consent should be obtained prior to respect his/her privacy provided his/her information is being shared in the identifiable format. However, in case of anonymized data and / or data available in the public domain being processed, there should not be any requirement for seeking user consent.

- Further, we are of the view that the consumer awareness of privacy principles through requirements of transparency by companies, such as through outlining a clear and accurate privacy policy and opt-outs for data usage, is the best way to empower users with respect to personal data. It will help users to take control of their

[4] The EU General Data Protection Regulation (GDPR), http://www.eugdpr.org/eugdpr.org.html

personal data and enable them to withdraw consent given earlier for commercial purposes which are not meeting their requirements / non fulfillment of a contract made for availing specific service(s).

- Similar practices are already outlined in European guidance on privacy and should be implemented in regulatory measures undertaken by countries outside of the EEA[5] to ensure consistent global regulations needed for the increasing uses of cross-border data.

Question 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.

Response:

- The rights and responsibilities of both data controllers and individuals, as well as those specified circumstances in which a data controller's rights may take precedence, are well defined by European regulations and are expressly addressed by the GDPR.

- Key rights of an data subject specified in GDPR (*Article 12 to 22*) are as follows (a) The right to be informed whether personal information collected or not (b) The right of access to personal data provided and purpose of processing (c) The right of rectification and right to be forgotten / erasure (delete) (d) The right to restriction of processing (e) The right to data portability (f) The right to object (g) Rights related to automated decision making and profiling.

- Similarly GDPR clearly mention about the responsibilities of Data controller(s) (Article 24 to 36) which are as follows: (a) Implementation of appropriate technical and organizational measures to ensure and demonstrate that processing is performed in accordance with GDPR (b) Implement data protection policies and ensure data protection by design and by default (c) processing of personal data necessary only for each specific purpose of the processing are processed (d) In case of joint data controllers, able to determine their respective responsibilities in transparent manner and inform contact point for data subjects (e) Any processor(s) processing personal data on behalf of data controller(s), controller shall use only processors providing sufficient guarantees to implement measures as per GDPR requirements (f) Processing of personal data under the authority of the controller or processor (g) Data Controller(s) / Processors shall on request cooperate with supervisory authority in the performance of its tasks (h) ensures security of the personal data (i) Notification of personal data breach to the supervisory authority (j) Communication of a personal data breach to the data subject (k) Carry out data protection impact assessment and identify the risk involved in processing under the

[5] The European Economic Area includes all 28 EU member states, plus Iceland, Lichtenstein and Norway. It does not include Switzerland.

advice of data protection officer (l) Prior consultation with supervisory authority before processing the personal data having high risk in the absence of measures taken by the controller to mitigate the risk.

- Aligning subsequent regulations with those of the European Directive, to be soon replaced by GDPR, provides a consistent global approach that will enable business while protecting consumers.

- In view of above, with respect to obtaining rights for use of user information should apply equally to all the stakeholders. Data Controllers rights over the sensitive personal data obtained from users residing in India would depend on the form of data i.e. raw data or processed data. Ownership of processed data to deliver better services is widely contested in a large part of the developed world. At this stage it may suffice to state that the user should have some rights with respect to providing additional data, correct the data or remove or delete the data. In the initial phase of privacy as a national legislation, awareness and transparency should be the pillars of maintaining privacy of personal data.

Question 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?

Response:

- Creation of a specified audit tool to monitor collection and use of personal data presents a number of problems, namely the nature of data and consent collection (in constant flux for most companies given the expanding use of data), the rapid advances in technology that would make maintaining such a tool and its workforce extremely costly- if at all possible, and the opening up of new possibilities for data hacking, mining, and abuse. In the best of scenarios, such a tool would be inefficient, expensive, and create additional exposure of consumer data by allowing new access points into the data.

- Instead, strengthening the requirements on companies to adequately protect this data, such as utilizing requirements similar to the European Directive, would advance the stated concern of protecting consumers.

- We suggest that each organisation processing personal data may implement internal mechanisms for certification of practices being adopted for data protection and submission of compliance to the designated authority annually. This is akin to the existing security related compliances being submitted by the licensed TSPs.

Question 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?

Response:

- Data driven businesses require consistent and predicable regulation that does not impede the development of new uses of data to meet the evolving needs of consumers.
- Maintaining compliance with conflicting regulatory schema, entering into business or developing new service offerings in a region with unpredictable or vague regulations or enforcement of the same, and having to seek approvals or comply with burdensome licensing and audit provisions for uses of data within the scope of existing collection and consent practices are strong deterrents for businesses and can lead to the decision to exist a market altogether.
- However, where a business can rely upon practices and processes that are uniform across the markets it serves and the services it seeks to provide the public, the efficiencies gained can continue to drive innovation. In India we may do well in encouraging all new technologies and businesses in the Digital market place and adopt lighter touch and future fit legislation approach equally applicable to all the stakeholders in the digital eco system.

Question 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?

Response:

- A data sandbox may provide businesses and academic/research bodies with the opportunity to gain insights into data sets that may not be readily available otherwise. However, the creation of such a sandbox both assumes that businesses are not in a better position to determine what data is relevant to the creation of new service offerings for its consumers, and provides opportunities for greater access to and duplication of the data in ways that threaten consumers.
- As with the audit tool referenced in Q4, to create such a sandbox implies that the data will be collected, stored, and made accessible on a much wider scale than is necessary to both administer the underlying consumer service and provide such data to the government where legally required. Again, new access points means new opportunities for data hacking, harvesting, and abuse, whereas clear regulation on the protection of this data at its source (the data controller and its authorized data processors) serves the stated purpose of consumer protection.

- In view of above, we are of the view that the Government or its authorized authority should not setup any data sandbox for, which allows the regulated companies to create anonymized data sets for the development of newer services. Instead, licensed TSPs should be allowed to do data analytics for their consumers. This will enable better and more relevant services to the consumers.

Question 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?

Response:

- Referring to the answer to question 8, we recommend that technical solutions for monitoring should be each partner's responsibility within their own domain. Each entity should be responsible for the data that they own.
- National authorities should ensure that monitoring is in place on important information exchange points. The monitoring performed by authorities, together with information provided by the network operators, will provide the needed national overview.

Question 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?

Response:

- The licensed TSPs are required to comply with the extensive and stringent security conditions laid down in the license. However, the other internet eco-system stakeholders who use data access channel of the TSPs to reach to the end customer with their services, including similar voice and messaging services are not subject to the same security restrictions as are imposed on the TSP.
- Therefore, collected industry efforts with the Government are required to protect the consumer personal data. In this regard, public – private partnership based on mutual trust between the network operators and authorities, including the national Computer Emergency Response Team (CERT) has to be the basis for any initiative regarding ecosystem monitoring.
- Exchange of information between the partners will enhance the capability of the national initiative to get an overview of existing and emerging threats as well as providing the network operators with important information to safeguard the communication.
- As suggested in the preamble, a national legislation under the independent national privacy regulator would serve the entire eco-system equally and will take care of future data protection and privacy issue that may arise across the digital ecosystem.

Question 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?

Response:

- All stakeholders in the digital ecosystem should have the same obligations related to collection and use of consumer data. Industry and method of service delivery should not be factors in the requirements of a data controller to collect and use personal data- a key component of the European Directive and GDPR. Please also refer to our response given in Q-3 above.

- Establishing requirements on telecoms and ISPs that do not flow to application providers and online service offerings, which frequently have the same or even greater access to consumer data, puts these service providers on unequal footing with others in the global economy while not adequately protecting consumers.

- The present licensing provisions and regulations pertaining to data privacy and protection is mostly applicable to TSPs and other stakeholders are having greater control and flexibility to use user generated data to get consumer insights for their business development and growth. Thus, it is important that TRAI should recommend consumer data protection framework which will be equally applicable to all the stakeholders ensuring level playing field.

Question 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?

Response:

- Again, all data controllers should be subject to the same obligations related to collection and use of consumer data. Where personal data is defined as broadly as this document and global privacy law requires, protections such as those outlined by the European Directive and GDPR provide a comprehensive set of requirements that do not distinguish between industry, service offering, or method of service delivery. Please also refer our response given for Q-2 and Q-3 above.

- While license restrictions applicable on TSPs have historically placed a greater regulatory burden on this industry, both because of greater than typical access to large amounts of personal data and a physical nexus to the region, these factors have become obsolete in the digital age.

- Players in all industries and with a global presence have as much or more access to personal data as do telecoms and ISPs and should be regulated just as stringently,

such as by a single set of guidelines that define acceptable data practices for all data controllers.

- The TSPs with Unified Licenses are heavily regulated under the unified license as well as to ensure compliance to the IT Act (as Amended) whereas the rest of the stakeholders of the digital eco-system are governed only by the IT act. In order to ensure level playing field among all the stakeholders of the digital ecosystem, all privacy, security and storage of user data should be governed by single national privacy legislation. Hence, onerous data and network security requirements, data storage requirements should be subsumed with a lighter touch requirement under common national privacy legislation.

Question 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?

Response:

- The data available in public domain accessible to all and anonymized data should not fall under the scope of data protection legislation. Moreover, the exceptions for data collection, use, and consent obligations for all data controllers are well specified by the European Directive and GDPR and should apply equally to TSPs and all other service providers in the digital ecosystem.

- Given the level of access required by law enforcement from TSPs, while also considering (a) the rights of consumers, (b) the need for companies to be transparent in their practices around sharing personal data with law enforcement, and (c) the need for mechanisms that allow companies to comply with requests for access in a predictable, legal, and consistent manner, the process by which law enforcement may require access to personal data must be outlined in clear terms that reflect the underlying legal process for such requests in the region.

- For example, where a signed court order is required by law enforcement to compel access to personal data from a business located in the region, the same requirements should be placed on TSPs. In addition, TSPs must be able to rely upon the established process without fear of penalty. Again, the goal is not to have special exceptions for TSPs but rather to put all businesses that hold Personal Data on equal footing and to provide consistent, predictable guidance that will allow businesses to design processes that comply with such guidance.

Question 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?

Response:

- The volume of cross-border data flow globally began to exceed the global value of trade in physical goods beginning in 2014 and will continue to increase year over year. TSPs are but a small portion of this cross-border data trend. For this reason, it is critical that regulations designed to protect consumer data are applied regardless of industry or service offering.

- Requirements like that found in the GDPR not only apply to players in the digital ecosystem but to all data controllers and have an extra-territorial effect for compliance and violations. While there may be greater challenges to enforcing data protection requirements for those business models without a physical presence in the region, this complication is addressed by the GDPR and is a fact of today's digital economy.

- Some of the key provisions specified in GDPR related to transfers of personal data to third countries or international organizations *(Article 44 to 50)* are as follows – (a) any personal data under processing / processing after transfer outside the country shall take place only after complying to the provisions of GDPR (b) Transfer of personal data after ensuring adequate level of protection (c) Transfer of personal data only after ensuring availability of appropriate safeguards – rights and legal remedies to data subjects (d) The binding corporate rules should be in place before any transfers (e) International cooperation for the protection of personal data.

- In order to remain competitive in the global marketplace, countries must facilitate service offerings that rely upon cross-border data flow (whether in the form of telecommunications services or e-commerce), and to do so requires a system of regulation that adequately addresses all business models and services providers.

****